

**CONTRATO PLURIANUAL DE 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, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ COMO EL INSTITUTO FONACOT, REPRESENTADO EN ESTE ACTO POR EL LIC. FRANCISCO JAVIER VILLAFUERTE HARO, EN SU CARÁCTER DE APODERADO LEGAL Y POR LA OTRA, LA EMPRESA DENOMINADA IQSEC, S.A DE C.V., REPRESENTADA EN ESTE ACTO POR LA SRA. YOLANDA SALDAÑA TAVERA, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ COMO EL PRESTADOR, DE CONFORMIDAD CON LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS:**

### **DECLARACIONES**

#### **I. DECLARA EL REPRESENTANTE DEL INSTITUTO FONACOT:**

- I.1. Que su representada, 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. Que su representada se encuentra inscrita en el Registro Federal de Contribuyentes de la Secretaría de Hacienda y Crédito Público, con la clave IFN060425C53.
- I.3. Cuenta con la facultad para suscribir el presente contrato, derivado del poder que le fue conferido mediante escritura pública número 212,692 de fecha 29 de julio de 2014, otorgada ante la fe del Lic. Eutiquio López Hernández, Notario Público número 35 de la Ciudad de México, instrumento que quedó debidamente inscrito en el Registro Público de Organismos Descentralizados, bajo el folio número 82-7-01082014-115726, el día 1° de agosto del 2014, con fundamento en los artículos 24 y 25 de la Ley Federal de las Entidades Paraestatales y 40, 41, 45 y 46 de su Reglamento.
- I.4. Que para el cumplimiento de sus funciones requiere la prestación del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones.
- I.5. Que en atención a lo anterior, el presente contrato se adjudicó al PRESTADOR mediante Licitación Pública Electrónica Nacional Con Reducción de Plazos No. LA-014P7R001-E349-2018, de conformidad con lo dispuesto en los artículos 134 Constitucional; 26 fracción I, 26 Bis fracción II, 27, 28 fracción I, 29, 32 tercer párrafo, 36 tercer párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 39 y 42 de su reglamento, 50 de la Ley de Presupuesto y Responsabilidad Hacendaria y 148 de su reglamento, así como del fallo emitido con fecha 10 de julio de 2018.
- I.6. Que para cubrir las erogaciones que se deriven del presente contrato, cuenta con recursos disponibles suficientes no comprometidos en la partida presupuestal número 33304, denominada "Servicios de Mantenimiento de aplicaciones informáticas", según oficio número SGA-077, de fecha 20 de abril de 2018, emitido por la Subdirección General de Administración, con la autorización del Director General del INSTITUTO FONACOT.

- I.7. Que no tiene conflicto de interés con el PRESTADOR, en términos de la fracción IX del artículo 49 de la Ley General de Responsabilidades Administrativas.
- I.8. Que su representado tiene su domicilio en Avenida Insurgentes Sur número 452, Colonia Roma Sur, Delegación Cuauhtémoc, C.P. 06760, Ciudad de México, mismo que señala para los fines y efectos legales de este contrato.

## II. DECLARA EL PRESTADOR, A TRAVÉS DE SU REPRESENTANTE:

- II.1. Que su representada es una sociedad anónima de capital variable, constituida conforme a las leyes mexicanas, como lo acredita con el instrumento número 79,927 de fecha 23 de agosto de 2007, otorgada ante la fe del Lic. Jorge Alfredo Domínguez Martínez, Notario Público No. 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. Que de acuerdo a sus estatutos, el objeto de su representada consiste entre otras actividades en comprar, vender, distribuir, sub distribuir, importar, arrendar, exportar y comercializar en general, toda clase de productos, mercancías, artículos y cualquier bien que esté en el comercio y en consecuencia sea susceptible de apropiación particular, enunciativa y no limitativamente toda clase de computadoras, sistemas de seguridad informática, sistemas de seguridad física, circuitos cerrados de televisión, enlaces de telecomunicaciones, equipos electrónicos de comunicación móvil para localización, programas y sistemas de cómputo, de información geográfica, para localización de unidades móviles, objetos y personas, mapas digitales y cartografía, equipos, componentes, mobiliario y accesorios relacionados con la actividad computacional, de telecomunicaciones y de oficina, elementos tecnológicos relacionados con la actividad computacional, de telecomunicaciones y de oficina, elementos tecnológicos relacionados y "hardware" y "software" en general.
- II.3. Que su representada se encuentra inscrita en el Registro Federal de Contribuyentes de la Secretaría de Hacienda y Crédito Público, bajo la clave IQS0708233C9.
- II.4. Que la señora YOLANDA SALDAÑA TAVERA, cuenta con facultades suficientes para representar y obligar al PRESTADOR en los términos del presente contrato, como así consta en el instrumento número 96,546 de fecha 18 de febrero de 2014, otorgado ante la fe del Lic. Jorge Alfredo Domínguez Martínez, Notario Público No. 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, así como poder especial, y se identifica con su credencial para votar clave de elector [REDACTED] expedida por el Instituto Nacional Electoral, con vigencia al año 2025.
- II.5. Que su representada dispone de la organización, experiencia, personal capacitado y demás recursos técnicos, humanos y económicos necesarios, así como de la capacidad legal suficiente para llevar a cabo los trabajos materia del presente contrato.
- II.6. Que su representada se encuentra al corriente en el cumplimiento de sus obligaciones fiscales de conformidad con lo dispuesto por el Artículo 32-D del Código Fiscal de la Federación y de la regla 2.1.31 de la Resolución Miscelánea Fiscal para 2018, relativo al procedimiento que debe observarse para contrataciones con la Federación y entidades federativas, habiendo obtenido opinión positiva.

Eliminado: una palabra del octavo renglón del séptimo párrafo. Datos de la Identificación Oficial Credencial para Votar con fotografía.

Fundamento Legal: artículo 116 Primer párrafo de la Ley General de Transparencia y Acceso a la Información Pública; artículo 113 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; artículo 3 fracción IX, 6, 18 primer párrafo y artículo 31 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, así como para la elaboración de versiones públicas.

Motivación: Se considera información confidencial la que contiene datos personales concernientes a una persona física identificada o identificable.

- II.7.** Que se encuentra al corriente en el cumplimiento de sus obligaciones fiscales en materia de seguridad social de conformidad con lo dispuesto en la regla primera del Anexo Único del Acuerdo ACDO. SAI.HCT.101214/281.P.DIR dictado por el H. Consejo Técnico del Instituto Mexicano del Seguro Social, relativo a las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social”, publicado en el Diario Oficial de la Federación el 27 de febrero de 2015, habiendo obtenido opinión positiva.
- II.8.** Que se encuentra al corriente en el cumplimiento de sus obligaciones fiscales en materia de aportaciones patronales y entero de descuentos, de conformidad con lo dispuesto en el Acuerdo Único del H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores, relativo a las “Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos”, publicado en el Diario Oficial de la Federación el 28 de junio de 2017, habiendo obtenido constancia de no adeudo.
- II.9.** Que manifiesta bajo protesta de decir verdad, que ninguno de sus socios o accionistas desempeña empleo, cargo o comisión en el servicio público, por lo que no se actualiza conflicto de interés, no encontrándose dentro del supuesto del artículo 49 fracción IX de la Ley General de Responsabilidades Administrativas, ni se encuentra en alguno de los supuestos de los artículos 50 y 60 antepenúltimo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En caso de que alguna de las personas físicas que forman parte del PRESTADOR se encuentre en los supuestos señalados anteriormente, el contrato será nulo previa determinación de la autoridad competente de conformidad con lo establecido en el artículo 15 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

- II.10.** Que, bajo protesta de decir verdad, manifiesta que su representada se encuentra clasificada como Mediana empresa, de conformidad con lo establecido en el artículo 3, fracción III de la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa y en el artículo 34 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
- II.11.** Que su representada tiene su domicilio en Avenida Patriotismo número 399, Colonia San Pedro de los Pinos, Delegación Benito Juárez, C.P. 03800, Ciudad de México, mismo que señala para los fines y efectos legales del presente contrato.

### **III. AMBAS PARTES DECLARAN:**

- III.1.** Que están de acuerdo en que los apartados, títulos e incisos del presente contrato, únicamente se asignan para fines de claridad y de referencia y de ninguna manera se consideran como interpretación de condiciones del texto de este contrato.
- III.2.** Que se reconocen la personalidad y facultades con las que se ostentan y manifiestan que las facultades con que actúan no les han sido revocadas o modificadas en forma alguna, por lo que están conformes en obligarse de acuerdo a las siguientes:



## CLÁUSULAS

**PRIMERA. OBJETO DEL CONTRATO.** El INSTITUTO FONACOT encomienda al PRESTADOR y éste se obliga a llevar a cabo la prestación del **Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones**, de conformidad con la descripción y especificaciones contenidas en el Anexo Técnico y en la Propuesta Económica del PRESTADOR que como Anexos I y II, se agregan al presente contrato, los cuales una vez rubricados por las partes, formarán parte integrante del mismo; para lo cual el PRESTADOR pondrá toda su experiencia y capacidad, dedicándole todo el tiempo que sea necesario.

**SEGUNDA. 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, integrará una serie de servicios que se llevarán a cabo para asegurar la correcta mitigación y control de los hallazgos resultado del servicio de *Assessment* de seguridad de la información que se llevó a cabo en el INSTITUTO FONACOT, así como los posibles eventos que pudiesen presentarse durante la vigencia del servicio y 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 protección y reputación de identidad institucional
7. Servicio de sensibilización de tecnologías de la información
8. Servicio de administración del SGSI
9. Servicio de protección de estaciones de trabajo

EL PRESTADOR se obliga apegarse a los lineamientos que establece la Estrategia Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de los Requerimientos de Seguridad de la Información (Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y en la Seguridad de la Información, MAAGTICSI), publicados en el Diario Oficial de la Federación el 08 de mayo de 2014 y el 04 de febrero de 2016, y en las versiones que se actualicen y estén vigentes durante la duración del presente contrato, y aquellas que se acuerden entre el INSTITUTO FONACOT y el PRESTADOR.

**TERCERA. LUGAR DE LA PRESTACIÓN DEL SERVICIO.** La prestación del servicio se llevará a cabo en el edificio sede del INSTITUTO FONACOT, sito en Av. Insurgentes Sur # 452, Colonia Roma Sur, Delegación Cuauhtémoc, C.P. 06760, Ciudad de México, de acuerdo a las necesidades del INSTITUTO FONACOT, el resto del personal prestará sus servicios en las oficinas del PRESTADOR, sin embargo, se presentarán cuando así lo requiera el INSTITUTO FONACOT, en un tiempo no mayor a 1 hora (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 a las necesidades del servicio previa notificación con 8 horas (ocho horas) por parte de la Subdirección General de Tecnologías de la Información y Comunicación del INSTITUTO FONACOT, en los domicilios que se enlistan en el Directorio de Sucursales incluido en el Anexo Técnico del PRESTADOR (Anexo I).

**CUARTA. ENTREGABLES.** El PRESTADOR generará 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 (cinco) 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 de Inicio del proyecto:**

- Minuta de la Reunión de *Kick Off*.
- Plan de Trabajo General.
- Plan de Trabajo detallado por Servicio a Implementar
- Memoria Técnica de cada servicio implementado

**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 *ciber*patrullaje e integridad de imagen institucional. (*dark web* y *deep web*)
- Reporte de disponibilidad de recursos.
- 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**)
  - o SOW.
  - o INFORME DE ANÁLISIS DE CÓMPUTO FORENSE – TÉCNICO.
  - o MEMORIA TÉCNICA DE ADQUISICIÓN DE INFORMACIÓN.
- Reporte de cambios en la configuración de los servicios.
- Reporte de estadísticas e indicadores de concientización.
- Reporte de histórico de políticas de cifrado de archivos.
- Reporte de trazabilidad de SVI.
- Reporte de dependencia lógica de los servicios críticos.
- Reporte de afectaciones de activos.
- Reporte de implementación de SGSI.

El PRESTADOR 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 PRESTADOR 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 el presente contrato y sus Anexos.

**QUINTA. PRECIOS UNITARIOS.** El INSTITUTO FONACOT pagará al PRESTADOR por los servicios a que se refiere el presente vínculo jurídico, los precios unitarios que se detallan en la Propuesta Económica del PRESTADOR que como Anexo II se agrega al presente contrato, el cual una vez rubricado por las partes, formará parte integrante del mismo.

Los precios son en moneda nacional y serán considerados fijos hasta que concluya la relación contractual, debiendo incluir el PRESTADOR todos los costos involucrados considerando todos los conceptos del servicio que requiere el INSTITUTO FONACOT, por lo que el PRESTADOR no podrá agregar ningún costo extra y serán inalterables durante la vigencia del presente contrato.

Asimismo, el INSTITUTO FONACOT, con fundamento en lo previsto en el artículo 66, fracción I del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, no pagará al PRESTADOR aquellos servicios solicitados y no proporcionados.

**SEXTA. MONTO TOTAL DEL CONTRATO.** Por la totalidad de los servicios efectivamente devengados a que se refiere el presente contrato, el INSTITUTO FONACOT pagará al PRESTADOR la cantidad de \$191,522,398.20 (ciento noventa y un millones quinientos veintidós mil trescientos noventa y ocho pesos 20/100 M. N.) más el Impuesto al Valor Agregado.

El pago de los servicios quedará condicionado, proporcionalmente al pago que el PRESTADOR deba efectuar en su caso por concepto de penas convencionales.

Si el PRESTADOR realiza trabajos por mayor valor del indicado, independientemente de la responsabilidad en que incurra por la ejecución de los trabajos excedentes, no tendrá derecho a reclamar pago alguno por ello.

**SÉPTIMA. EJERCICIO PRESUPUESTAL.** El presupuesto a ejercer por los servicios prestados durante los ejercicios fiscales del 2018 al 2021, serán por las cantidades que a continuación se describen, más el Impuesto al Valor Agregado:

Año	2018	2019	2020	2021	TOTAL
Monto	\$32,832,411.12	\$65,664,822.24	\$65,664,822.24	\$27,360,342.60	\$191,522,398.20

La ejecución y pago del servicio, estarán sujetos a la disponibilidad del presupuesto que sea autorizado por la H. Cámara de Diputados en el Presupuesto de Egresos de la Federación para cada ejercicio fiscal y al oficio de Liberación del Presupuesto que la Secretaría de Hacienda y Crédito Público, emita al INSTITUTO FONACOT por cada período del 2018 al 2021, respectivamente. No habrá penalización ni responsabilidad alguna de ningún tipo para el INSTITUTO FONACOT, en caso de que ocurra alguna variación por asignación y cuantía menor en los presupuestos que aprueben las autoridades mencionadas en este párrafo, que impida la continuidad del servicio objeto de este contrato, para cualquiera de los ejercicios fiscales.

**OCTAVA. FORMA DE PAGO.** En el presente servicio no se otorgarán anticipos. Para que la obligación de pago se haga exigible, el PRESTADOR deberá presentar a partir del día hábil siguiente a la prestación de los servicios y presentación de los entregables, la documentación completa y debidamente requisitada para realizar el trámite de pago, y de conformidad con lo

dispuesto en el artículo 29 del Código Fiscal de la Federación, el PRESTADOR deberá emitir comprobantes fiscales digitales por Internet (CFDI), que son facturas electrónicas que el PRESTADOR pondrá a disposición del INSTITUTO FONACOT en archivo XML (archivo electrónico del comprobante fiscal digital por Internet) y de manera adicional entregará la representación de la factura electrónica en un documento impreso en papel, esta última debidamente sellada y firmada por el Administrador del Contrato, desglosando el Impuesto al Valor Agregado y los descuentos que en su caso se otorguen al INSTITUTO FONACOT.

El INSTITUTO FONACOT cubrirá al PRESTADOR la cantidad señalada en la cláusula que antecede, en pagos mensuales, excepto el primer mes, el cual se pagará, si fuera el caso, de manera proporcional a partir del día 11 de julio de 2018 y hasta el final del mes el día 31 de Julio de 2018, de acuerdo a los servicios devengados debidamente soportado y acompañado con los entregables que apliquen de acuerdo a lo establecido en el presente contrato y sus anexos. El pago mensual se realizará a través del programa de cadenas productivas o depósito interbancario a la cuenta [REDACTED]

[REDACTED] dentro de los 20 (veinte) días naturales, posteriores a la presentación de la factura correspondiente, la cual deberá contener los requisitos de ley y contar con el visto bueno del administrador del contrato.

El PRESTADOR podrá modificar el número de cuenta y el nombre de la institución bancaria citada en esta cláusula, siempre que dé aviso al INSTITUTO FONACOT por lo menos con 10 (diez) días naturales de anticipación a la presentación de la factura.

**NOVENA. PAGOS.** Para el pago de los servicios efectivamente proporcionados, el PRESTADOR deberá entregar lo siguiente:

- a. 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, considerando el Anexo 20 "Guía de llenado de los comprobantes fiscales digitales por internet". Dichos comprobantes serán entregados en las oficinas centrales del INSTITUTO FONACOT, ubicadas en Avenida Insurgentes Sur No. 452, Col. Roma Sur, C.P. 06760, Delegación Cuauhtémoc, Ciudad de México, 2° piso, en la oficina de la Dirección de Tecnologías de la Información, en un horario de labores de lunes a viernes de 9:00 a las 15:00 horas y en el caso de la factura enviar al siguiente correo electrónico: [angel.gascon@fonacot.gob.mx](mailto:angel.gascon@fonacot.gob.mx) con copia al correo [javier.jimenez@fonacot.gob.mx](mailto:javier.jimenez@fonacot.gob.mx)
- b. De conformidad con lo dispuesto en el artículo 89 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, para efectos de contabilizar el plazo a que hace referencia el primer párrafo del artículo 51 de la Ley mencionada, se tendrán como recibidos los comprobantes fiscales citados en el inciso anterior que reúnan los requisitos fiscales correspondientes, a partir de que el PRESTADOR los entregue al INSTITUTO FONACOT, al momento de concluir la prestación total o parcial del servicio, conforme a los términos del contrato celebrado y el INSTITUTO FONACOT los reciba a satisfacción, en los términos de los lineamientos que emita la Secretaría de la Función Pública para promover la agilización del pago.

Dentro de los veinte días naturales contados a partir de la entrega de los comprobantes fiscales, previa prestación de los servicios, en los términos del presente contrato, el INSTITUTO FONACOT deberá requerir en su caso, al PRESTADOR, la corrección de errores o deficiencias contenidos en dichos comprobantes fiscales que reúnan los requisitos

Eliminado: séptimo y octavo renglón del segundo párrafo. Datos de la Cuenta Bancaria (No. de Cuenta, CLABE, Sucursal y Plaza)  
Fundamento Legal: artículo 116 tercer párrafo de la Ley General de Transparencia y Acceso a la Información Pública; artículo 113 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública; artículos 46 y 142 de la Ley de Instituciones de Crédito y artículo 31 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; así como los lineamientos Trigésimo Octavo fracción III y Cuadragésimo Segundo 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 tratarse de Información que identifica un Secreto Bancario.



fiscales correspondientes; tramitar el pago de esos comprobantes fiscales y realizar el pago al PRESTADOR.

El INSTITUTO FONACOT dará al PRESTADOR la opción de recibir el pago por medios electrónicos.

Asimismo, de acuerdo a lo establecido en el artículo 90 del Reglamento referido, en caso de que los comprobantes fiscales entregados por el PRESTADOR para su pago, presenten errores o deficiencias, el INSTITUTO FONACOT dentro de los tres días hábiles siguientes al de su recepción, indicará por escrito al PRESTADOR las deficiencias que deberá corregir. El periodo que transcurra a partir de la entrega del citado escrito y hasta que el PRESTADOR presente las correcciones, no se computará para efectos del artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

**DÉCIMA. VIGENCIA.** La vigencia del presente contrato será del 11 de julio de 2018 al 31 de mayo de 2021, la cual será forzosa para el PRESTADOR y voluntaria para el INSTITUTO FONACOT.

Si terminada la vigencia de este contrato el INSTITUTO FONACOT tuviera la necesidad de seguir utilizando los servicios del PRESTADOR, se requerirá la celebración de un nuevo contrato.

**DÉCIMA PRIMERA. GARANTÍA DE CUMPLIMIENTO DEL CONTRATO ABIERTO PLURIANUAL.** El PRESTADOR garantizará el cumplimiento del presente contrato entregando al INSTITUTO FONACOT dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato abierto plurianual, tal como se refiere en la fracción II del artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, póliza de fianza, en moneda nacional, expedida por institución legalmente autorizada para operar en el ramo, conforme a la legislación mexicana, a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores (INSTITUTO FONACOT), por un importe equivalente al 10% (Diez por ciento) del monto máximo total a erogar en el ejercicio fiscal 2018, sin incluir el Impuesto al Valor Agregado, renovando la garantía en los ejercicios fiscales del 2019, 2020 y 2021, de conformidad con el artículo 85 fracción III del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, bajo las mismas condiciones que se describen en la presente cláusula.

De conformidad con lo dispuesto por el artículo 103 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, cuando la forma de garantía sea mediante fianza, cada una de las pólizas de fianza deberá contener en su texto, como mínimo, las siguientes previsiones:

- a) Que cada una de las fianzas que se otorgan, atenderán a todas las estipulaciones contenidas en el presente contrato abierto plurianual.
- b) Que para cancelar cada una de las fianzas, será requisito contar con la constancia de cumplimiento total de las obligaciones contractuales de cada ejercicio presupuestal, para lo cual se requerirá la respectiva manifestación expresa y por escrito del INSTITUTO FONACOT.
- c) Que cada una de las fianzas permanecerá vigente durante el cumplimiento de la obligación que garantice cada ejercicio presupuestal y continuará vigente en caso de que se otorgue prórroga al cumplimiento del contrato, así como durante la substanciación de todos los recursos legales o de los juicios que se interpongan y hasta que se dicte resolución definitiva que quede firme, y



- d) Que la afianzadora acepta expresamente someterse a los procedimientos de ejecución previstos en la Ley de Instituciones de Seguros y de Fianzas, para la efectividad de las fianzas, aún para el caso de que proceda el cobro de indemnización por mora, con motivo del pago extemporáneo del importe de la póliza de fianza requerida, quedando a elección del INSTITUTO FONACOT poder reclamar el pago de la fianza por cualquiera de los procedimientos establecidos en los artículos 282 y 283 de dicha Ley.

Que la institución afianzadora otorga expresamente y en forma automática, sin necesidad de que medie aviso, su consentimiento en términos del artículo 179 de la Ley de Instituciones de Seguros y de Fianzas, en caso de que el INSTITUTO FONACOT decida otorgar prórrogas y/o esperas al PRESTADOR.

En el supuesto de rescisión de este contrato por causas imputables al PRESTADOR, la fianza se hará exigible de inmediato sin necesidad de juicio previo ni declaración judicial alguna, sin perjuicio de la responsabilidad que pudiese fincarle el INSTITUTO FONACOT al PRESTADOR ante autoridad competente.

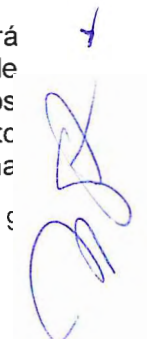
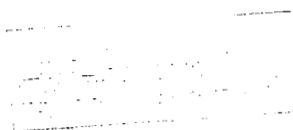
La garantía de cumplimiento del contrato, se hará exigible de inmediato, sin necesidad de juicio previo ni declaración judicial alguna, y sin perjuicio de la responsabilidad que pudiese fincarle el INSTITUTO FONACOT al PRESTADOR ante autoridad competente, cuando se presente de manera enunciativa y no limitativa, alguno de los siguientes casos:

- Cuando por causas imputables al PRESTADOR, se incumpla con cualquiera de las condiciones pactadas en el contrato y consecuentemente se rescinda el mismo, o
- Cuando se haya vencido el plazo para el inicio de la vigencia del contrato y el PRESTADOR por sí mismo o a requerimiento del INSTITUTO FONACOT, no sustente debidamente las razones del incumplimiento en el inicio, previo agotamiento de las penas convencionales respectivas, o
- Cuando se detecten vicios ocultos o defectos de la calidad de los servicios recibidos.

**DÉCIMA SEGUNDA. DEVOLUCIÓN DE LA GARANTÍA DE CUMPLIMIENTO.** La fianza a que se refiere la cláusula que antecede será cancelada por el INSTITUTO FONACOT a través de la Dirección de Recursos Materiales y Servicios Generales, una vez que el PRESTADOR demuestre haber cumplido con la totalidad de las obligaciones adquiridas en el presente contrato; para cancelar la fianza será indispensable la constancia de cumplimiento total de las obligaciones, donde conste la manifestación expresa y por escrito del INSTITUTO FONACOT en ese sentido, con fundamento en el artículo 103, fracción I, inciso b, del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

**DÉCIMA TERCERA. RESPONSABILIDAD CIVIL.** El PRESTADOR se compromete ante el INSTITUTO FONACOT a responder por los daños y perjuicios que le pudiera ocasionar el ejercicio del presente contrato 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.

**DÉCIMA CUARTA. GARANTÍA DE RESPONSABILIDAD CIVIL.** El PRESTADOR garantizará durante la vigencia del contrato, 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. Mediante una



póliza de responsabilidad civil, expedida por institución autorizada por las Leyes Mexicanas a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores (INSTITUTO FONACOT), por un monto 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 IQSEC, S.A. de C.V. La cual deberá ser entregada dentro de 5 (cinco) días hábiles contados a partir del día 11 de julio de 2018, en la Dirección de Tecnologías de la Información sito en Avenida Insurgentes Sur No. 452, 2º Piso, Colonia 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 válida la garantía por responsabilidad civil que el PRESTADOR se obliga a presentar al Administrador del Contrato a través del titular de la Dirección de Tecnologías de Información.

En caso de que algún siniestro supere el monto de la Póliza requerida, el PRESTADOR se hará cargo de la totalidad de los gastos que este llegue a generar, por lo que el PRESTADOR se compromete ante el INSTITUTO FONACOT a responder por los daños y perjuicios que le pudiera ocasionar el ejercicio del presente contrato 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.

**DÉCIMA QUINTA. RESPONSABILIDAD LABORAL.** El PRESTADOR bajo su más estricta responsabilidad, podrá nombrar los auxiliares, especialistas o técnicos que requiera para la prestación del servicio materia del presente contrato, en el entendido de que asumirá responsabilidad total de la actuación de los mismos, respondiendo de los daños y/o perjuicios que en su caso éstos en el desempeño de su participación llegaren a ocasionar al INSTITUTO FONACOT.

El PRESTADOR como patrón de las personas que en su caso designen como sus auxiliares, especialistas o técnicos para llevar a cabo el objeto del presente contrato, será el único responsable de las obligaciones derivadas de las disposiciones legales y demás ordenamientos aplicables en materia de trabajo y seguridad social, obligándose a responder de todas y cada una de las reclamaciones que dichas personas presenten en su contra o en contra del INSTITUTO FONACOT, obligándose en este mismo acto a dejar en paz, a salvo y libre de cualquier responsabilidad al INSTITUTO FONACOT, reconociendo expresamente el PRESTADOR que es el único responsable del pago de sus sueldos, salarios, cuotas del Instituto Mexicano del Seguro Social y todas las demás prestaciones establecidas en los ordenamientos legales, comprometiéndose a mantener a salvo en todo momento al INSTITUTO FONACOT, en caso de cualquier reclamación que se presentare en su contra derivada de su relación contractual con el INSTITUTO FONACOT o, en su caso, contra el INSTITUTO FONACOT por dicho concepto.

En caso de que las personas designadas por el PRESTADOR como sus auxiliares, especialistas o técnicos, sufran accidentes de trabajo, en su acepción establecida por la Ley Federal del Trabajo, el PRESTADOR asumirán la responsabilidad, dejando libre al INSTITUTO FONACOT de cualquier acción que pudiera interponerse por tal acontecimiento.

El PRESTADOR se obliga a cubrir al INSTITUTO FONACOT los gastos y costas judiciales erogadas por este último, a causa de que concurra cualquier circunstancia planteada en la presente cláusula.

**DÉCIMA SEXTA. OBLIGACIONES DEL PRESTADOR.** El PRESTADOR se obliga a:





- a) Cumplir totalmente y a satisfacción del INSTITUTO FONACOT con el servicio objeto del presente contrato.
- b) Contar con el personal profesional, técnico y administrativo, especializados en el ramo, que sean necesarios y suficientes para cumplir con los planes de trabajo programados, para la ejecución, operación y supervisión continua de los servicios, que abarcan la instalación, puesta en marcha y operación del Servicio.
- c) Mantener el nivel de experiencia y especialidad que señaló tener el personal propuesto para realizar los servicios.
- d) Asegurar la correcta implementación de todas las soluciones tecnológicas a través de su personal y que de manera simultánea aseguren la correcta implementación y transición de los servicios.

**DÉCIMA SÉPTIMA. CALIDAD DEL SERVICIO.** EL PRESTADOR quedará obligado ante el INSTITUTO FONACOT a responder de la calidad de los servicios prestados, así como de cualquier otra responsabilidad en que hubiere incurrido, en los términos señalados en el presente contrato, en lo dispuesto por la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y/o en la legislación aplicable.

El PRESTADOR deberá contar con la infraestructura necesaria, personal profesional y/o técnico especializado en el ramo, herramientas, procedimientos, refacciones técnicas y equipos adecuados, para el tipo de servicios solicitados, a fin de garantizar que los servicios objeto del presente contrato sean proporcionados con la calidad, oportunidad y eficiencia requerida para tal efecto, comprometiéndose a desarrollarlo a satisfacción del INSTITUTO FONACOT.

El PRESTADOR, para efectos de la prestación de los servicios, deberá cumplir con la certificación ISO 27001, certificación ISO/IEC 27001, y certificación CERT (*COMPUTER EMERGENCY RESPONSE TEAM*, EQUIPO DE RESPUESTA ANTE EMERGENCIAS INFORMÁTICAS), así como con las normas oficiales mexicanas, las normas mexicanas y a falta de éstas, las normas internacionales o en su caso, las normas de referencia vigentes que resulten aplicables para el tipo de los servicios solicitados.

El personal autorizado del INSTITUTO FONACOT, cuando así lo estime conveniente, se encargará de comprobar, supervisar y verificar la realización correcta y eficiente de los servicios objeto del presente contrato.

El PRESTADOR manifiesta su conformidad para que el INSTITUTO FONACOT supervise los servicios que se compromete a proporcionar. Dicha supervisión no exime ni libera al PRESTADOR de las obligaciones y responsabilidades contraídas en virtud de este contrato.

El INSTITUTO FONACOT podrá rechazar los servicios si no reúnen las especificaciones y alcances establecidos en este contrato, obligándose el PRESTADOR en este supuesto a realizarlos nuevamente bajo su exclusiva responsabilidad y sin costo adicional para el INSTITUTO FONACOT.

**DÉCIMA OCTAVA. GARANTÍA DE LA CALIDAD DE LOS SERVICIOS.** El PRESTADOR corregirá los 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 el presente contrato y el Anexo Técnico del PRESTADOR (Anexo I), y con cargo al PRESTADOR, .

**DÉCIMA NOVENA. OBSERVACIONES AL SERVICIO.** Convienen las partes en que el INSTITUTO FONACOT queda facultado para hacer las observaciones que estime pertinentes para el mejor desarrollo del servicio objeto de este contrato, las cuales serán atendidas de inmediato por el PRESTADOR.

**VIGÉSIMA. CONFIDENCIALIDAD.** Con motivo de la prestación del SERVICIO contratado, el INSTITUTO FONACOT proporcionará al PRESTADOR toda la información y documentación necesaria para el debido desempeño de sus funciones, misma que el PRESTADOR se obliga a guardar y a hacer guardar estricta confidencialidad y reserva.

Toda la documentación que con motivo del presente contrato, el INSTITUTO FONACOT entregue al PRESTADOR, así como toda la información que el PRESTADOR desarrolle, será 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 Gubernamental y de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, debiendo el PRESTADOR 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 PRESTADOR 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 llegarán 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 PRESTADOR sea constitutiva de delito, en perjuicio del INSTITUTO FONACOT, éste podrá proceder a 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, diskettes o cualquier otro material que tenga información jurídica, operativa, técnica, financiera, de análisis, compilaciones, estudios, gráficas o cualquier otro similar.

**VIGÉSIMA PRIMERA. UTILIZACIÓN DE LA INFORMACIÓN CONFIDENCIAL.** Con la información que sea proporcionada al PRESTADOR, éste se obliga a:

- a) Utilizar toda la información a que tenga acceso o generada con motivo del servicio, únicamente para prestar el objeto de este contrato.
- b) Limitar la revelación de la información y documentación a que tenga acceso, únicamente a las personas que dentro de su propia organización se encuentren autorizadas para conocerla, haciéndose responsable del uso que dichas personas puedan hacer de la misma.
- c) No hacer copias de la información, sin la autorización por escrito del INSTITUTO FONACOT.
- d) No revelar a ningún tercero la información sin la previa autorización por escrito del INSTITUTO FONACOT.





- e) Una vez concluida la vigencia del presente contrato, el PRESTADOR entregará al INSTITUTO FONACOT todo el material y copias que contenga la información confidencial recabada o que le haya sido proporcionada por el INSTITUTO FONACOT, así como la documentación e información proporcionada, conocida, desarrollada u obtenida con motivo del desempeño de sus actividades materia de contratación.

**VIGÉSIMA SEGUNDA. IMPUESTOS Y DERECHOS.** Los impuestos y derechos que procedan con motivo de la contratación de los servicios, serán pagados por cada una de las partes, según corresponda, de acuerdo con lo establecido en las disposiciones legales vigentes en la materia.

**VIGÉSIMA TERCERA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES.** El PRESTADOR no podrá en forma alguna ceder ni transferir en forma total o parcial los derechos y obligaciones derivados de este contrato, salvo los derechos de cobro, mismos que sólo podrán ser cedidos con la aceptación expresa que por escrito otorgue el INSTITUTO FONACOT al PRESTADOR, conforme a lo establecido en el último párrafo del artículo 46, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

**VIGÉSIMA CUARTA. MODIFICACIONES.** El INSTITUTO FONACOT con fundamento en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, podrá incrementar el monto del contrato o la cantidad de los servicios, siempre que las modificaciones no rebasen en su conjunto, el veinte por ciento del monto o cantidad de los conceptos o volúmenes establecidos originalmente en los mismos, dentro de su vigencia, y que el precio sea igual al pactado originalmente en el contrato que se modifique.

Por lo que se refiere a la vigencia, ésta podrá ser ampliada, siempre que no se rebase el primer trimestre del ejercicio fiscal siguiente y resulte indispensable para no interrumpir la operación regular del INSTITUTO FONACOT, de conformidad con lo establecido el artículo 92 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y último párrafo del artículo 146 del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.

**VIGÉSIMA QUINTA. NIVELES DE SERVICIO.** El PRESTADOR considerará 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 y especificados en el presente contrato y el Anexo Técnico del PRESTADOR (Anexo I).

CONCEPTO	Atención y solución de las incidencias o problemas con base a su complejidad			
	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.
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

**VIGÉSIMA SEXTA. PROCEDIMIENTO PARA LA APLICACIÓN DE PENAS CONVENCIONALES.** Conforme a lo dispuesto en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y primer párrafo del artículo 96 de su Reglamento, en caso de atraso en el cumplimiento de la prestación de los servicios objeto del presente contrato, el PRESTADOR queda obligado a pagar penas convencionales, por cada día natural de atraso en el servicio, hasta su cumplimiento a entera satisfacción del INSTITUTO FONACOT, considerando los siguientes casos:






PENAS CONVENCIONALES		
No.	Descripción	Monto
1	Minuta de la Reunión de Kick Off de este con el numeral 29. ENTREGABLES Anexo Técnico "Características Técnicas del Servicio".	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 del Prestador, la cual deberá entregarse <u>a más tardar a los cinco días hábiles de haberse llevado a cabo la referida reunión.</u>
2	Atraso en la entrega del Plan de Trabajo General de conformidad con el numeral 29. ENTREGABLES Anexo Técnico "Características Técnicas del Servicio".	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 <u>a más tardar a los cinco días hábiles después de firmado el Contrato.</u>
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 29 ENTREGABLES Anexo Técnico "Características Técnicas del Servicio".	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 29 ENTREGABLES del Anexo Técnico "Características Técnicas del Servicio".	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 <u>a más tardar a los cinco días de concluido la implementación respectiva del servicio correspondiente.</u>
5	Atraso en los tiempos establecidos en la implementación de los servicios objetos de conformidad con el numeral 29 ENTREGABLES del Anexo Técnico "Características Técnicas del Servicio".	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.

Cuando el monto total de aplicación de las penas convencionales rebase el 10% del valor total del presente contrato, el INSTITUTO FONACOT podrá iniciar el procedimiento de rescisión del contrato, en los términos del artículo 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

De conformidad con el segundo párrafo del artículo 95 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el pago 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 no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento.

Para determinar la aplicación de las penas convencionales, no se tomarán en cuenta las demoras motivadas por caso fortuito o causas de fuerza mayor o cualquier otra causa no imputable al PRESTADOR.

De conformidad con lo dispuesto en la parte final del primer párrafo del artículo 96 del Reglamento citado, la suma de todas las penas convencionales aplicadas al PRESTADOR por ningún concepto podrá exceder el monto de la garantía de cumplimiento del Contrato.

Si en un término de 10 (diez) días naturales persiste el atraso, el INSTITUTO FONACOT podrá rescindir administrativamente el contrato y, en su caso, hará efectiva la fianza para el cumplimiento del contrato.

Para el pago de las penas convencionales, el INSTITUTO FONACOT a través del Administrador del Contrato informará por escrito al PRESTADOR el cálculo de la pena correspondiente, indicando el número de días de atraso, así como la base para su cálculo y el monto de la pena a que se hizo acreedor, debiendo el PRESTADOR realizar el pago correspondiente, a través de referencia bancaria que se genera el mismo día en el que efectuará el pago, la cual será proporcionada en la




Dirección de Recursos Materiales y Servicios Generales o bien contar con la autorización del PRESTADOR a fin de que se efectúe el descuento directo a su factura.

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. En el supuesto de que el cálculo de la penalización contenga centavos, el monto se ajustará a pesos, de tal suerte que las que contengan cantidades que incluyan de 1 hasta 50 centavos, el importe de la penalización se ajustará a pesos a la unidad inmediata inferior y las que contengan de 51 a 99 centavos, el importe de la penalización se ajustará a pesos a la unidad inmediata superior.

Ambas partes acuerdan, que aquellas obligaciones que no tengan establecido en el contrato plazo determinado de cumplimiento, no serán objeto de penalización alguna, pero su incumplimiento parcial o deficiente dará lugar a que el INSTITUTO FONACOT deduzca su costo del importe correspondiente.

**VIGÉSIMA SÉPTIMA. DEDUCTIVAS.** El INSTITUTO FONACOT aplicará al PRESTADOR deductivas por concepto de deducción al pago de los servicios con motivo del incumplimiento parcial o deficiente en que incurra el PRESTADOR, respecto a las partidas o conceptos que integran el presente contrato, de conformidad en el artículo 53 BIS de la Ley de Adquisiciones, Arrendamiento y Servicios del Sector Público y 97 de su Reglamento, considerando los siguientes casos:

DEDUCTIVAS		
No.	Descripción	Monto
1	Incumplimiento parcial o entrega mal realizada o incompleta en los <u>niveles de servicio</u> establecidos en el numeral 28. NIVELES DE SERVICIO (SLA's), del Anexo Técnico "Características Técnicas del Servicio",	3% del monto total mensual del mes en cuestión, por incumplimiento parcial o entrega mal realizada o incompleta a los <u>niveles de servicio</u> .
2	Incumplimiento en la <u>entrega total</u> de cada uno de los servicios, ya sea por mala realización o entrega incompleta, de cualquiera de los servicios plasmados en el numeral 4. DESCRIPCIÓN GENERAL DEL SERVICIO del Anexo Técnico "Características Técnicas del Servicio",	3% del monto total mensual del mes en cuestión, por incumplimiento en la <u>entrega total</u> 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 parcial o entrega mal realizada o incompleta en los tiempos establecidos en la <u>implementación</u> de los servicios establecidos en el 4. DESCRIPCIÓN GENERAL DEL SERVICIO del Anexo Técnico "Características Técnicas del Servicio".	3% del monto total mensual del mes en cuestión, por día natural por incumplimiento parcial o entrega mal realizada o incompleta en la <u>implementación</u> de cada uno de los servicios.
4	Incumplimiento en el tiempo de asignación o reemplazo de los recursos humanos, establecidos en el numeral 15. ADMINISTRACIÓN DE LOS SERVICIOS del Anexo Técnico "Características Técnicas del Servicio.	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.
5	Incumplimiento parcial o entrega mal realizada o incompleta por cada uno de los entregables mensuales, establecidos en el numeral 15. ADMINISTRACIÓN DE LOS SERVICIOS del Anexo Técnico "Características Técnicas del Servicio".	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.

El límite de incumplimiento por la aplicación de deductivas, a partir del cual se podrá proceder a rescindir el contrato será del 10% (diez por ciento) del importe total del contrato, sin incluir el Impuesto al Valor Agregado, que corresponde al importe de la garantía de cumplimiento.





**VIGÉSIMA OCTAVA. SANCIONES.** Se hará efectiva la garantía relativa al cumplimiento del contrato, cuando el PRESTADOR incumpla a cualquiera de sus obligaciones contractuales por causas a él imputables; teniendo el INSTITUTO FONACOT facultad potestativa para rescindir el presente contrato.

La aplicación de la garantía de cumplimiento será proporcional al monto de las obligaciones incumplidas.

Independientemente de lo anterior, cuando el PRESTADOR incumpla con sus obligaciones contractuales por causas imputables a él, y como consecuencia, cause daños y/o perjuicios graves al INSTITUTO FONACOT, o bien, proporcione información falsa, actúe con dolo o mala fe en la celebración del contrato o durante la vigencia del mismo, se hará acreedor a las sanciones establecidas en los artículos 59 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

**VIGÉSIMA NOVENA. PAGOS EN EXCESO.** De conformidad con lo previsto en el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público tratándose de pagos en exceso que haya recibido el PRESTADOR, éste deberá reintegrar las cantidades pagadas en exceso, más los intereses correspondientes, conforme a la tasa de recargo 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 intereses 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.

**TRIGÉSIMA. CAUSAS DE RESCISIÓN ADMINISTRATIVA.** Serán causas de rescisión del presente contrato, sin responsabilidad para EL INSTITUTO FONACOT, si el PRESTADOR:

- A) No inicia la prestación de los servicios objeto de este contrato en la fecha pactada.
- B) No ejecuta los servicios de conformidad a lo establecido en el presente contrato, o sin motivo justificado no acata las indicaciones del INSTITUTO FONACOT.
- C) Suspende injustificadamente los servicios materia del presente contrato.
- D) Por cualquier causa deja de tener capacidad técnica y los elementos necesarios para proporcionar el servicio.
- E) En el caso de sustitución de personal, si éste tiene un nivel inferior al propuesto inicialmente.
- F) Cede en forma parcial o total a terceras personas los derechos u obligaciones derivados del presente contrato.
- G) No da al INSTITUTO FONACOT las facilidades y datos necesarios para la supervisión y verificación de los servicios contratados.
- H) Se declara en quiebra o suspensión de pagos o le sobreviene una huelga o por cualquier causa análoga.
- I) Cuando el importe que se haya deducido, sea igual o superior al 10% (diez por ciento) del monto total del contrato sin incluir el Impuesto al Valor Agregado, y
- J) En general, por cualquier incumplimiento a las obligaciones pactadas en el presente contrato.





**TRIGÉSIMA PRIMERA. PROCEDIMIENTO DE RESCISIÓN ADMINISTRATIVA.** El incumplimiento del PRESTADOR a cualquiera de sus obligaciones pactadas en el presente contrato, lo hará rescindible en cualquier momento y sin necesidad de juicio o declaración judicial previa, para lo cual el INSTITUTO FONACOT deberá motivar la rescisión en alguna de las causales previstas para tal efecto. Si es el PRESTADOR quien decide rescindir el contrato será necesario que acuda ante la autoridad judicial federal y obtenga la declaración correspondiente; lo anterior, con fundamento en lo previsto en los artículos 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 98 y 99 de su Reglamento, bajo el siguiente procedimiento:

1. Se iniciará a partir de que al PRESTADOR le sea comunicado por escrito el incumplimiento en que haya incurrido, para que en un término de 5 (cinco) días hábiles exponga lo que a su derecho convenga y aporte, en su caso, las pruebas que estime pertinentes;
2. Transcurrido el término a que se refiere el punto anterior, se resolverá considerando los argumentos y pruebas que hubiere hecho valer;
3. La determinación de dar o no por rescindido el contrato deberá estar debidamente fundada, motivada y comunicada al PRESTADOR dentro de los 15 (quince) días naturales siguientes a lo señalado en el punto 1, y
4. 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 de los servicios recibidos hasta el momento de la rescisión. Si previamente a la determinación de dar por rescindido el contrato, se hiciera prestación de los servicios, el procedimiento iniciado quedará sin efecto, previa aceptación y verificación del INSTITUTO FONACOT de que continúa vigente la necesidad de los mismos, 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 contrato 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 Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En el supuesto del cuarto párrafo del artículo 54 de la Ley mencionada, 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.

**TRIGÉSIMA SEGUNDA. TERMINACIÓN ANTICIPADA.** El INSTITUTO FONACOT podrá dar por terminado anticipadamente el contrato mediante comunicación por escrito con 5 (cinco) días hábiles de antelación al PRESTADOR, cuando por convenir a los intereses del INSTITUTO FONACOT así lo determine; cuando concurren 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 al INSTITUTO FONACOT, quedando únicamente obligado el INSTITUTO FONACOT a reembolsar al PRESTADOR los gastos no recuperables en que haya incurrido,



siempre que éstos sean razonables, estén comprobados y se relacionen directamente con el contrato correspondiente.

El PRESTADOR podrá solicitar al INSTITUTO FONACOT, el pago de gastos no recuperables en un plazo máximo de un mes, contado a partir de la fecha de la terminación anticipada del contrato o de la suspensión del servicio, según corresponda.

Si los gastos no recuperables son por los supuestos a que se refieren los artículos 101 y 102 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, serán pagados dentro de un término que no podrá exceder de cuarenta y cinco días naturales posteriores a la solicitud fundada y documentada del PRESTADOR.

Todo lo anterior, de conformidad con lo establecido en los artículos 54 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 102 de su Reglamento.

**TRIGÉSIMA TERCERA. TRANSPARENCIA Y ACCESO A LA INFORMACIÓN.** Las partes acuerdan de forma expresa que la información que se maneje con motivo de la celebración del presente contrato, se sujetará a lo establecido por la legislación aplicable a cada una de las partes en materia de transparencia y acceso a la información pública.

Las partes acuerdan que en virtud del presente contrato podrán recibir de la otra parte información técnica, jurídica y financiera de carácter confidencial y reservada en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ley General de Transparencia y Acceso a la Información Pública, Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados y de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que para efectos del presente contrato se denominará "Información Confidencial", la cual podrá ser recibida de manera enunciativa mas no limitativa en forma oral, escrita, visual, en formatos escritos, electrónicos, ópticos, magnéticos y por cualquier otro medio conocido o por conocerse.

Asimismo, las partes reconocen que dicha "Información Confidencial" podría constituir un secreto industrial, en términos del artículo 82 de la Ley de la Propiedad Industrial.

Las partes se obligan a mantener con toda la reserva que sea necesaria la confidencialidad de la "Información Confidencial" que reciban de la otra Parte a partir de la fecha de firma de este contrato o con anterioridad a la misma y a no enajenarla, arrendarla, prestarla, grabarla, negociarla, revelarla, publicarla, enseñarla, darla a conocer, transmitirla o de alguna otra forma divulgarla o proporcionarla, total o parcialmente a cualquier persona física o moral, nacional o extranjera, pública o privada, por cualquier medio conocido o por conocerse, aun cuando se trate de incluirla o entregarla en otros documentos como estudios, reportes, propuestas u ofertas, en todo o en parte.

Las partes se obligan a hacer extensiva la obligación de confidencialidad con sus directivos, funcionarios, empleados, trabajadores, agentes, contratistas independientes, representantes, asesores o cualquier otra persona con ellas vinculadas y que tengan acceso a la citada información, y quienes deberán obligarse a mantener de manera confidencial la misma, con excepción de sus empresas filiales o entidades coordinadoras.

Las partes se obligan a utilizar la "Información Confidencial" que mutuamente se proporcionen única y exclusivamente para dar cumplimiento al objeto del presente Contrato, obligándose a no utilizarla en su provecho o en provecho de terceros por ningún medio.



Las obligaciones de confidencialidad previstas en esta cláusula serán aplicables a toda información que reciban Las partes entre sí, con excepción de que en la misma se indique lo contrario, o:

- a) Que la información sea de dominio público al momento en que sea revelada o se vuelva del dominio público a través de un medio que no implique incumplimiento de las partes a las obligaciones contenidas en el presente Contrato;
- b) Que la información se encontrará legalmente en posesión de una de las partes, con anterioridad a la fecha en la que fue recibida por la otra sin ninguna obligación de confidencialidad.
- c) Que la información fuera recibida en forma independiente de un tercero que podía revelarla legalmente a las partes o,
- d) Que la revelación de la información fuera requerida por una orden judicial o de cualquier otra autoridad gubernamental, o disposición legal, siempre y cuando la Parte requerida notifique en forma inmediata y por escrito a la otra, a fin de que ésta tenga oportunidad de impugnar legalmente la orden de que se trate.

Las partes reconocen que la "Información Confidencial" que se proporcionen entre sí, seguirá siendo propiedad de aquella que la haya proporcionado, por lo que cualquiera de ellas podrá solicitar a la otra la destrucción o devolución inmediata de la "Información Confidencial" proporcionada durante o con posteridad a la vigencia del presente Contrato.

Las partes acuerdan que las obligaciones de confidencialidad de la presente cláusula estarán vigentes durante y con posteridad de la vigencia de este Contrato, en el entendido de que dicha limitación no operará respecto a la capacidad, experiencia y desarrollo que su personal haya adquirido derivado del presente Contrato.

**TRIGÉSIMA CUARTA. DERECHOS DE AUTOR, PATENTES Y/O MARCAS.** El PRESTADOR se obliga con el INSTITUTO FONACOT, a responder personal e ilimitadamente de los daños y perjuicios que pudiera causar al INSTITUTO FONACOT o a terceros, si con motivo de la prestación de los servicios contratados viola derechos de autor, patentes y/o marcas registradas, de terceros u otro derecho intelectual reservado. 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 y en la Ley de la Propiedad Industrial.

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

Además, los derechos de autor o en su caso de propiedad industrial que lleguen a generarse por los productos que se deriven de dicha actividad, serán propiedad exclusiva del INSTITUTO FONACOT, en términos de lo dispuesto por el artículo 45, fracción XX de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

**TRIGÉSIMA QUINTA. CASO FORTUITO O FUERZA MAYOR.** Ninguna de las partes será responsable por cualquier retraso o incumplimiento de este contrato que resulte de caso fortuito,





fuerza mayor o por causas atribuibles al INSTITUTO FONACOT, en la inteligencia de que, una vez superados los dos primeros eventos, se reanudará la prestación de los servicios objeto del presente contrato, si así lo manifiesta el INSTITUTO FONACOT.

Para los supuestos de caso fortuito o fuerza mayor, el PRESTADOR deberá notificar y acreditar dicha situación el INSTITUTO FONACOT previo al vencimiento de las fechas de cumplimiento estipuladas originalmente; igual procedimiento llevará a cabo el INSTITUTO FONACOT, para el caso de que, por causas atribuibles a éste, no se cumpla con el servicio en las fechas pactadas, procediéndose a modificar el presente contrato a efecto de diferir la fecha para la prestación de los servicios. En este supuesto deberá formalizarse el convenio modificatorio respectivo, no procediendo la aplicación de penas convencionales por atraso, lo anterior de conformidad con lo previsto en el artículo 55 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 91 de su Reglamento.

Se entiende por caso fortuito o fuerza mayor, cualquier acontecimiento imprevisible e insuperable que impida a las partes afectadas el cumplimiento de sus obligaciones bajo este contrato, si dicho evento se encuentra más allá del control razonable de dicha parte, y no es resultado de su falta o negligencia, y si dicha parte no ha sido capaz de superar dicho acontecimiento mediante el ejercicio de la debida diligencia. Sujeto a la satisfacción de las condiciones precedentes, el caso fortuito o fuerza mayor incluirá, en forma enunciativa y no limitativa:

- A) Fenómenos de la naturaleza, tales como tormentas, inundaciones y terremotos;
- B) Incendios;
- C) Guerras, disturbios civiles, motines, insurrecciones y sabotaje;
- D) Huelgas u otras disputas laborales en México, y
- E) Leyes de aplicación general de cualquier autoridad gubernamental.

Queda expresamente convenido que caso fortuito o fuerza mayor no incluirá ninguno de los siguientes eventos:

- i) Incumplimiento de cualquier obligación contractual de las partes para la realización de los servicios, excepto y en la medida en que dicho retraso en la entrega sea causado por un caso fortuito o fuerza mayor; o
- ii) Cualquier acto u omisión derivados de la falta de previsión por parte de EL PRESTADOR.

**TRIGÉSIMA SEXTA. SUSPENSIÓN DE LA PRESTACIÓN DEL SERVICIO.** Cuando durante la vigencia del contrato sobrevinieran causas de fuerza mayor o de caso fortuito el INSTITUTO FONACOT, podrá suspender la prestación del servicio, en cuyo caso únicamente se pagarán aquellos servicios efectivamente devengados.

Cuando dicha suspensión obedezca a causas imputables al INSTITUTO FONACOT, el PRESTADOR tendrá derecho al pago de los gastos no recuperables durante el tiempo en que dure esta suspensión.

En cualquiera de los casos anteriores, el plazo que no podrá ser mayor a 10 (diez) días hábiles, a cuyo término podrá iniciarse la terminación anticipada de este contrato, previa solicitud del Administrador del mismo.

**TRIGÉSIMA SÉPTIMA. PRÓRROGAS Y/O DIFERIMIENTOS.** La fecha de inicio o de terminación total de los servicios, podrán ser prorrogadas en los siguientes casos:

- A) Por caso fortuito o fuerza mayor, en este supuesto será necesario que el PRESTADOR notifique el evento al Administrador del Contrato, y solicite por escrito la prórroga ante el INSTITUTO FONACOT inmediatamente al vencimiento de la fecha que corresponda, acompañando las pruebas que permitan corroborar que dicho evento actualiza los supuestos de caso fortuito o fuerza mayor.
- B) Si el servidor público designado como Administrador del Contrato por el INSTITUTO FONACOT ordena al PRESTADOR la suspensión de la totalidad o parte de los servicios.
- C) Si los servicios no pueden ser realizados o son retrasados debido a cualquier acto u omisión del INSTITUTO FONACOT. En este supuesto, será necesario que el PRESTADOR notifique el evento al Administrador del Contrato, solicite por escrito la prórroga ante el INSTITUTO FONACOT, inmediatamente al vencimiento de la fecha que corresponda, acompañando las pruebas que permitan acreditar que el evento es imputable al INSTITUTO FONACOT.

En los supuestos establecidos en los incisos A) y C), el Administrador del Contrato analizará la solicitud, así como los razonamientos y documentación comprobatoria que presente el PRESTADOR, notificándole por escrito si se concede o no la prórroga, en un plazo no mayor de 5 (cinco) días naturales, contados a partir de la fecha de recepción de la solicitud del PRESTADOR, la prórroga será formalizada mediante la celebración de un convenio entre las partes.

**TRIGÉSIMA OCTAVA. ADMINISTRACIÓN DEL CONTRATO.** De conformidad con lo previsto en el artículo 84 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el Lic. Javier Jiménez Jiménez, Subdirector General de Tecnología de la Información y Comunicación, será el encargado de administrar, verificar, vigilar y supervisar el cumplimiento del presente contrato.

**TRIGÉSIMA NOVENA. DISCREPANCIA.** El PRESTADOR acepta que, en caso de discrepancia entre la convocatoria del proceso de contratación o la solicitud de cotización y el modelo de contrato, de los cuales deriva el presente instrumento, prevalecerá lo establecido en la convocatoria, invitación o solicitud respectiva.

**CUADRAGESIMA. PROCEDIMIENTO PARA LA RESOLUCIÓN DE CONTROVERSIAS DISTINTOS AL PROCEDIMIENTO DE CONCILIACIÓN PREVISTO EN LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO.** En principio, la solución de las controversias que pudieran surgir entre el PRESTADOR y el INSTITUTO FONACOT se resolverán siguiendo las disposiciones contenidas en el Título Sexto de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, según lo establece el artículo 15 de la ley mencionada.

**CUADRAGESIMA PRIMERA. PROCEDIMIENTO PARA LA CONCILIACIÓN.** El PRESTADOR y el INSTITUTO FONACOT, con fundamento en el artículo 77 de la citada ley, podrán en cualquier momento, presentar ante la Secretaría de la Función Pública la solicitud de conciliación, en caso de que hubiere desavenencias derivadas del cumplimiento del presente contrato, conforme al procedimiento establecido en los artículos 77, 78 y 79 de la referida ley.

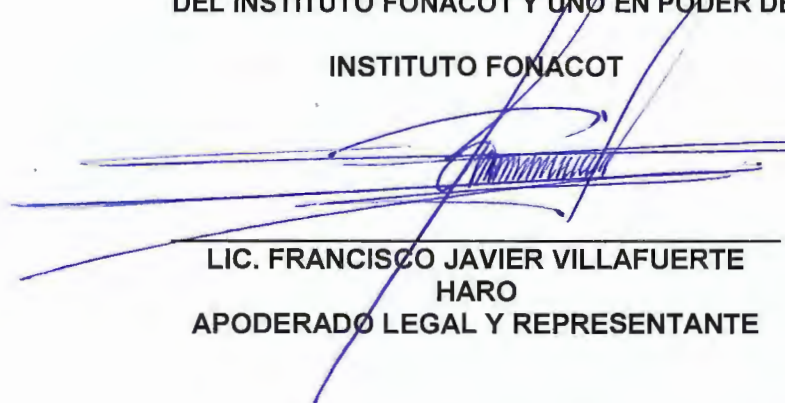
En caso de no someterse a la conciliación mencionada, ambas partes, de común acuerdo podrán someterse a un compromiso arbitral, de conformidad con lo señalado en los artículos 80, 81 y demás relativos y aplicables de dicha ley, 137 de su Reglamento, o en su defecto podrán acudir a los tribunales federales si así lo decidieran.

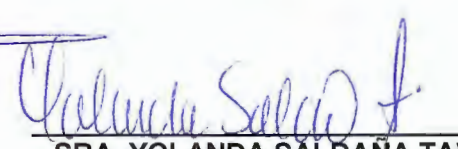
**CUADRAGESIMA SEGUNDA. JURISDICCIÓN Y LEGISLACIÓN APLICABLE.** Para los efectos de interpretación y cumplimiento del presente contrato, las partes se someten a las leyes, particularmente a la de Adquisiciones, Arrendamientos y Servicios del Sector Público, a la Federal de Presupuesto y Responsabilidad Hacendaria y sus respectivos Reglamentos, al Código Civil Federal, Ley Federal de Procedimiento Administrativo; Código Federal de Procedimientos Civiles; así como todas aquellas que por el carácter de entidad paraestatal del INSTITUTO FONACOT resulten aplicables, así como a la jurisdicción de los tribunales competentes de la Ciudad de México, por lo que renuncian al fuero que por razón de sus domicilios presentes y futuros les correspondan o les llegaren a corresponder.

**LEIDO EL PRESENTE CONTRATO POR LAS PARTES QUE EN EL INTERVIENEN, LO RATIFICAN Y LO FIRMAN POR TRIPLICADO, EXPRESANDO SU CONFORMIDAD EN LA CIUDAD DE MÉXICO, EL DÍA 11 DE JULIO DE 2018, POR TRIPLICADO, QUEDANDO DOS EJEMPLARES EN PODER DEL INSTITUTO FONACOT Y UNO EN PODER DEL PRESTADOR.**

**INSTITUTO FONACOT**

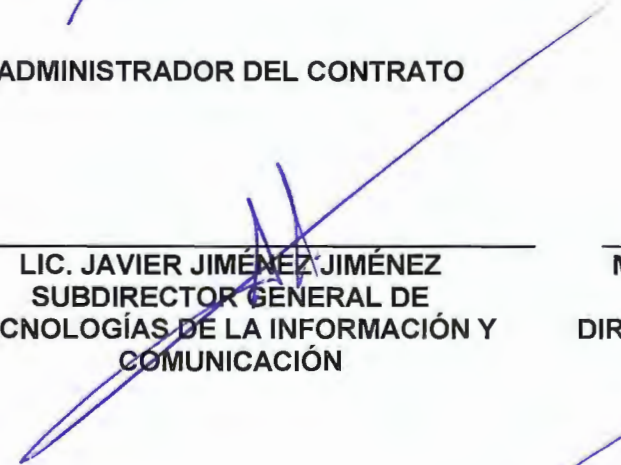
**EL PRESTADOR**

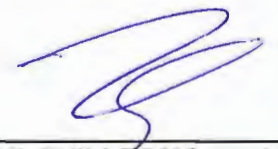
  
\_\_\_\_\_  
**LIC. FRANCISCO JAVIER VILLAFUERTE HARO**  
**APODERADO LEGAL Y REPRESENTANTE**

  
\_\_\_\_\_  
**SRA. YOLANDA SALDAÑA TAVERA**  
**APODERADA LEGAL**

**ADMINISTRADOR DEL CONTRATO**

**ÁREA CONTRATANTE**

  
\_\_\_\_\_  
**LIC. JAVIER JIMÉNEZ JIMÉNEZ**  
**SUBDIRECTOR GENERAL DE**  
**TECNOLOGÍAS DE LA INFORMACIÓN Y**  
**COMUNICACIÓN**

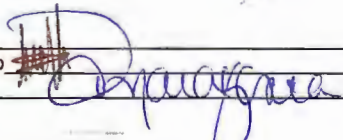
  
\_\_\_\_\_  
**MTRO. EDGAR GUILLERMO URBANO**  
**AGUILAR**  
**DIRECTOR DE RECURSOS MATERIALES Y**  
**SERVICIOS GENERALES**

Contrato No. I-SD-2018-114

Visto Bueno del Área Contratante

Elaboró: Lic. Leticia Velis Delgadillo

Supervisó: Lic. Dora Nava García

  
\_\_\_\_\_  
\_\_\_\_\_



# ANEXO I ANEXO TÉCNICO

El presente Anexo consta de 267 páginas, el cual una vez rubricado por las partes, formará parte integrante del Contrato I-SD-2018-114.

Visto Bueno del Área Requirente \_\_\_\_\_



LICITACION PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS  
No. LA-014P7R001-E349-2018  
RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración  
y control de la seguridad de las tecnologías de la información y comunicaciones",



84

# INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES

Convocatoria

Licitación Pública Nacional NO. LA-014P7R001-E349-2018

**"CONTRATACIÓN PLURIANUAL DEL SERVICIO INTEGRAL DE FORTALECIMIENTO EN LA GESTIÓN, ADMINISTRACIÓN Y CONTROL DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES".**



Anexo 13

PROPUESTA TÉCNICA

"CARACTERÍSTICAS TÉCNICAS DEL SERVICIO"

78



## 1. Información General

### 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 el año pasado, al área de la Subdirección General de Tecnologías de la Información y Comunicación (SGTIC) con respecto al "Assessment de Seguridad de la Información", se identificaron hallazgos sobre este rubro que deben de gestionarse y fortalecerse de manera inmediata, robusta y recurrente, dado que la seguridad es un estado de tiempo.

Estos hallazgos resultantes del Assessment antes mencionado, deberán de ejercérselos la remediación correspondiente para evitar riesgos asociados a fraudes, fugas o robo de información, gestión inadecuada de accesos, protección contra software malicioso, uso inadecuado de dispositivos de almacenamiento de datos y explotación de vulnerabilidades, además de asegurar las propiedades de integridad, confidencialidad y disponibilidad de la información.

### 1.2 Objeto del Servicio

**IQsec, S.A. de C.V.** proveerá al El Instituto FONACOT un "**Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones**", que le permitiera al Instituto la correcta remediación, control y mitigación de riesgos, y amenazas detectadas por el realizado "Assessment de Seguridad de la Información" mencionado anteriormente, 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.

La contratación del "**Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las**





**Tecnologías de la Información y Comunicaciones"**, permitirá que el Instituto FONACOT dé cumplimiento a las normas, regulaciones y estándares que permitan la correcta y segura operación del Instituto 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 y procesos adyacentes a este.

Las acciones antes referidas se realizarán con un enfoque de servicio integral en el rubro de la seguridad de la información que interactúa con el Instituto de manera interna y externa para estar en condiciones de garantizar el adecuado manejo, resguardo y tratamiento de la información que transita a través de la infraestructura y aplicaciones informáticas institucionales.

Como parte del servicio integral IQsec, S.A. de C.V. implementará un mecanismo de sensibilización que permita el desarrollo de la cultura de fortalecimiento de la seguridad de la información en todos y cada uno de los elementos de las tecnologías de la información y comunicaciones, así como en el personal que intervienen en la operación y servicios que proporciona el Instituto FONACOT día a día a la Sociedad Mexicana.

## 2. Alcance del Servicio

El alcance del "**Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones**", requerido por el Instituto FONACOT asegurará la implementación de servicios que permitan la eficaz y eficiente gestión, administración, control, y mitigación de los hallazgos consecuencia del Assessment de seguridad de la información del Instituto FONACOT y cumplir con las normas, regulaciones y estándares aplicables durante el uso, operación, funcionalidad e interoperabilidad de las operaciones que proporciona el Instituto FONACOT día a día como apoyo en los procesos y operación sustantiva tales como: proceso de originación de créditos, recuperación de cartera, bursatilización, por mencionar algunos.

Para asegurar la adecuada administración, control y mitigación de los hallazgos, consecuencia del Assessment anteriormente mencionado, **IQsec, S.A. de C.V.** implementará, en el Instituto FONACOT, los servicios enunciados en el **Numeral 4. Descripción General del Servicio.**





Las soluciones tecnológicas necesarias para la prestación del servicio por parte de IQsec, S.A. de C.V. para el Instituto FONACOT serán instaladas en la infraestructura tecnológica del Instituto FONACOT, tomando en cuenta que el Instituto FONACOT únicamente facilitará el espacio físico, las condiciones ambientales y energía eléctrica que se requieran para las mismas. **IQsec, S.A. de C.V.** considerará la infraestructura tecnológica necesaria como racks, cableado de red, etcétera., para la instalación y puesta en marcha en las instalaciones del Instituto FONACOT.

**IQsec, S.A. de C.V.**, contemplará un enlace de comunicación vía VPN o LAN to LAN para el control y seguimiento de las soluciones tecnológicas implementadas dentro del Instituto FONACOT.

### 3. Justificación

El Instituto FONACOT requiere de la contratación del **"Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones"**, que permita robustecer, y en su caso, reforzar la seguridad informática de la infraestructura tecnológica, fortalecer sus procesos y procedimientos conforme a las normas, regulaciones y las mejores prácticas de seguridad de la información, asimismo, el servicio deberá considerar los mecanismos de sensibilización del personal respecto a la cultura de seguridad informática.

El Instituto FONACOT debe asegurar la correcta mitigación y control de los hallazgos, detectados con base en el Assessment de seguridad de la información, a través de la implementación del **"Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones"**.

El **"Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones"**, tiene como uno de sus objetivos asegurar las propiedades de integridad, confidencialidad y disponibilidad de los activos inherentes al presente en cuanto a los términos de seguridad en la infraestructura de las tecnologías de la información y comunicaciones.

El Instituto FONACOT mediante el **"Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones"**, y los servicios que integran el mismo evitará tener riesgos asociados a

LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



fraudes, fugas o robo de información, gestión inadecuada de accesos, protección contra software malicioso, uso inadecuado de dispositivos de almacenamiento de datos y explotación de vulnerabilidades que pudieran haber sido detectados como parte de los hallazgos del servicio proporcionado a través del "Assessment de Seguridad de la Información".

Patriotismo 399, San Pedro de los Pinos, 03800, CDMX.  
RFC: IQsec, S.A. De C.V. / IQS0708233C9

000005

+





#### 4. 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, integrará una serie de servicios que se llevarán a cabo para asegurar la correcta mitigación y control de los hallazgos resultado del servicio de Assessment de seguridad de la información que se llevó a cabo en el instituto FONACOT, así como los posibles eventos que pudiesen presentarse durante la vigencia del servicio y 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 protección y reputación de identidad institucional.
7. Servicio de sensibilización de tecnologías de la información.
8. Servicio de administración del SGSI.
9. Servicio de protección de estaciones de trabajo.

**IQsec, S.A. de C.V.** cuenta 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.

#### 5. Servicios de Gestión, Seguimiento y Control de Incidentes



## 5.1 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.

IQsec, S.A. de C.V., proporcionará 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. IQsec, S.A. de C.V., llevará 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.

IQsec, S.A. de C.V., integrará un análisis de comportamiento de usuario contemplando al menos 1800 usuarios para este servicio, 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.

IQsec, S.A. de C.V., implementará 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.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 16 de la empresa "IQSEC S.A. DE C.V." de la página 7 de 36 que a la letra dice:

Se le solicita amablemente a la convocante nos ayude a confirmar el número de usuarios a contemplar para llevar a cabo el análisis de comportamiento.

**Respuesta de la Covocante: "Se deberán contemplar al menos 1800 usuarios para el análisis de comportamiento."**





## 5.2 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.

**IQsec, S.A. de C.V.** cuenta 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 dispone de las siguientes características:

- Centro de datos:
  - Sistema de video vigilancia.
  - Sistema de control de acceso físico es 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 monitoreo ambiental. (humedad, condiciones anómalas de accesos y electricidad, temperatura).
  - Área de operación:
    - Esta separada de la red de **IQsec, S.A. de C.V.**
    - Es de acceso exclusivo para el personal que realiza el servicio.
    - Aloja únicamente al personal que realiza el servicio.
    - El control de acceso es a través de controles biométricos o automatizados.
  - Infraestructura del área de operación:
    - IQsec, S.A. de C.V. Cuenta con una Consola de monitoreo para visualizar los eventos o incidentes inherentes a los servicios ofertados.
    - IQsec, S.A. de C.V. Usa Herramientas de monitoreo en tiempo real de la disponibilidad de los equipos para los servicios inherentes ofertados.



- o Sistema de administración de tickets para la atención de solicitudes.
- o Tableros de control con pantallas dedicadas para el monitoreo de los servicios inherentes ofertados.
- o IQsec, S.A. de C.V. Utiliza un Sistema de administración de tickets para la atención de solicitudes.
- o IQsec, S.A. de C.V. Emplea Tableros de control con pantallas dedicadas para el monitoreo de los servicios inherentes ofertados.

**Referirse al documento:**

Sistema de monitoreo.pdf

Accesos Biométricos.pdf

Separación de red (lógica).pdf

Cableado Estructurado.pdf

Aire acondicionado.pdf

Detectores de incendios.pdf

UPS y plantas de emergencia.pdf

Datasheet Synology.pdf

Propuesta Mesa de Ayuda.pdf





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

Los servicios de gestión, seguimiento y control de incidentes que **IQsec, S.A. de C.V.** proveerá, se realizará de manera remota y efectuarán 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).

que operen bajo condiciones normales (CPU, memoria, disco duro, los cuales se mencionan de manera enunciativa más no limitativa).

**Referirse al documento:**

Propuesta Mesa de Ayuda\_pag 6.pdf

Propuesta Mesa de Ayuda\_pag 8-12.pdf

**Referirse a la pagina:**

<http://cert.iqsec.com.mx/es/#&panel1-1>

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

**IQsec, S.A. de C.V.** considerará a 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 IQsec, S.A. de C.V. y el 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.

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 es capaz de recibir y analizar reportes de amenazas, incidentes y alertas de vulnerabilidades. El análisis incluye acciones específicas para aplicarse en el entorno de TI.
- El personal analiza e identifica eventos anómalos que son detectados por las soluciones administradas, integra 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 recibe y analiza noticias relacionadas con la seguridad de la información. Así mismo, cuenta 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.
- Indicadores sobre la actividad de amenaza cibernéticas y mitigaciones recomendadas.
- El personal de seguridad de la información utiliza 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 entregará 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 realiza la actualización y el respaldo periódico de las configuraciones de los componentes que integran la solución del servicio propuesto.
- El personal tiene el 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 cumple con experiencia, competencias, habilidades, cursos y/o certificaciones, los cuales se incluyen en la propuesta técnica y están vigentes.





- El personal deberá cumplir con experiencia, competencias, habilidades, cursos y/o certificaciones, los cuales deberán incluirse en la propuesta técnica y estar vigentes.

**Referirse al documento:**

Metodología\_CCS\_pag 8.pdf

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 reemplazar el hardware y software por fallas, ineficiencia, obsolescencia y/o crecimiento de las soluciones.

El servicio que **IQsec, S.A. de C.V.** proveerá, considerará la actualización periódica de la totalidad de los componentes de seguridad administrados, y realizará la migración a nuevas versiones de software. En caso de presentarse alguna falla o inestabilidad en los equipos, **IQsec, S.A. de C.V.** reparará o sustituirá el componente dañado. También será responsable de reemplazar el hardware y software por fallas, ineficiencia, obsolescencia y/o crecimiento de las soluciones.

**Referirse al documento:**

Propuesta Mesa de Ayuda\_pag 4.pdf

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

El servicio que **IQsec, S.A. de C.V.** proveerá, contemplará un grupo resolutor, el cuál recibirá los requerimientos técnicos, incidentes operativos o de seguridad del instituto para cada incidente o requerimiento en particular, dicho grupo resolutor estará disponible en un formato de 7 días por 24 horas los 365 días del año.

**Referirse al documento:**



Metodología\_CCS\_pag 15.pdf

Propuesta Mesa de Ayuda\_pag 6.pdf

Propuesta Mesa de Ayuda\_pag 8-12.pdf

**Referirse a la pagina:**

<http://cert.iqsec.com.mx/es/#&panel1-1>

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

**IQsec, S.A. de C.V.** priorizará la atención de solicitudes e incidentes con 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

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

**Referirse al documento:**

Propuesta Mesa de Ayuda\_pag 9-11.pdf





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.

El servicio propuesto por **IQsec, S.A. de C.V.** considera 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.

**Referirse al documento:**

Metodología\_CCS\_pag 6.pdf

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.

El servicio que **IQsec, S.A. de C.V.** proveerá, incluye 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 de **IQsec, S.A. de C.V.**

**Referirse al documento:**

Certificado\_ISO27001.PDF

Metodología\_CCS\_pag 9.pdf

### 5.3 Descripción de Componentes

5.3.1 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.

El servicio propuesto por **IQsec, S.A. de C.V.** de gestión, seguimiento y control de incidentes, brindará el servicio de correlación de eventos y análisis de comportamiento que pueda soportar la cantidad de 5000 mensajes por segundo y considerará la capacidad de almacenamiento de hasta 3 meses en línea para la consulta de información. Considerando además el almacenamiento fuera de línea de toda la información colectada durante la vigencia del contrato.

**Referirse al documento:**

high-performance-appliances-data-sheet\_pag 2.pdf

5.3.2 La solución deberá permitir la expansión de memoria hasta 128GB.

La solución propuesta por **IQsec, S.A. de C.V.**, permitirá la expansión de memoria hasta 128GB.

**Referirse al documento:**

high-performance-appliances-data-sheet\_pag 2.pdf







5.3.3 La solución deberá contener al menos 10 TB de almacenamiento interno.

La solución propuesta por **IQsec, S.A. de C.V.**, contendrá al menos 10 TB de almacenamiento interno.

**Referirse al documento:**

high-performance-appliances-data-sheet\_pag 2.pdf

5.3.4 La solución deberá permitir compresión 20:01.

La solución propuesta por **IQsec, S.A. de C.V.**, permitirá compresión 20:01.

**Referirse al documento:**

high-performance-appliances-data-sheet\_pag 2.pdf

5.3.3 La solución deberá contener 12 / 24 CPU's físicos o virtuales.

La solución propuesta por **IQsec, S.A. de C.V.** contendrá 12 / 24 CPU's (Cores) físicos o virtuales.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 13 de la empresa "IQSEC S.A. DE C.V." de la página 14 de 36 que a la letra dice:

*"Se le solicita amablemente a la convocante nos pueda ayudar a especificar si el numeral mencionado en la pregunta hace referencia al número de cores?"*



**Respuesta de la Convocante: Es correcta su apreciación, el numeral hace referencia al numero de cores ya sean virtuales o físicos.**

**Referirse al documento:**

high-performance-appliances-data-sheet\_pag 2.pdf

5.3.4 La solución deberá soportar AC Broadcom 5720 QP (4 x 1Gb) (Ethernet).

La solución propuesta por **IQsec, S.A. de C.V.** soportará AC Broadcom 5720 QP (4 x 1Gb) (Ethernet).

**Referirse al documento:**

high-performance-appliances-data-sheet\_pag 2.pdf

5.3.5 La solución deberá soportar al menos 25,000 MPS de capacidad máxima de archivos (Max Archiving Rates).

La solución propuesta por **IQsec, S.A. de C.V.** soportará al menos 25,000 MPS de capacidad máxima de archivos (Max Archiving Rates).

**Referirse al documento:**

high-performance-appliances-data-sheet\_pag 2.pdf

5.3.6 La solución deberá incluir componentes adicionales para aumentar la tolerancia a errores, la capacidad y el rendimiento.

La solución propuesta por **IQsec, S.A. de C.V.** incluirá componentes adicionales para aumentar la tolerancia a errores, la capacidad y el rendimiento.





**Referirse al documento:**

dell-poweredge-r730-spec-sheet\_pag 2.pdf

5.3.7 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.

La solución propuesta por IQsec, S.A. de C.V. contará 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.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 6.pdf

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 5.pdf

5.3.8 La solución deberá contar por cada unidad con fuentes de poder redundantes internas y alimentadas ya sea con 120 o 240 VAC. Además, de ser reemplazables en caliente sin pérdida de servicio.

La solución propuesta por **IQsec, S.A. de C.V.** contará por cada unidad con fuentes de poder redundantes internas y alimentadas ya sea con 120 o 240 VAC. Además, de ser reemplazables en caliente sin pérdida de servicio.

**Referirse al documento:**



- 5.3.9 La solución deberá contar por cada unidad con ventiladores para flujo de aire. La solución propuesta por **IQsec, S.A. de C.V.** contará por cada unidad con ventiladores para flujo de aire.
- Referirse al documento:**  
high-performance-appliances-data-sheet\_pag 2.pdf
- 5.3.10 La solución deberá tener al menos 16 puertos de Fibra Giga Ethernet para el uso de herramientas. La solución propuesta por **IQsec, S.A. de C.V.** tendrá al menos 16 puertos de Fibra Giga Ethernet para el uso de herramientas.
- Referirse al documento:**  
dell-poweredge-r730-spec-sheet\_pag 2.pdf
- 5.3.11 La solución deberá contar por unidad el poder de instalarse en racks, y si lo requiriere contar con charolas para su correcta instalación. La solución propuesta por **IQsec, S.A. de C.V.** contará por unidad el poder de instalarse en racks, y si lo requiriere contar con charolas para su correcta instalación.
- Referirse al documento:**  
NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 1.pdf
- 5.3.12 La solución deberá contar con la capacidad de recibir módulos con puertos ópticos de fibra (1,10 y 40) de tecnología GE. La solución propuesta por **IQsec, S.A. de C.V.** contará con la capacidad de recibir módulos con puertos ópticos de fibra (1,10 y 40) de tecnología GE.
- Referirse al documento:**  
Características LR-XM6401\_pag 1.pdf





**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
6.pdf

5.3.13 La solución deberá contar con un puerto de consola y al menos un puerto 10/100/1000BaseTX para administración.

La solución propuesta por **IQsec, S.A. de C.V.** contará con un puerto de consola y al menos un puerto 10/100/1000BaseTX para administración.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
5.pdf

5.3.14 La solución deberá contar con un GUI (interface de usuario) grafica e intuitiva de fácil operación y configuración.

La solución propuesta por **IQsec, S.A. de C.V.** contará con un GUI (interface de usuario) grafica e intuitiva de fácil operación y configuración.

**Referirse al documento:**

advanced-intelligence-engine-data-sheet\_pag 2.pdf

5.3.15 Los equipos propuestos en la solución deberán disponer de recursos de procesamiento y memoria independiente para la gestión.

Los equipos propuestos en la solución ofertada por **IQsec, S.A. de C.V.** dispondrán de recursos de procesamiento y memoria independiente para la gestión.



**Referirse al documento:**

dell-poweredge-r730-spec-sheet\_pag 2.pdf

5.3.16 Los equipos propuestos en la solución deberán contar con la certificación FIPS 140-2.

Los equipos propuestos en la solución ofertada por **IQsec, S.A. de C.V.** contará con la certificación FIPS 140-2.

**Referirse al documento:**

LogRhythm 6 Receives FIPS 140-2 Certification.pdf

5.3.17 Los equipos propuestos en la solución deberán contar con la certificación Common Criteria.

Los equipos propuestos en la solución propuesta por **IQsec, S.A. de C.V.** contará con la certificación Common Criteria.

**Referirse al documento:**

LogRhythm 6.3 Criteria Certification.pdf

5.3.18 La solución deberá incluir todas las licencias requeridas para el completo y correcto funcionamiento de toda la solución en general por tres años.

La solución propuesta por **IQsec, S.A. de C.V.** incluirá todas las licencias requeridas para el completo y correcto funcionamiento de toda la solución en general por tres años.

**Referirse al documento:**

Propuesta Económica.pdf





5.3.19 Los equipos propuestos de la solución deberán contar con el mismo Sistema Operativo.

Los equipos propuestos de la solución ofertada por **IQsec, S.A. de C.V.** contarán con diferentes Sistemas Operativos, se integrarán de manera transparente y no afectarán la operación y la interoperabilidad de las soluciones.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 14 de la empresa "IQSEC S.A. DE C.V." de la página 14 de 36 que a la letra dice:

*"Se le solicita amablemente a la convocante acepte que los sistemas operativos de las soluciones ofertadas puedan ser diferentes siempre y cuando se garantice la operación e inter operatividad de las soluciones ¿Se acepta nuestra solicitud?"*

**Respuesta de la Convocante: Se acepta su solicitud, siempre y cuando la integración entre los diferentes sistemas operativos sea transparente y no afecte la operación e inter operatividad de las soluciones.**

**Referirse al documento:**

PFOS\_3.13\_UG\_733-0998\_pag 10.pdf

5.3.20 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de cortado de tráfico.

La solución propuesta por **IQsec, S.A. de C.V.** incluirá el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de cortado de tráfico.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
3.pdf

5.3.21 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.

Este punto no será cubierto por nuestra solución.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 2 de la empresa "MSG CONSULTORIA EN SISTEMAS DE INFORMACION S.A. DE C.V." de la página 6 de 36 que a la letra dice:

"Se le solicita amablemente a la convocante, permita ofertar como opcional la funcionalidad de visibilidad de sesiones cifradas, ya que dicha funcionalidad no es propia de un equipo de agregación de tráfico y limita la participación a un solo fabricante.

¿Se acepta nuestra propuesta?"

**Se tomará en cuenta la respuesta "Se acepta su propuesta, será opcional la funcionalidad de visibilidad de sesiones cifradas para la solución."**

5.3.22 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de enmascaramiento de tráfico.

La solución propuesta por **IQsec, S.A. de C.V.** incluirá el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de enmascaramiento de tráfico







**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
3.pdf

- 5.3.23 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. La solución propuesta por **IQsec, S.A. de C.V.** incluirá el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de identificación de puerto de origen

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
1.pdf

- 5.3.24 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. La solución propuesta por **IQsec, S.A. de C.V.** incluirá el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de creación de túneles seguros.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
4.pdf

- 5.3.25 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de supresión de encapsulados. La solución propuesta por **IQsec, S.A. de C.V.** incluirá el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de supresión de encapsulados



**Referirse al documento:**

PFOS\_3.13\_UG\_733-0998-pag 91.pdf

- 5.3.26 La solución propuesta deberá incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de duplicación de paquetes. La solución propuesta por **IQsec, S.A. de C.V.** incluirá el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de duplicación de paquetes.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 2.pdf

- 5.3.27 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. La solución propuesta por **IQsec, S.A. de C.V.** incluir el software y licenciamiento en todos los puertos para la correcta aplicación de las funciones de generación 1:1 de paquetes tipo FLOW.

**Referirse al documento:**

netscout-ngenius-netflow-application-note\_pag 1.pdf

- 5.3.28 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. La solución propuesta por **IQsec, S.A. de C.V.** incluirá 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.





agregación de etiquetas a los paquetes con el fin de medir el tiempo de respuesta.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 3.pdf

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

Los artefactos contemplados en este esquema de solución propuesta por **IQsec, S.A. de C.V.** contendrán las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

**Referirse al documento:**

Programa de asistencia Gold NETSCOUT.pdf

Servicio de soporte global LogRhythm.pdf

#### 5.4 Descripción de Funcionalidades

5.4.1 La solución deberá considerar un dispositivo de administración de información y eventos de seguridad en las instalaciones del Instituto

La solución propuesta por **IQsec, S.A. de C.V.** considera un dispositivo de administración de información y eventos de seguridad en las instalaciones del Instituto FONACOT, mismo que debe estar



FONACOT, mismo que debe estar considerado dentro del "cuadrante mágico de Gartner" para el año 2017 y categorizado como "Leader".

considerado dentro del "cuadrante mágico de Gartner" para el año 2017 y categorizado como "Leader".

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 15 de la empresa "IQSEC S.A. DE C.V." de la página 15 de 36 que a la letra dice:

*"Se le solicita amablemente a la convocante nos ayude a aclarar si será suficiente con que al menos uno de los equipos propuestos para el servicio (en el caso que sean mas de uno) cumpla con estar como líder en el cuadrante de Ghartner para poder dar cumplimiento al numeral.*

*¿Se acepta nuestra propuesta?*

**Se acepta su propuesta, bastará con que al menos una de las soluciones tecnologicas ofertadas para la prestación del servicio de Servicio de gestión, seguimiento y control de incidentes. Cumpla con estar dentro del cuadrante magico de Gartner categorizado como "Leader".**

**Referirse al documento:**

2017 SIEM Gartner Magic Quadrant LogRhythm\_pag 1-2.pdf

*MS*





5.4.2 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.

5.4.3 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

La solución propuesta por IQsec, S.A. de C.V. proveerá 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.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 7-8.pdf

La solución de Inteligencia de Seguridad (Security Intelligence) con la que se aprovisione la solución propuesta por **IQsec, S.A. de C.V.** contará 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



- Manejo de Incidentes y casos
- Manejo de flujos de trabajo con posibilidad de automatización
- Reporteo
- Análisis forense de la red (Network Forensics)

- Análisis forense de la red (Network Forensics)

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 6-7.pdf

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

La solución propuesta por IQsec, S.A. de C.V. no accederá en ningún momento a soluciones externas para brindar las funcionalidades aquí expresadas.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 8.pdf

5.4.5 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).

La solución propuesta por **IQsec, S.A. de C.V.** permitirá 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).

**Referirse al documento:**

LogRhythm-WebConsole-UserGuide-7.2.5-revA\_pag 4-6.pdf

MS





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

La solución propuesta por **IQsec, S.A. de C.V.** contará con la posibilidad de que la consola administrativa sea accesible por Internet Explorer/Chrome/Firefox/Safari vía web (HTTPS).

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 85-86.pdf

5.4.7 La solución deberá contar con la posibilidad de distribuirse geográficamente en distintas locaciones conteniendo integridad en la información que está siendo analizada.

La solución propuesta por **IQsec, S.A. de C.V.** contará con la posibilidad de distribuirse geográficamente en distintas locaciones conteniendo integridad en la información que está siendo analizada.

**Referirse al documento:**

es.logrhythm.com-.pdf

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.

La solución propuesta por **IQsec, S.A. de C.V.** mantendrá 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.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 45.pdf



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

La solución propuesta por **IQsec, S.A. de C.V.** permitirá un modelo de (delivery) entrega basado en: Appliance.

**Referirse al documento:**

Ir-high-performance-appliances\_pag 1.pdf

5.4.9 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.

La solución propuesta por **IQsec, S.A. de C.V.** estará 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

**Referirse al documento:**

LogRhythm 6.3 Criteria Certification.pdf

5.4.10 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

La solución propuesta por **IQsec, S.A. de C.V.** aplicará 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.





regular el acceso a los parches de sistema operativo y componentes específicos alternos a la solución ofertada.

**Referirse a los documentos:**

LogRhythm Help - LogRhythm Compatibility and System Monitor Functionality Guide.pdf

LogRhythm Help - System Requirements\_pag 1.pdf

- 5.4.11 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.
- La solución propuesta por **IQsec, S.A. de C.V.** coleccionará logs de las plataformas además de poderlo realizar de forma "agentless" sin agentes, o de manera hibrida en un deployment específico.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 9.pdf

- 5.4.12 Los componentes de las soluciones propuestas deberán estar certificados por el fabricante, además de disponibles para plataformas:
- Los componentes de las soluciones propuestas por **IQsec, S.A. de C.V.** estarán 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 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
- 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

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 87-91.pdf





5.4.13

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.

La solución propuesta por **IQsec, S.A. de C.V.** soportará 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.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 87-91.pdf

5.4.14

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

La solución de Inteligencia de Seguridad (Security Intelligence), propuesta por **IQsec, S.A. de C.V.** contará 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



información en reposo (cold data) siempre permitiendo utilizar datos viejos archivados fuera de la infraestructura en reportes e investigaciones forenses inclusive hasta 10 años.

infraestructura en reportes e investigaciones forenses inclusive hasta 10 años.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 651.pdf

5.4.15 La solución de Inteligencia de Seguridad (Security Intelligence), deberá acoplarse a utilizar las soluciones de STORAGE que la institución ya ha adquirido NAS/SAN del Instituto FONACOT, sin necesidad de sustituirlas por las soluciones propietarias.

La solución de Inteligencia de Seguridad (Security Intelligence), propuesta por **IQsec, S.A. de C.V.** se acoplará a utilizar las soluciones de STORAGE que la institución ya ha adquirido NAS/SAN del Instituto FONACOT, sin necesidad de sustituirlas por las soluciones propietarias.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 257.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** no presentará ningún tipo de costo extra a la adquisición de STORAGE propietario ni mucho menos representar este costo en la cotización para la utilización del STORAGE ya adquirido o en el esquema que este contemplado por el Instituto Fonacot.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 12.pdf





5.4.17 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.

Los logs archivados de la solución propuesta por **IQsec, S.A. de C.V.** tendrá 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.

**Referirse al documento:**

lr-processing-and-indexing- datasheet.pdf

5.4.18 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.

La solución propuesta por **IQsec, S.A. de C.V.** realizará 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.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 21.pdf

5.4.19 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

La solución propuesta por IQsec, S.A. de C.V. podrá 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.

**Referirse al documento:**



configuración que se plantee, sin tener que trabajar con la plataforma completa.

HLP-LogRhythm-7.2.5-Help\_pag 145.pdf

5.4.20 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.

Cuando en la solución propuesta por IQsec, S.A. de C.V. la cantidad de logs recibida sobrepase la capacidad licenciada de logs la solución NO "tirara/borrara" los logs sino los meterá en un proceso de espera para su procesamiento futuro cuando su carga baje.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 18.pdf

5.4.21 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.

La solución propuesta por **IQsec, S.A. de C.V.** contará 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.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 913.pdf

5.4.22 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.

El sistema de administración de logs de la solución propuesta por **IQsec, S.A. de C.V.** contará 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.





**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 245.pdf

5.4.23 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.

El sistema de administración de logs de la solución propuesta por IQsec, S.A. de C.V. proporcionará 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.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 250.pdf

5.4.24 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.

El sistema de administración de logs de la solución propuesta por **IQsec, S.A. de C.V.** contará 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.

**Referirse al documento:**

HLP-LogRhythm-7.2.5-Help\_pag 41.pdf

5.4.25 El producto de Inteligencia de Seguridad (Security Intelligence) de la solución deberá poder brindar auto-clasificación de los datos

El producto de Inteligencia de Seguridad (Security Intelligence) de la solución propuesta por **IQsec, S.A. de C.V.** podrá brindar auto-clasificación de los datos capturados en modo estructurado con fines de

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.

5.4.26 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.

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

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.

**Referirse a los documentos:**

HLP-LogRhythm-7.2.5-Help\_pag 274.pdf

lr-precision-search-datasheet.pdf

La solución propuesta por **IQsec, S.A. de C.V.** detectará y neutralizará 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.

**Referirse al documento:**

user-and-entity-behavior-analytics-data-sheet.pdf

La solución propuesta por **IQsec, S.A. de C.V.** distinguirá entre cuentas de usuario legítimas y comprometidas mediante la identificación de actividad anómala.





**Referirse al documento:**

Análisis de comportamiento de entidad y usuario UEBA\_pag 2.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** supervisará e informará automáticamente sobre la creación de cuentas con privilegios y la elevación de permisos.

**Referirse al documento:**

Análisis de comportamiento de entidad y usuario UEBA\_pag 2.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** detectará cuándo un usuario accede indebidamente a datos protegidos.

**Referirse al documento:**

user-and-entity-behavior-analytics-datasheet-pag 2.pdf

5.4.30 La solución deberá correlacionar la información de registro con identidades únicas que

La solución propuesta por **IQsec, S.A. de C.V.** correlacionará la información de registro con identidades únicas que permitan conocer quién está detrás una acción maliciosa.



permitan conocer quién está detrás una acción maliciosa.

5.4.31 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.

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

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

**Referirse al documento:**

user-and-entity-behavior-analytics-datasheet-pag 2.pdf

La solución propuesta por **IQsec, S.A. de C.V.** tendrá 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.

**Referirse al documento:**

user-and-entity-behavior-analytics-datasheet-pag 2.pdf

La solución propuesta por **IQsec, S.A. de C.V.** usará inteligencia artificial y tecnologías de aprendizaje automático que permitan mejorar el tiempo de detección y respuesta a amenazas.

**Referirse al documento:**

Análisis de comportamiento de entidad y usuario UEBA\_pag 5.pdf

La solución propuesta por **IQsec, S.A. de C.V.** proporcionará administración de casos, investigación de incidentes y generación de reportes exhaustivos.





**Referirse al documento:**

user-and-entity-behavior-analytics-datasheet\_pag 2.pdf

5.4.34 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.

La solución propuesta por **IQsec, S.A. de C.V.** será 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.

**Referirse al documento:**

EPDS\_014-1700 - vSTREAM Virtual Appliance\_pag 1.pdf

5.4.35 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.

La solución propuesta por IQsec, S.A. de C.V. será capaz de soportar la modificación, manipulación, transformación y transporte de paquetes de las capas 2,3,4 del modelo de referencia OSI.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 3.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** será capaz de crear filtrado de patrones basados en los atributos definidos de usuario (UDA).

**Referirse al documento:**

PFOS\_3.13\_UG\_733-0998\_pag 48.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** contará con un BYPASS, integrado dentro de la solución tecnológica.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 6 de la empresa "MSG CONSULTORIA EN SISTEMAS DE INFORMACION S.A. DE C.V." de la página 7 de 36 que a la letra dice:

*"Se le solicita a la convocante de la manera más atenta, que el requerimiento de BYPASS pueda ser externo o interno, es decir, ya se encuentre integrado dentro de la solución.*

*¿Se acepta nuestra propuesta?"*

**"Se acepta su propuesta, el BYPASS podrá estar integrado dentro de la solución tecnológica propuesta por el licitante."**

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_5010\_Packet\_Flow\_Switch\_pag 2.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** contará con la activación de todas las funcionalidades de forma concurrente en todos los puertos y equipos solicitados.





**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
1.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** podrá realizar modificación, manipulación, transformación y transporte de paquetes de las capas 2, 3, 4 del modelo de referencia OSI.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
3.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** será capaz de crear filtrado de patrones basados en los atributos definidos de usuario (UDA).

**Referirse al documento:**

PFOS\_3.13\_UG\_733-0998\_pag 48.pdf

5.4.41 La solución deberá poder seleccionar, modificar, manipular, transformar y transportar de tráfico específico a cada una de las

La solución propuesta por **IQsec, S.A. de C.V.** podrá 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.



herramientas para las capas 2, 3, 4 del modelo de referencia OSI.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 3.pdf

5.4.42 La solución deberá permitir la autenticación de los usuarios administradores mediante RADIUS, TACACS, LDAP y base de datos LOCAL.

La solución propuesta por **IQsec, S.A. de C.V.** permitirá la autenticación de los usuarios administradores mediante RADIUS, TACACS y base de datos LOCAL.

De acuerdo con la junta de aclaraciones de bases y considerando

la respuesta a la pregunta número 3 de la empresa "MSG CONSULTORIA EN SISTEMAS DE INFORMACION S.A. DE C.V." de la página 6 de 36 que a la letra dice:

*"Se solicita amablemente a la convocante, que se considere como cumplimiento del requerimiento, el soportar la autenticación de al menos 3 métodos de los 4 solicitados"*

*¿Se acepta nuestra propuesta?*

**Respuesta de la Convocante: "Se acepta su propuesta, la solución propuesta por el licitante deberá soportar la autenticación de al menos 3 métodos de los 4 solicitados".**





**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
4.pdf

5.4.43 La solución deberá mediante el uso de mapas administrados por usuario (RBAC), permitir el aprovechamiento de un mismo puerto para distintos usos.

La solución propuesta por **IQsec, S.A. de C.V.** podrá mediante el uso de mapas administrados por usuario (RBAC), permitir el aprovechamiento de un mismo puerto para distintos usos.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
3.pdf

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
4.pdf

5.4.44 La solución deberá soportar el manejo de tráfico Multicast a varios puertos permitiendo así el acceso del mismo tráfico a distintas herramientas conectadas.

La solución propuesta por **IQsec, S.A. de C.V.** soportará el manejo de tráfico Multicast a varios puertos permitiendo así el acceso del mismo tráfico a distintas herramientas conectadas.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
1.pdf



5.4.45 La solución deberá soportar el estándar IEEE 802.1Q (encapsulado de varias vlans sobre el mismo enlace físico).

La solución propuesta por **IQsec, S.A. de C.V.** soportará el estándar IEEE 802.1Q (encapsulado de varias vlans sobre el mismo enlace físico).

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 7.pdf

5.4.46 La solución deberá soportar el estándar IEEE 802.3ad (agregación de varios enlaces físicos).

La solución propuesta por **IQsec, S.A. de C.V.** soportará el estándar IEEE 802.3ad (agregación de varios enlaces físicos).

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 7.pdf

5.4.47 La solución deberá soportar Jumbo Frames (MTU 9000 bytes).

La solución propuesta por **IQsec, S.A. de C.V.** soportará Jumbo Frames (MTU 9000 bytes).

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 7.pdf

5.4.48 La solución deberá soportar IPv6 e IPv4.

La solución propuesta por **IQsec, S.A. de C.V.** soportará IPv6 e IPv4.





**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
7.pdf

5.4.49 La solución deberá proteger el tráfico (Inline) de todas las herramientas (Firewalls, IPS, antimalware, SSL encryption) conectadas en los puertos de los equipos propuestos.

La solución propuesta por **IQsec, S.A. de C.V.** protegerá el tráfico (Inline) de todas las herramientas (Firewalls, IPS, antimalware, SSL encryption) conectadas en los puertos de los equipos propuestos.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
2.pdf

5.4.50 La solución deberá soportar la relación inline de muchos a muchos.

La solución propuesta por **IQsec, S.A. de C.V.** soportará la relación inline de muchos a muchos.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
3.pdf

5.4.51 La solución deberá soportar la capacidad de creación de CLUSTER con otras plataformas

La solución propuesta por **IQsec, S.A. de C.V.** Soportará la capacidad de creación de CLUSTER con otras plataformas del mismo fabricante y deberán ser administrados por la misma consola.



del mismo fabricante y deberán ser administrados por la misma consola.

5.4.52 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.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 4.pdf

La solución propuesta por **IQsec, S.A. de C.V.** soportará al menos los siguientes tipos de conectores: SFP, SFP+, QSFP+, incluyendo los siguientes tipos de cables: SR, LR, ER, BIDI.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 4 de la empresa "MSG CONSULTORIA EN SISTEMAS DE INFORMACION S.A. DE C.V." de la página 7 de 36 que a la letra dice:

*"Se solicita amablemente a la convocante que permita como opcional el soporte de conectores QSFP28 que se refieren a tecnologías de 100G, ya que en las soluciones requeridas en este concurso no se contemplan interfaces a 100G.*

*¿Se acepta nuestra propuesta?"*

**"Se acepta su propuesta, se permite como opcional el soporte de conectores QSFP28 que se refieren a tecnologías de 100G".**



**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
6.pdf

5.4.53 La solución deberá soportar la capacidad NON BLOCKING en los STACKS con otras soluciones similares del mismo fabricante.

La solución propuesta por **IQsec, S.A. de C.V.** soportará la capacidad NON BLOCKING en los STACKS con otras soluciones similares del mismo fabricante.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
1.pdf

5.4.54 La solución deberá soportar la capacidad NON BLOCKING en el BACKPLANE de la plataforma ofertada.

La solución propuesta por **IQsec, S.A. de C.V.** soportará la capacidad NON BLOCKING en el BACKPLANE de la plataforma ofertada.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
1.pdf

5.4.55 La solución deberá contar con módulos intercambiables en caliente (HOTSWAP).

La solución propuesta por **IQsec, S.A. de C.V.** contará con módulos intercambiables en caliente (HOTSWAP).

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag 1.pdf

- 5.4.56 La solución deberá poder clasificar el tráfico en tiempo real identificando geolocalización y tipo de equipo.

**Por lo tanto, este punto no será cubierto por la solución propuesta.**

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 5 de la empresa "MSG CONSULTORIA EN SISTEMAS DE INFORMACION S.A. DE C.V." de la página 7 de 36 que a la letra dice:

*"Se solicita a la convocante de la manera más atenta, que elimine esta funcionalidad ya que es una funcionalidad propietaria la cual cumple un solo fabricante, limitando así la libre competencia.*

*¿Se acepta nuestra propuesta?"*

**"Se acepta su propuesta, la funcionalidad será opcional como parte del servicio".**

- 5.4.57 La solución deberá tener balanceo de cargas para tráfico en línea y tráfico en paralelo.

La solución propuesta por **IQsec, S.A. de C.V.** tendrá balanceo de cargas para tráfico en línea y tráfico en paralelo.





**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
3.pdf

5.4.58 La solución deberá poder terminar túneles de GRE para una comunicación alterna y así soportar una alta disponibilidad de las interconexiones de red.

La solución propuesta por **IQsec, S.A. de C.V.** podrá terminar túneles de GRE para una comunicación alterna y así soportar una alta disponibilidad de las interconexiones de red.

**Referirse al documento:**

NETSCOUT\_DS\_nGenius\_4200\_Series\_Packet\_Flow\_Switch\_pag  
3.pdf

5.4.59 El licitante deberá entregar de manera mensual un reporte de inteligencia con los siguientes rubros:

**IQsec, S.A. de C.V.** entregará 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
- 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





- Acciones de respuesta
- Perfil de los atacantes
- Recomendaciones Generales
- ANEXOS
- GLOSARIO
- Recomendaciones Generales
- ANEXOS
- GLOSARIO

## 6. Servicios de Validación de Identidad

### 6.1 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**”, permitirá 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. Dicho servicio permitirá al Instituto FONACOT estar en condiciones de cumplir con las regulaciones y normas mexicanas aplicables.

### 6.2 Características del Servicio

- 6.2.1 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.
- Derivado de la sensibilidad de los trámites de crédito que realiza El Instituto FONACOT, el servicio de validación de identidad propuesto por **IQsec, S.A. de C.V.** estará soportado por un producto de fabricante que cuente con base instalada y no será un desarrollo de software a la medida.

**Referirse al documento:**





FielNet\_Brochure.pdf

Contrato de NAFIN 11-2018.pdf

6.2.2 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 El Instituto FONACOT, para el uso desde las sucursales y las diferentes caravanas.

El servicio de validación de identidad propuesto por **IQsec, S.A. de C.V.** se integrará con los dispositivos biométricos y estaciones de trabajo con los que ya cuenta la plataforma tecnológica del El Instituto FONACOT, para el uso desde las sucursales y las diferentes caravanas.

**Referirse al documento:**

IQsec\_SoluciondeValidacionIdentidad\_pag 2.pdf

6.2.3 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.

El servicio de validación de identidad propuesto por **IQsec, S.A. de C.V.** será 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.

**Referirse al documento:**

Docufiel – API.pdf

6.2.4 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

En el momento que El Instituto FONACOT requiera el servicio de validación de identidad, la solución propuesta por **IQsec, S.A. de C.V.** cumplirá con las bases y mecanismos técnicos necesarios establecidos por el Instituto Nacional Electoral (INE), considerando una arquitectura de alta disponibilidad y



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.

DRP que permitirá 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.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 8 de la empresa "MSG CONSULTORIA EN SISTEMAS DE INFORMACION S.A. DE C.V." de la página 8 de 36 que a la letra dice:

*"Se le solicita amablemente a la convocante nos ayude a precisar si es correcto entender que para dar cumplimiento con lo requerido en el numeral 6.2.4 se debe contemplar el tener un ambiente de HA y DRP, para poder cumplir con los niveles de disponibilidad del servicio que se requieren para el servicio de Validación de Identidad y poder realizar las verificaciones del padrón electoral del INE.*

*¿Se acepta nuestra propuesta?"*

**Respuesta de la Convocante: "Es correcta su apreciación, la solución ofertada por el licitante deberá estar configurada en alta disponibilidad y contar con un DRP en caso de solicitarse alguna contingencia, los cuáles deberán estar considerados en la propuesta económica que presenta el licitante"**

**Referirse al documento:**





IQsec\_SoluciondeValidacionIdentidad\_pag 2.pdf

6.2.5 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).

En el momento que El Instituto FONACOT efectúe el acuerdo para realizar validación de identidad contra el Padrón Electoral del INE, facilitará a **IQsec, S.A. de C.V.** las características del hardware de seguridad que integrará con el INE y la solución de validación de identidad contará 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).

**Referirse al documento:**

IQsec\_SoluciondeValidacionIdentidad\_pag 1.pdf

IQsec\_SoluciondeValidacionIdentidad\_pag 2.pdf

6.2.6 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).

El servicio de validación de identidad propuesto por **IQsec, S.A. de C.V.** autenticará, cifrará, y firmará electrónicamente las peticiones de consulta de los puntos de verificación y validación hacia el (INE).

**Referirse al documento:**

Commercefiel\_pag 2.pdf

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

El servicio propuesto por **IQsec, S.A. de C.V.** realizará funciones de auditoría para validar la integridad de la información ante una posible controversia derivado de las peticiones de consulta.



- Referirse al documento:**
- Docufiel\_pag 1.pdf
- Docufiel\_pag 2.pdf
- 6.2.8 El servicio deberá mantener y ofrecer el monitoreo de las transacciones a lo largo de todo el proceso de consulta. El servicio propuesto por **IQsec, S.A. de C.V.** mantendrá y ofrecer el monitoreo de las transacciones a lo largo de todo el proceso de consulta.
- Referirse al documento:**
- Docufiel\_pag 2.pdf
- 6.2.9 El servicio deberá cumplir con la emisión de sellos de tiempo conforme al estándar RFC 3161 para cada solicitud de consulta generada. El servicio propuesto por **IQsec, S.A. de C.V.** cumplirá con la emisión de sellos de tiempo conforme al estándar RFC 3161 para cada solicitud de consulta generada.
- Referirse al documento:**
- Commercefiel\_pag 2.pdf
- 6.2.10 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. El servicio propuesto por **IQsec, S.A. de C.V.** realizará la validación de documentos oficiales como comprobantes de domicilio, recibos de nómina, y estados de cuenta a través de archivos XML.
- Referirse al documento:**
- Docufiel\_pag 2.pdf
- 6.2.11 La solución propuesta deberá tener la capacidad de personalizar las interfaces web de acuerdo con la imagen institucional del Instituto FONACOT. La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad de personalizar las interfaces web de acuerdo con la imagen institucional del Instituto FONACOT.





**Referirse al documento:**

Docufiel\_pag 2.pdf

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

El servicio propuesto por **IQsec, S.A. de C.V.** tendrá la capacidad de realizar validaciones con entidades de verificación de información, como: RENAPO, SAT e INE principalmente.

**Referirse al documento:**

IQsec\_SoluciondeValidacionIdentidad\_pag.1.pdf

6.2.13 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).

El servicio propuesto por **IQsec, S.A. de C.V.** tendrá 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).

**Referirse al documento:**

Commercefiel\_pag 2.pdf

6.2.14 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.

El servicio propuesto por **IQsec, S.A. de C.V.** ofrecerá la capacidad de otorgar visibilidad sobre el estado de dispositivos de seguridad en hardware (HSM). Así, mismo ofrecerá un esquema de monitoreo en intervalos de tiempo de al menos un minuto.

**Referirse al documento:**

CipherTrust-Monitor-ds\_pag 2.pdf



6.2.15 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.

El servicio propuesto por **IQsec, S.A. de C.V.** tendrá la capacidad de generar las alertas correspondientes a dicho monitoreo de acuerdo con los parámetros de criticidad definidos por El Instituto FONACOT

**Referirse al documento:**

CipherTrust-Monitor-ds\_pag 2.pdf

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

El servicio propuesto por **IQsec, S.A. de C.V.** permitirá la implementación de dominios de trabajo para segmentar y delimitar el acceso de los componentes del servicio.

**Referirse al documento:**

CipherTrust-Monitor-ds\_pag 2.pdf

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

El servicio propuesto por **IQsec, S.A. de C.V.** tener la capacidad de integrarse con dispositivos que realicen la validación física de credenciales para votar y pasaportes.

**Referirse al documento:**

Docufiel\_pag 2.pdf

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

La solución de validación de identidad de **IQsec, S.A. de C.V.** cumplirá con los siguientes estándares:

- Llaves públicas y privadas RSA a 1024/2048/4096 bits.
- Certificados digitales X509 v3.

- 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-1, 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.
- Estándares de criptografía PKCS#1, PKCS#7, CAdES, SAdES y PAdES.
  - Algoritmos de digestión MD5, SHA-1, 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.

**Referirse al documento:**

Docufiel - API.pdf

Commercefiel\_pag 2.pdf

nShield-Connect-span-ds\_pag 2.pdf

thales\_nshield\_pag 2.pdf

### 6.3 Descripción de Componentes



- |       |  |  |
|-------|--|--|
| 6.3.1 | La solución deberá cumplir con los estándares de seguridad UL, CE, FCC, C-TICK, Canadá ICES, RoHS2 y WEEE.                             | La solución propuesta por IQsec, S.A. de C.V. cumplirá con los estándares de seguridad UL, CE, FCC, C-TICK, Canadá ICES, RoHS2 y WEEE.<br><br><b>Referirse al documento:</b><br><br>nShield-Connect-span-ds_pag 2.pdf                                    |
| 6.3.2 | La solución deberá soportar API's PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG.  | La solución propuesta por <b>IQsec, S.A. de C.V.</b> soportará API's PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG<br><br><b>Referirse al documento:</b><br><br>nShield-Connect-span-ds_pag 2.pdf   |
| 6.3.3 | La solución deberá soportar algoritmos criptográficos asimétricos RSA, Diffie-Hellman, ECMQV, DSA, KCDSA, ECDSA, ECDH.                 | La solución propuesta por <b>IQsec, S.A. de C.V.</b> soportará algoritmos criptográficos asimétricos RSA, Diffie-Hellman, ECMQV, DSA, KCDSA, ECDSA, ECDH.<br><br><b>Referirse al documento:</b><br><br>nShield-Connect-span-ds_pag 2.pdf                 |
| 6.3.4 | La solución deberá soportar algoritmos criptográficos simétricos AES, AES-GCM, ARIA, Camellia, CAST, RIPEMD160 HMAC, SEED, Triple DES. | La solución propuesta por <b>IQsec, S.A. de C.V.</b> soportará algoritmos criptográficos simétricos AES, AES-GCM, ARIA, Camellia, CAST, RIPEMD160 HMAC, SEED, Triple DES.<br><br><b>Referirse al documento:</b><br><br>nShield-Connect-span-ds_pag 2.pdf |





6.3.5 La solución deberá contar con los cumplimientos de seguridad FIPS 140-2 Level 2 and Level 3, USGv6 accreditation.

La solución propuesta por **IQsec, S.A. de C.V.** contará con los cumplimientos de seguridad FIPS 140-2 Level 2 and Level 3, USGv6 accreditation.

**Referirse al documento:**

nShield-Connect-span-ds\_pag 2.pdf

6.3.6 La solución deberá soportar los sistemas operativos:

La solución propuesta por **IQsec, S.A. de C.V.** soportará los sistemas operativos:

- Microsoft Windows 7 x64, 10 x64
- Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- 2016 Nano x64i
- 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 7 x64, 10 x64
- Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- 2016 Nano x64i
- 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

- Microsoft Windows Hyper-V Server 2012 R2,
- 2016 VMware ESXi 5.5
- Citrix XenServer 6.5
- AIX LPARs

6.3.7 La solución deberá soportar alta disponibilidad (HA).

**Referirse al documento:**

nShield-Connect-span-ds\_pag 2.pdf

La solución propuesta por **IQsec, S.A. de C.V.** soportará alta disponibilidad (HA).

**Referirse al documento:**

nShield-Connect-span-ds\_pag 2.pdf

6.3.8 La solución deberá soportar un consumo de energía, up to 2.0A at 110V AC, 60Hz | 1.0A at 220V AC, 50Hz.

La solución propuesta por **IQsec, S.A. de C.V.** soportará un consumo de energía, up to 2.0A at 110V AC, 60Hz | 1.0A at 220V AC, 50Hz.

**Referirse al documento:**

nShield-Connect-span-ds\_pag 2.pdf

6.3.9 La solución deberá soportar altas capacidades de transacción dónde el rendimiento es crítico.

La solución propuesta por **IQsec, S.A. de C.V.** soportará altas capacidades de transacción dónde el rendimiento es crítico.

**Referirse al documento:**





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

nShield-Connect-span-ds\_pag 2.pdf

Los artefactos contemplados en este esquema de solución propuesta por **IQsec, S.A. de C.V.** contendrán las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

**Referirse al documento:**

Premium Plus Support Technical Support Thales e-Security.pdf

Propuesta de mesa de ayuda\_pag 4.pdf

## 6.4 Descripción de Funcionalidades

6.4.1 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.

La solución propuesta por **IQsec, S.A. de C.V.** realizará 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.

**Referirse al documento:**

nShield-Connect-span-ds\_pag 2.pdf



- 6.4.2 La solución deberá permitir el almacenamiento y procesamiento seguro de llaves y aplicaciones. La solución propuesta por **IQsec, S.A. de C.V.** permitirá el almacenamiento y procesamiento seguro de llaves y aplicaciones  
**Referirse al documento:**  
thales\_nshield\_pag 2.pdf
- 6.4.3 La solución deberá poder realizar descarga y aceleración criptográfica. La solución propuesta por **IQsec, S.A. de C.V.** podrá realizar descarga y aceleración criptográfica.  
**Referirse al documento:**  
thales\_nshield\_pag 2.pdf
- 6.4.4 La solución deberá proporcionar control de accesos multinivel autenticado. La solución propuesta por **IQsec, S.A. de C.V.** proporcionará control de accesos multinivel autenticado.  
**Referirse al documento:**  
thales\_nshield\_pag 2.pdf
- 6.4.5 La solución deberá permitir autenticación de cliente utilizando hardware token. La solución propuesta por **IQsec, S.A. de C.V.** permitirá autenticación de cliente utilizando hardware token.  
**Referirse al documento:**  
thales\_nshield\_pag 2.pdf
- 6.4.6 La solución deberá poder realizar copia de seguridad, replicación y recuperación de la llave. La solución propuesta por **IQsec, S.A. de C.V.** podrá realizar copia de seguridad, replicación y recuperación de la llave.  
**Referirse al documento:**  
thales\_nshield\_pag 2.pdf





6.4.7 La solución deberá brindar un almacenamiento ilimitado de llaves protegidas.

La solución propuesta por **IQsec, S.A. de C.V.** brindará un almacenamiento ilimitado de llaves protegidas.

**Referirse al documento:**

thales\_nshield\_pag 2.pdf

6.4.8 La solución deberá soportar agrupamiento y balanceo de carga.

La solución propuesta por **IQsec, S.A. de C.V.** soportará agrupamiento y balanceo de carga.

**Referirse al documento:**

thales\_nshield\_pag 2.pdf

6.4.9 La solución deberá poder realizar separación criptográfica lógica de las llaves de la aplicación.

La solución propuesta por **IQsec, S.A. de C.V.** podrá realizar separación criptográfica lógica de las llaves de la aplicación.

**Referirse al documento:**

thales\_nshield\_pag 2.pdf

6.4.10 La solución deberá tener la capacidad de realizar autenticación multifactor.

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad de realizar autenticación multifactor.

**Referirse al documento:**

thales\_nshield\_pag 2.pdf



## 7. Servicio de Detección e Investigación de Vulnerabilidades y Pruebas de Penetración

### 7.1 Descripción del Servicio

**IQsec, S.A. de C.V.**, proveerá 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.

**IQsec, S.A. de C.V.**, identificará y solucionará 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 permitirá la detección de vulnerabilidades en los sistemas internos y realizará 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 e **IQsec, S.A. de C.V.**, 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.

### 7.2 Características del Servicio





7.2.1 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.

El servicio propuesto por **IQsec, S.A. de C.V.** permitirá obtener un nivel realista de riesgo y vulnerabilidades en contra de la tecnología, que comprenden las redes, aplicaciones, enrutadores, conmutadores, dispositivos, etc.

**Referirse al documento:**

Propuesta Tipo Pentest pag 4.pdf

7.2.2 El servicio deberá realizar ataques múltiples que involucra varias facetas de pruebas de penetración, de aplicaciones, de la red y de los sistemas operativos.

El servicio propuesto por **IQsec, S.A. de C.V.** realizará ataques múltiples que involucra varias facetas de pruebas de penetración, de aplicaciones, de la red y de los sistemas operativos.

**Referirse al documento:**

Propuesta Tipo Pentest pag 5.pdf

7.2.3 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.

El servicio propuesto por **IQsec, S.A. de C.V.** realizará 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

**Referirse al documento:**

Propuesta Tipo Pentest pag 5.pdf



7.2.4 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.

El alcance del servicio propuesto por **IQsec, S.A. de C.V.** constará de al menos 1900 IP'S y host como parte del alcance:

- 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.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 9 de la empresa "MSG CONSULTORIA EN SISTEMAS DE INFORMACION S.A. DE C.V." de la página 8 de 36 que a la letra dice:

*"Se le solicita amablemente a la convocante que nos ayude a precisar el número de IP'S y host a los cuáles se estaría revisando los servicios de investigación de vulnerabilidades y pruebas de penetración, lo anterior, con la intención de poder garantizar la correcta operación y continuidad del mismo servicio durante la vigencia de contrato".*

*¿Se acepta nuestra propuesta?"*





**"Se requiere que las soluciones tecnológicas utilizadas para prestación del servicio de detección e investigación de vulnerabilidades y pruebas de penetración contemple al menos 1900 IP'S y Host como parte del alcance".**

**Referirse al documento:**

Propuesta Tipo Pentest pag 5.pdf

El servicio propuesto por **IQsec, S.A. de C.V.** se llevará a cabo consistentemente, utilizando marcos y estándar aceptados a nivel mundial y de la industria como OWASP, a fin de garantizar una operación sólida.

**Referirse al documento:**

Propuesta Tipo Pentest pag 8.pdf

El servicio propuesto por **IQsec, S.A. de C.V.** tendrá una fase de pruebas para corroborar el nivel de seguridad actual de la institución, las cuales estarán divididas en las siguientes fases:

7.2.5 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.

7.2.6 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

- Reconocimiento
- Explotación
- Acciones sobre el objetivo
- Análisis de resultados



- Recomendaciones y acciones de remediación

- Recomendaciones y acciones de remediación

**Referirse al documento:**

Propuesta Tipo Pentest pag 5.pdf

7.2.7 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.

**IQsec, S.A. de C.V.** contará 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.

**Referirse al documento:**

Propuesta Tipo Pentest pag 5.pdf

7.2.8 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.

El servicio propuesto por **IQsec, S.A. de C.V.** utilizará 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.

**Referirse al documento:**

Propuesta Tipo Pentest pag 15-16.pdf

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

El servicio propuesto por **IQsec, S.A. de C.V.** 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.
- 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.

**Referirse al documento:**

Propuesta Tipo Pentest pag 18.pdf

### 7.3 Descripción de Componentes

- 7.3.1 Los servicios de detección e investigación de vulnerabilidades se deben de dar por lo menos dos veces al año.
- Los servicios de detección e investigación de vulnerabilidades propuestos por **IQsec, S.A. de C.V.** se darán por lo menos dos veces al año.





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

**IQsec, S.A. de C.V.** refiere que en dado caso que la institución lo requiera más de dos veces al año, no representará ningún costo adicional para el Instituto FONACOT.

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

Los artefactos contemplados en este esquema de solución propuesta por **IQsec, S.A. de C.V.** contendrán las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

**Referirse al documento:**

Tenable\_Technical\_Support\_Plans.pdf

Propuesta de mesa de ayuda\_pag 4.pdf

#### 7.4 Descripción de Funcionalidades

7.4.1 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 informe deberá destacar los riesgos de seguridad provenientes de los hallazgos y proporcionar una visión clara del nivel de seguridad de la organización.

El servicio propuesto por **IQsec, S.A. de C.V.** contemplará 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 informe deberá destacar los riesgos de seguridad provenientes de los hallazgos y proporcionar una visión clara del nivel de seguridad de la organización.



7.4.2 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.

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

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

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 306-315.pdf

El servicio de detección e investigación de vulnerabilidades propuesto por **IQsec, S.A. de C.V.** contemplará la infraestructura actual del instituto y **IQsec, S.A. de C.V.**, generará un plan de trabajo en conjunto con El Instituto FONACOT y utilizará herramientas comerciales para ejecutar este servicio, actualizadas y vigentes previo al análisis.

El servicio propuesto por **IQsec, S.A. de C.V.** contará con opciones de implementación en ambientes virtuales y físicos.

**Referirse al documento:**

SecurityCenterCV-(DS)-EsLa\_pag 2.pdf

El servicio propuesto por **IQsec, S.A. de C.V.** soportará sistemas operativos Windows y Linux Red Hat y/o CentOS para su implementación.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 18.pdf





7.4.5 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.

El servicio propuesto por **IQsec, S.A. de C.V.** permitirá la administración de los componentes a través de interfaces web, soportando los principales navegadores web, así como navegadores en tabletas o dispositivos móviles.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 22.pdf

7.4.6 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.

El servicio propuesto por **IQsec, S.A. de C.V.** ofrecerá visibilidad continua sobre las posibles vulnerabilidades existentes dentro del instituto aun cuando no se estén ejecutando revisiones activas sobre la infraestructura.

**Referirse al documento:**

SecurityCenterCV-(DS)-EsLa\_pag 1.pdf

7.4.7 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.

El servicio propuesto por **IQsec, S.A. de C.V.** permitirá 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.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 134.pdf

7.4.8 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.

El servicio propuesto por **IQsec, S.A. de C.V.** garantizará 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.



7.4.9 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.

7.4.10 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.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 123.pdf

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.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 156-157.pdf

SecurityCenter\_UserGuide\_pag 156.pdf

SecurityCenter\_UserGuide\_pag 160.pdf

SecurityCenter\_UserGuide\_pag 166.pdf

El servicio propuesto por **IQsec, S.A. de C.V.** ofrecerá 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.





7.4.11 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.

**Referirse al documento:**

SecurityCenterCV-(DS)-EsLa\_pag 1.pdf

El servicio propuesto por **IQsec, S.A. de C.V.** ofrecerá 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.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 104-114.pdf

SecurityCenter\_UserGuide\_pag 251-252.pdf

7.4.12 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.

El servicio propuesto por **IQsec, S.A. de C.V.** generará 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.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 131.pdf

SecurityCenter\_UserGuide\_pag 306-315.pdf

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

El servicio propuesto por **IQsec, S.A. de C.V.** generará un impacto mínimo en la red del instituto durante el proceso de escaneo.



7.4.14 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.

7.4.15 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).

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 156.pdf

SecurityCenter\_UserGuide\_pag 160.pdf

SecurityCenter\_UserGuide\_pag 166.pdf

El servicio propuesto por **IQsec, S.A. de C.V.** contará 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.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 132.pdf

SecurityCenter\_UserGuide\_pag 141.pdf

SecurityCenter\_UserGuide\_pag 145.pdf

El servicio propuesto por **IQsec, S.A. de C.V.** de contará 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).

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 104-109.pdf

SecurityCenter\_UserGuide\_pag 251-252.pdf



7.4.16 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

7.4.17 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.

La solución propuesta por **IQsec, S.A. de C.V.** ofrecerá 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

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 319-323.pdf

La solución propuesta por **IQsec, S.A. de C.V.** permitirá 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

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 139.pdf

SecurityCenter\_UserGuide\_pag 172.pdf





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

SecurityCenter\_UserGuide\_pag 173.pdf

SecurityCenter\_UserGuide\_pag 188.pdf

SecurityCenter\_5.1\_Admin\_Guide\_pag 65.pdf

SecurityCenter\_5.1\_Admin\_Guide\_pag 66.pdf

La solución propuesta por **IQsec, S.A. de C.V.** contará con soporte para el desarrollo de scripts personalizados para el análisis de sistemas, dispositivos de comunicaciones y aplicativos instalados.

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

**Referirse al documento:**

SecurityCenter\_5.1\_Admin\_Guide\_pag 23.pdf

La solución propuesta por **IQsec, S.A. de C.V.** proporcionará plantillas predefinidas para el modelo ISO 27001.

7.4.20 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.

**Referirse al documento:**

ISOIEC2700127002\_EN\_SB\_v3\_web.pdf

La solución propuesta por **IQsec, S.A. de C.V.** permitirá la priorización de los escaneos, de modo que aquellos prioritarios puedan ejecutarse a toda velocidad, mientras que los demás se ejecuten más lentamente.





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

**Referirse al documento:**

Custom Scan Policy Options (SC)\_pag 2-3.pdf

La solución propuesta por **IQsec, S.A. de C.V.** será capaz de conectarse con herramientas de escaneos pasivos y correlacionadores de eventos

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

**Referirse al documento:**

SecurityCenter\_5.1\_Admin\_Guide\_pag 41.pdf

SecurityCenter\_5.1\_Admin\_Guide\_pag 43.pdf

SecurityCenter\_UserGuide\_pag 261-263.pdf

La solución propuesta por **IQsec, S.A. de C.V.** permitirá especificar exclusiones para cada escaneo, para prevenir el escaneo de sistemas críticos.

7.4.23 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

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 168.pdf

La solución propuesta por **IQsec, S.A. de C.V.** realizará escaneos con secuencias de comandos Web para detectar vulnerabilidades de las aplicaciones de servidor, tales como:

- a. Microsoft Internet Information Server (IIS)

28



- c. Java
- d. JBoss
- e. Tomcat

- b. Apache
- c. Java
- d. JBoss
- e. Tomcat

7.4.24 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.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 167-171.pdf

SecurityCenter\_UserGuide\_pag 312.pdf

La solución propuesta por **IQsec, S.A. de C.V.** permitirá 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.

7.4.25 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:

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 134-136.pdf

La solución propuesta por **IQsec, S.A. de C.V.** contará 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.





- 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.

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.



**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 350-353.pdf

SecurityCenter\_UserGuide\_pag 356.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** proporcionará el análisis y mostrar los comentarios inmediatos a los desarrolladores sobre problemas y vulnerabilidades.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 293-296.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** realizará verificación de seguridad a nivel de acceso.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 293-296.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** hará escaneos en el código en busca de vulnerabilidades

**Referirse al documento:**

<https://www.tenable.com/products/tenable-io/lumin>





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

La solución propuesta por **IQsec, S.A. de C.V.** permitirá la administración de los accesos de los usuarios.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 87.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** realizará análisis de código de diferentes lenguajes de programación.

**Referirse al documento:**

<https://www.tenable.com/products/tenable-io/lumin>

7.4.31 La solución deberá permitir la verificación de compilación independiente.

La solución propuesta por **IQsec, S.A. de C.V.** permitirá la verificación de compilación independiente.

**Referirse al documento:**

<https://www.tenable.com/blog/understanding-tenable-plugins>

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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad para integrarse con la infraestructura ya sea de forma local o remota.

**Referirse al documento:**



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

Tenable.io-Platform-(DS)-EsLa\_pag 1.pdf

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad de responder ante aplicaciones críticas sin afectar el rendimiento

7.4.34 La solución deberá contar con Independent Secure Build Verification.

**Referirse al documento:**

SecurityCenter\_UserGuide\_pag 156-157.pdf

La solución propuesta por **IQsec, S.A. de C.V.** contará con Independent Secure Build Verification.

**Referirse al documento:**

<https://www.tenable.com/blog/secure-configuration-baselines-for-network-devices>

38





## 8. Servicio de Control y Gestión de Usuarios

### 8.1 Descripción del Servicio

El servicio asegurará el acceso a la infraestructura y sistemas informáticos del Instituto FONACOT. **IQsec, S.A. de C.V.**, asignará 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, robustecerá el control de acceso, recabará y mantendrá 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. Realizará aprovisionamiento, cambio de privilegios y baja de usuarios.

El servicio permitirá 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, orquestará acciones de contención o prevención con tecnologías como firewall y escáner de vulnerabilidades entre otros. Realizará la administración de movilidad desde una única consola de administración centralizada que permita administrar la seguridad de las aplicaciones, los datos y la red.

### 8.2 Descripción de Componentes

- 8.2.1. 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.
- La solución propuesta por **IQsec, S.A. de C.V.** permitirá 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 adicionalmente integrar 100 servidores y 10 usuarios de

28



administración de accesos privilegiados como parte de la solución.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 10 de la empresa "MSG CONSULTORIA EN SISTEMAS DE INFORMACION S.A. DE C.V." de la página 9 de 36 que a la letra dice:

*"Se le solicita de la manera más amable a la convocante nos ayude a confirmar el número de dispositivos que el Instituto contempla dentro de la prestación del servicio y su crecimiento estimado durante la vigencia del contrato".*

*¿Se acepta nuestra propuesta?"*

**Respuesta de la Convocante: "El número de dispositivos propuestos para la prestación del servicio será determinado por cada licitante y en base al mismo deberá generar su propuesta de la licitación, contemplando que adicionalmente se prodría requerir integrar 100 servidores y 10 usuarios de adminsitración de accesos privilegiados como parte de la solución.**

8.2.2. La solución deberá permitir la administración mediante el Puerto serial.

La solución propuesta por **IQsec, S.A. de C.V.** permitirá la administración mediante el Puerto serial.





**Referirse al documento:**

VCT-CT-appliances-with-v8-specs\_pag 3.pdf

8.2.3. La solución deberá tener 2 puertos USB, 2 back panel USB 2.0 + 1 front panel USB 2.0.

La solución propuesta por **IQsec, S.A. de C.V.** tendrá 2 puertos USB, 2 back panel USB 2.0 + 1 front panel USB 2.0.

**Referirse al documento:**

VCT-CT-appliances-with-v8-specs\_pag 3.pdf

8.2.4. La solución deberá soportar hard drives.

La solución propuesta por **IQsec, S.A. de C.V.** soportará hard drives.

**Referirse al documento:**

VCT-CT-appliances-with-v8-specs\_pag 3.pdf

8.2.5. La solución deberá soportar requisitos de enfriamiento de 2891 BTU/Hr.

La solución propuesta por **IQsec, S.A. de C.V.** soportará requisitos de enfriamiento de 2891 BTU/Hr.

**Referirse al documento:**

VCT-CT-appliances-with-v8-specs\_pag 3.pdf

8.2.6. La solución deberá permitir multi-Gbps de ancho de banda.

La solución propuesta por **IQsec, S.A. de C.V.** permitirá multi-Gbps de ancho de banda.



**Referirse al documento:**

- 8.2.7. La solución deberá tener un consume de energía máximo de 744W.

VCT-CT-appliances-with-v8-specs\_pag 3.pdf

La solución propuesta por **IQsec, S.A. de C.V.** tendrá un **consumo de energía** máximo de 744W.

**Referirse al documento:**

- 8.2.8. La solución deberá contar con las entradas de VGA y CD-ROM.

VCT-CT-appliances-with-v8-specs\_pag 3.pdf

La solución propuesta por **IQsec, S.A. de C.V.** contará con las entradas de VGA y CD-ROM

**Referirse al documento:**

- 8.2.9. La solución deberá contar al menos con la capacidad de interfaces de cobre y de fibra óptica de 1G y 10G.

VCT-CT-appliances-with-v8-specs\_pag 3.pdf

La solución propuesta por **IQsec, S.A. de C.V.** contará al menos con la capacidad de interfaces de cobre y de fibra óptica de 1G y 10G.

**Referirse al documento:**

VCT-CT-appliances-with-v8-specs\_pag 3.pdf





### 8.3 Descripción de Funcionalidades

- 8.3.1. 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.
- La solución propuesta por **IQsec, S.A. de C.V.** podrá 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.

**Referirse al documento:**

Appliance Matrix Data Sheet\_pag 1-2.pdf

- 8.3.2. La solución del licitante deberá poder soportar modo activo/pasivo, para hacer la replicación de datos y alta disponibilidad
- La solución propuesta por **IQsec, S.A. de C.V.** podrá soportar modo activo/pasivo, para hacer la replicación de datos y alta disponibilidad

**Referirse al documento:**

PBPS 6.2 Deployment and Failover\_pag 10-11.pdf

- 8.3.3. La solución del licitante deberá poder tener un appliance en un sitio alternativo (físico o virtual) que pueda servir como recuperación de desastres (DRP)
- La solución propuesta por **IQsec, S.A. de C.V.** podrá tener un appliance en un sitio alternativo (físico o virtual) que pueda servir como recuperación de desastres (DRP)



**Referirse al documento:**

UVM Appliance User Guide\_pag 59-61.pdf

8.3.4. La solución del licitante deberá poder soportar alta disponibilidad activo/activo nativamente para dividir las cargas entre los appliances y utilizar ambas plataformas simultáneamente

La solución propuesta por **IQsec, S.A. de C.V.** podrá soportar alta disponibilidad activo/activo nativamente para dividir las cargas entre los appliances y utilizar ambas plataformas simultáneamente

**Referirse al documento:**

PBPS 6.2 Deployment and Failover\_pag 6-9.pdf

8.3.5. 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.

La solución propuesta por **IQsec, S.A. de C.V.** tendrá 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.

**Referirse al documento:**

BeyondInsight User Guide\_pag 56-57.pdf

BeyondInsight User Guide\_pag 83-84.pdf

8.3.6. La solución del licitante deberá poder detectar automáticamente nuevas credenciales privilegiados de

La solución propuesta por **IQsec, S.A. de C.V.** podrá detectar automáticamente nuevas credenciales





activos administrados de forma automática y hace cumplir la política de contraseñas para establecer estas nuevas credenciales

privilegiados de activos administrados de forma automática y hace cumplir la política de contraseñas para establecer estas nuevas credenciales

**Referirse al documento:**

Password Safe Administration Guide\_pag 108-115.pdf

8.3.7. La solución del licitante deberá ser compatible con la gestión de cuentas privilegiadas con nombre, ejemplo "usuario", "usuario.admin" y "usuario\_admin".

La solución propuesta por **IQsec, S.A. de C.V.** será compatible con la gestión de cuentas privilegiadas con nombre, ejemplo "usuario", "usuario.admin" y "usuario\_admin".

**Referirse al documento:**

Password Safe Administration Guide\_pag 112-113.pdf

8.3.8. 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

La solución propuesta por **IQsec, S.A. de C.V.** podrá 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

**Referirse al documento:**

BeyondInsight User Guide\_pag 221-227.pdf



8.3.9. 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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad de gestionar las cuentas con privilegios en los servidores con sistema operativo Windows Server 2008, 2008R2, 2012R2 y Server 2012

**Referirse al documento:**

ds-pbps-platform-support\_pag 1.pdf

8.3.10. 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.

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad de gestionar las cuentas con privilegios en los sistemas operativos para servidores Unix, Linux - Red Hat, SuSE, CentOS, Ubuntu, Debian, Solaris, etc.

**Referirse al documento:**

ds-pbps-platform-support\_pag 1.pdf

Password Safe Administration Guide\_pag 129-131.pdf

8.3.11. 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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad de gestionar las cuentas con privilegios en los sistemas de bases de datos Oracle, MySQL, MS-SQL

**Referirse al documento:**





ds-pbps-platform-support\_pag 1.pdf

8.3.12. 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.

La solución propuesta por **IQsec, S.A. de C.V.** será compatible con la gestión de las cuentas con privilegios para las aplicaciones Web como Facebook, Twitter, Instagram, LinkedIn, etc.

**Referirse al documento:**

Password Safe Administration Guide\_pag 85.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad de gestionar las cuentas con privilegios de activos de infraestructura de seguridad de la red.

**Referirse al documento:**

Password Safe Administration Guide\_pag 129-131.pdf

8.3.14. 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

La solución propuesta por **IQsec, S.A. de C.V.** contará con un asistente para la creación de conectores para ejecutar el cambio de contraseña en plataformas que no están en la lista predeterminada.

**Referirse al documento:**



Password Safe Administration Guide\_pag 129-131.pdf

8.3.15. 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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá 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.

**Referirse al documento:**

Password Safe Administration Guide\_pag 40-41.pdf

8.3.16. 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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá 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

**Referirse al documento:**

Password Safe Administration Guide\_pag 40-41.pdf

BreakGlass PBPS via Custom Platform and API\_pag 3-4.pdf

8.3.17. 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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá una herramienta de flujos de trabajo para la definición de aprobaciones para solicitar el acceso a las credenciales





notificación a los aprobadores vía e-mail y la notificación por parte del interfaz de la herramienta

privilegiadas, con notificación a los aprobadores vía e-mail y la notificación por parte del interfaz de la herramienta.

**Referirse al documento:**

Password Safe Administration Guide\_pag 22-24.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** podrá configurar un flujo de trabajo con el fin de tener dos o más aprobadores para liberar una contraseña.

**Referirse al documento:**

Password Safe Administration Guide\_pag 22-24.pdf

8.3.19. La solución del licitante deberá tener la posibilidad de permitir el acceso pre autorizados

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la posibilidad de permitir el acceso preautorizado

**Referirse al documento:**

Password Safe Administration Guide\_pag 22-24.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** podrá configurar un flujo de trabajo sincronizado para la gestión de proveedores y terceros.



**Referirse al documento:**

Password Safe Administration Guide\_pag 134-139.pdf

8.3.21. 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

La solución propuesta por **IQsec, S.A. de C.V.** será 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.

**Referirse al documento:**

Password Safe Administration Guide\_pag 45-46.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** soportará "passphrases" en la gestión de claves SSH.

**Referirse al documento:**

Password Safe Administration Guide\_pag 45-46.pdf

8.3.23. 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

La solución propuesta por **IQsec, S.A. de C.V.** ofrecerá conmutación para recuperación de clave a través de contraseñas en caso de problemas de conexión a través de llaves SSH.





**Referirse al documento:**

Password Safe Administration Guide\_pag 45-46.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** será compatible con el cambio de contraseñas (rotación) en los archivos de configuración web.config.

**Referirse al documento:**

BeyondInsight and Password Safe API User Guide\_pag 6.pdf

8.3.25. 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

Password Safe Administration Guide\_pag 156-160.pdf

La solución propuesta por **IQsec, S.A. de C.V.** tendrá 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.

**Referirse al documento:**

BeyondInsight and Password Safe API User Guide\_pag 6.pdf



8.3.26. 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

La solución propuesta por **IQsec, S.A. de C.V.** contendrá un mecanismo propio de caché para permitir que miles de peticiones por segundo no afecten el rendimiento de las aplicaciones.

**Referirse al documento:**

Password Safe Password Cache Guide\_pag 5.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** permitirá reproducir sesiones grabadas en la misma consola de gestión de contraseñas seguras

**Referirse al documento:**

Password Safe Administration Guide\_pag 60-61.pdf

8.3.28. 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

La solución propuesta por **IQsec, S.A. de C.V.** proporcionará 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.





**Referirse al documento:**

PBPS End User Guide\_pag 4-7.pdf

PBPS End User Guide\_pag 12-13.pdf

8.3.29. 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

La solución propuesta por **IQsec, S.A. de C.V.** será compatible con una conexión transparente a los activos en cuestión, sin que el usuario puede ver e introducir la contraseña para realizar una conexión.

**Referirse al documento:**

Password Safe Administration Guide\_pag 73-74.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** proporcionará la capacidad de soportar la conexión directa con el sistema Windows para los activos administrados.

**Referirse al documento:**

Password Safe Administration Guide\_pag 77-78.pdf

8.3.31. 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

La solución propuesta por **IQsec, S.A. de C.V.** podrá realizar la reproducción de vídeo, y con todo el acceso privilegiado que se lleva a cabo en un servidor específico.



**Referirse al documento:**

Password Safe Administration Guide\_pag 60-61.pdf

8.3.32. 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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá 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.

**Referirse al documento:**

Password Safe Administration Guide\_pag 60-61.pdf

8.3.33. 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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá 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.

**Referirse al documento:**

Password Safe Administration Guide\_pag 60-61.pdf

8.3.34. 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

La solución propuesta por **IQsec, S.A. de C.V.** podrá delegar el acceso a una aplicación específica (por ejemplo, MS-SQL Studio, Oracle Developer, consola de administración de Checkpoint, Facebook, etc.) a los





una sesión completa de SSH o RDP en un servidor en particular

usuarios, en lugar de dar una sesión completa de SSH o RDP en un servidor en particular.

**Referirse al documento:**

Password Safe Administration Guide\_pag 80-81.pdf

8.3.35. 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

La solución propuesta por IQsec, S.A. de C.V. permitirá 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.

**Referirse al documento:**

Password Safe Administration Guide\_pag 68-70.pdf

8.3.36. 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.

La solución propuesta por **IQsec, S.A. de C.V.** permitirá 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.

**Referirse al documento:**



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

Password Safe Administration Guide\_pag 68-70.pdf

La solución propuesta por **IQsec, S.A. de C.V.** permitirá a un usuario administrador terminar una sesión activa de forma remota.

**Referirse al documento:**

Password Safe Administration Guide\_pag 68-70.pdf

8.3.38. 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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá un mecanismo para auditar las sesiones abiertas por "fuera" de la caja de seguridad en los servidores de Windows.

**Referirse al documento:**

PowerBroker for Windows User Guide 7.4\_pag 103.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá mecanismo para auditar comandos privilegiados por "sudo" en Linux / Unix.

**Referirse al documento:**

PowerBroker\_Admin\_v10.0.1\_pag 35-41.pdf





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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá mecanismos para identificar cuáles son las vulnerabilidades de cada activo en la organización, debido a su configuración o software.

**Referirse al documento:**

BeyondInsight User Guide\_pag 58-72.pdf

8.3.41. 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.

La solución propuesta por **IQsec, S.A. de C.V.** permitirá la identificación de vulnerabilidades en Windows, Linux, Unix, Oracle, MS-SQL, dispositivos de red Cisco, Firewalls, Java, Adobe, etc.

**Referirse al documento:**

BeyondInsight User Guide\_pag 58-72.pdf

Retina OS Detection List\_pag 1-2.pdf

8.3.42. 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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá 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.



**Referirse al documento:**

BeyondInsight User Guide\_pag 61-62.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** contendrá reportes que indican las acciones para remediación de vulnerabilidades, ya sea a través de parches y/o ajustes.

**Referirse al documento:**

Report Book- BeyondInsight\_pag 143.pdf

8.3.44. 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

La solución propuesta por **IQsec, S.A. de C.V.** permitirá 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.

**Referirse al documento:**

BeyondInsight User Guide\_pag 139-141.pdf

8.3.45. 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

En la solución propuesta por **IQsec, S.A. de C.V.** 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.





**Referirse al documento:**

BeyondInsight and Password Safe API User Guide\_pag 6.pdf

8.3.46. 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.

La solución propuesta por **IQsec, S.A. de C.V.** proporcionará 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.

**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 1.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** podrá clasificar y evaluar dispositivos e instancias virtuales.

**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 2-3.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** permitirá monitorear continuamente los dispositivos a medida que entran y sales de la red.



**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 3.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** podrá implementarse fuera de banda en la red sin agregar latencia o un posible punto de falla de la red.

**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 3.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** permitirá, de manera enunciativa más no limitativa, rastrear y controlar usuarios, aplicaciones, procesos, puertos, dispositivos externos.

**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 3.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá un motor de informes integrado que permita controlar el nivel de cumplimiento de políticas, cumplir con requisitos de auditorías.





**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 3.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad de crear informes de inventario en tiempo real.

**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 3.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** podrá implementarse sin afectar a los usuarios o dispositivos.

**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 3.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad de crear políticas de seguridad que se adecuen a los lineamientos del Instituto FONACOT.

**Referirse al documento:**



ForeScout-CounterACT-Datasheet\_pag 3.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** podrá contar con plantillas, reglas e informes incorporados en las políticas, que permitan configurarse y administrarse.

**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 3.pdf

8.3.56. 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.

La solución propuesta por **IQsec, S.A. de C.V.** podrá identificar, clasificar, autenticar y controla el acceso a la red sin un agente. Realice una inspección profunda del punto final sin un agente.

**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 4.pdf

8.3.57. 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

La solución propuesta por **IQsec, S.A. de C.V.** podrá identificar automáticamente las infracciones de las políticas, remediar las deficiencias de seguridad de los puntos finales y medir el cumplimiento de lo reglamentado.

**Referirse al documento:**





ForeScout-CounterACT-Datasheet\_pag 4.pdf

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

La solución propuesta por **IQsec, S.A. de C.V.** podrá detectar dispositivos sin direcciones IP, como dispositivos de captura de paquetes.

**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 4.pdf

8.3.59. La solución deberá garantizar que las personas correctas con los dispositivos adecuados tengan acceso a los recursos de red apropiados

La solución propuesta por **IQsec, S.A. de C.V.** garantizará que las personas correctas con los dispositivos adecuados tengan acceso a los recursos de red apropiados.

**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 4.pdf

8.3.60. 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

La solución propuesta por **IQsec, S.A. de C.V.** resolverá 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.

**Referirse al documento:**



ForeScout-CounterACT-Datasheet\_pag 4.pdf

8.3.61. La solución deberá poder utilizar 802.1X u otras tecnologías de autenticación como LDAP, Active Directory, RADIUS, Oracle y Sun

La solución propuesta por **IQsec, S.A. de C.V.** podrá utilizar 802.1X u otras tecnologías de autenticación como LDAP, Active Directory, RADIUS, Oracle y Sun.

**Referirse al documento:**

ForeScout-CounterACT-Datasheet\_pag 4.pdf

8.3.62. La solución deberá instrumentar inteligencia de fuentes abiertas accionables con contexto del país, inteligencia de amenazas incluyendo direcciones IP, dominios, URLs y hashes

La solución propuesta por **IQsec, S.A. de C.V.** instrumentará inteligencia de fuentes abiertas accionables con contexto del país, inteligencia de amenazas incluyendo direcciones IP, dominios, URLs y hashes.

**Referirse al documento:**

DatasheetAugurio\_pag 2.pdf

8.3.63. La solución deberá de clasificar por medio de algoritmos de reducción del ruido y añejamiento de los alimentadores de inteligencia de amenazas tanto dinámico como cuantitativo.

La solución propuesta por **IQsec, S.A. de C.V.** clasificará por medio de algoritmos de reducción del ruido y añejamiento de los alimentadores de inteligencia de amenazas tanto dinámico como cuantitativo.

**Referirse al documento:**





DatasheetAugurio\_pag 6.pdf

8.3.64. La solución deberá proporcionar geolocalización de amenazas e información de infraestructura de los adversarios potenciales

La solución propuesta por **IQsec, S.A. de C.V.** proporcionará geolocalización de amenazas e información de infraestructura de los adversarios potenciales.

**Referirse al documento:**

DatasheetAugurio\_pag 7.pdf.

8.3.65. La solución deberá de tener capacidad de clasificar amenazas de IoT para tener visibilidad de las últimas tendencias y vectores de explotación

La solución propuesta por **IQsec, S.A. de C.V.** tendrá capacidad de clasificar amenazas de IoT para tener visibilidad de las últimas tendencias y vectores de explotación.

**Referirse al documento:**

DatasheetAugurio\_pag 4.pdf

8.3.66. La solución deberá de tener monitores históricos que permita la visualización y analice cambios en el nivel de riesgo de la infraestructura adversaria para mejorar la toma de decisiones

La solución propuesta por **IQsec, S.A. de C.V.** tendrá monitores históricos que permita la visualización y analice cambios en el nivel de riesgo de la infraestructura adversaria para mejorar la toma de decisiones.

**Referirse al documento:**



DatasheetAugurio\_pag 6.pdf

8.3.67. La solución deberá de categorizar las amenazas por malware, exploits, spam, atacantes comprometidos, IoT, fraude, malware móvil, shellcode, troyanos, gusanos, ataques emergentes, dos, ddos, específicos para clientes web, específicos para servidores web, específicos para aplicaciones web, y políticas maliciosas o sospechosas

La solución propuesta por **IQsec, S.A. de C.V.** categorizará las amenazas por malware, exploits, spam, atacantes comprometidos, IoT, fraude, malware móvil, shellcode, troyanos, gusanos, ataques emergentes, dos, ddos, específicos para clientes web, específicos para servidores web, específicos para aplicaciones web, y políticas maliciosas o sospechosas.

**Referirse al documento:**

DatasheetAugurio\_pag 7.pdf

8.3.68. La solución deberá de monitorizar al menos las siguientes operaciones y campañas en el país cryptowall, locky, teslacrypt, torrentlocker, dyre, geodo, hesperbot, necurs, pushdo, ramnit, suppobox, simda, banjori, tinba, palevo, ursnif, andromeda, betabot, spyeye, y Zeus así como diversos C2.

La solución propuesta por **IQsec, S.A. de C.V.** monitoreará al menos las siguientes operaciones y campañas en el país cryptowall, locky, teslacrypt, torrentlocker, dyre, geodo, hesperbot, necurs, pushdo, ramnit, suppobox, simda, banjori, tinba, palevo, ursnif, andromeda, betabot, spyeye, y Zeus, así como diversos C2.

**Referirse al documento:**

DatasheetAugurio\_pag 7.pdf





8.3.69. La solución deberá de presentar notas descriptivas de los indicadores de amenazas, fecha de detección y recomendaciones para el Curso de Acción donde aplique.

La solución propuesta por **IQsec, S.A. de C.V.** presentará notas descriptivas de los indicadores de amenazas, fecha de detección y recomendaciones para el Curso de Acción donde aplique.

**Referirse al documento:**

DatasheetAugurio\_pag 4.pdf.

8.3.70. La solución deberá de aplicar dentro de la inteligencia táctica modelos de ciber inteligencia de amenazas para proteger las redes y dar conciencia situacional como es el alineamiento de indicadores a Cadena de Progresión de la Amenaza, con mapas de calor por fases y visualizaciones de treemaps en cada una de las fases donde se presente el volumen de indicadores, la criticidad, el servicio atacado y el indicador de la amenaza.

La solución propuesta por **IQsec, S.A. de C.V.** aplicará dentro de la inteligencia táctica modelos de ciber inteligencia de amenazas para proteger las redes y dar conciencia situacional como es el alineamiento de indicadores a Cadena de Progresión de la Amenaza, con mapas de calor por fases y visualizaciones de treemaps en cada una de las fases donde se presente el volumen de indicadores, la criticidad, el servicio atacado y el indicador de la amenaza.

**Referirse al documento:**

DatasheetAugurio\_pag 7.pdf.

8.3.71. La solución clasificará automáticamente los indicadores alineándolos a Cadena de Progresión de la Amenaza y permitirá la reclasificación de los mismos.

La solución propuesta por **IQsec, S.A. de C.V.** clasificará automáticamente los indicadores alineándolos a Cadena de Progresión de la Amenaza y permitirá la reclasificación de los mismos.



**Referirse al documento:**

DatasheetAugurio\_pag 6.pdf

8.3.72. La solución permitirá la carga masiva de indicadores de manera manual para clasificarlos con Cadena de Progresión de la Amenaza.

La solución propuesta por **IQsec, S.A. de C.V.** permitirá la carga masiva de indicadores de manera manual para clasificarlos con Cadena de Progresión de la Amenaza.

**Referirse al documento:**

DatasheetAugurio\_pag 2.pdf

8.3.73. La solución desplegará el número de indicadores agrègados, indicadores pre clasificados e indicadores modificados por el analista.

La solución propuesta por **IQsec, S.A. de C.V.** desplegará el número de indicadores agrègados, indicadores pre clasificados e indicadores modificados por el analista.

**Referirse al documento:**

DatasheetAugurio\_pag 2.pdf

8.3.74. La solución deberá de presentar reportes con visualizaciones de líneas de tiempo gráfica por fase de la Cadena de Progresión de la Amenaza representando gráficamente los indicadores por criticidad.

La solución propuesta por **IQsec, S.A. de C.V.** presentará reportes con visualizaciones de líneas de tiempo gráfica por fase de la Cadena de Progresión de la Amenaza representando gráficamente los indicadores por criticidad.

98





**Referirse al documento:**

DatasheetAugurio\_pag 6-7.pdf

8.3.75. La solución deberá de poder ejecutar consultas, pivotear o enriquecer indicadores primitivos para hacer triaje de amenazas.

La solución propuesta por **IQsec, S.A. de C.V.** podrá ejecutar consultas, pivotear o enriquecer indicadores primitivos para hacer triaje de amenazas.

**Referirse al documento:**

DatasheetAugurio\_pag 2.pdf

DatasheetAugurio\_pag 6.pdf

8.3.76. La solución deberá de presentar reportes alineados a Cadena de Progresión de la Amenaza de manera logarítmica para mejorar la visualización de indicadores, riesgo y fases.

La solución propuesta por **IQsec, S.A. de C.V.** presentará reportes alineados a Cadena de Progresión de la Amenaza de manera logarítmica para mejorar la visualización de indicadores, riesgo y fases.

**Referirse al documento:**

DatasheetAugurio\_pag 6.pdf.

8.3.77. La solución deberá de tener capacidad de la generación de monitores para detección de cambios de comportamiento, riesgo y compromiso de manera dinámica en las

La solución propuesta por **IQsec, S.A. de C.V.** tendrá capacidad de la generación de monitores para detección de cambios de comportamiento, riesgo y compromiso de manera dinámica en las organizaciones por medio de



organizaciones por medio de indicadores primitivos como direcciones IP, dominios y URLs.

indicadores primitivos como direcciones IP, dominios y URLs.

**Referirse al documento:**

DatasheetAugurio\_pag 2.pdf

DatasheetAugurio\_pag 6.pdf

8.3.78. La solución deberá de permitir la carga de inteligencia manual para complementar el proceso de investigación o respuesta a incidentes y se retroalimente de los servicios de inteligencia y DFIR.

La solución propuesta por **IQsec, S.A. de C.V.** permitirá la carga de inteligencia manual para complementar el proceso de investigación o respuesta a incidentes y se retroalimente de los servicios de inteligencia y DFIR.

**Referirse al documento:**

DatasheetAugurio\_pag 2.pdf

8.3.79. La solución deberá de permitir la carga de inteligencia automática por medio de colectores para automatizar el proceso de investigación o respuesta a incidentes.

La solución propuesta por **IQsec, S.A. de C.V.** permitirá la carga de inteligencia automática por medio de colectores para automatizar el proceso de investigación o respuesta a incidentes.

**Referirse al documento:**

DatasheetAugurio\_pag 2.pdf





8.3.80. Los colectores deberán de monitorizarse para determinar el estatus de conectividad y alertar en caso de pérdida de conectividad.

Los colectores de la solución propuesta por **IQsec, S.A. de C.V.** se monitorizarán para determinar el estatus de conectividad y alertar en caso de pérdida de conectividad.

**Referirse al documento:**

DatasheetAugurio\_pag 9.pdf

8.3.81. La comunicación entre el sensor y el controlador deberá de ser cifrada para conservar la confidencialidad de la información transmitida.

La comunicación entre el sensor y el controlador de la solución propuesta por **IQsec, S.A. de C.V.** será cifrada para conservar la confidencialidad de la información transmitida.

**Referirse al documento:**

DatasheetAugurio\_pag 9.pdf

8.3.82. La solución deberá de dar inteligencia operativa por medio de APIs y tener un histórico de clasificación de riesgo por indicador.

La solución propuesta por **IQsec, S.A. de C.V.** dará inteligencia operativa por medio de APIs y tendrá un histórico de clasificación de riesgo por indicador.

**Referirse al documento:**

DatasheetAugurio\_pag 6.pdf

8.3.83. La solución deberá de presentar un resumen con mapa de palabras, para que visualmente el analista tenga contexto

La solución propuesta por **IQsec, S.A. de C.V.** presentará un resumen con mapa de palabras, para que visualmente el



antes de abordar el detalle de los indicadores de amenazas.

analista tenga contexto antes de abordar el detalle de los indicadores de amenazas.

**Referirse al documento:**

DatasheetAugurio\_pag 6.pdf

8.3.84. La solución deberá de presentar y alinearse con el modelo integral de servicios para la generación de la estrategia de inteligencia por cliente o vertical, así como visualización de los indicadores por sector.

La solución propuesta por **IQsec, S.A. de C.V.** presentará y se alineará con el modelo integral de servicios para la generación de la estrategia de inteligencia por cliente o vertical, así como visualización de los indicadores por sector.

**Referirse al documento:**

DatasheetAugurio\_pag 6.pdf

8.3.85. La solución deberá de tener un mapa mundial donde visualmente se pueda hacer atribución de amenazas.

La solución propuesta por **IQsec, S.A. de C.V.** tendrá un mapa mundial donde visualmente se pueda hacer atribución de amenazas.

**Referirse al documento:**

DatasheetAugurio\_pag 7.pdf





8.3.86. La solución deberá de tener un mapa mundial donde visualmente se pueda hacer atribución de las conexiones realizadas para la detección anómala en un periodo determinado con los siguientes filtros:

- Top Talkers All Connections.
- All Connections Long Tail Analysis.
- Top Talkers Malicious.
- Malicious Long Tail Analysis

8.3.87. La solución presentará información de amenazas por país en un mapa de geolocalización por vertical con diversas categorías al menos con inteligencia de malware, troyanos, shellcode, p2p, TOR, reconocimiento, netbios, respuesta de ataques, amenazas en DNS, chat, y eventos disruptivos.

8.3.88. La solución deberá de integrarse y alinearse al Sistema Integral de Gestión de Inteligencia aplicado al ciber dominio

La solución propuesta por **IQsec, S.A. de C.V.** tendrá un mapa mundial donde visualmente se pueda hacer atribución de las conexiones realizadas para la detección anómala en un periodo determinado con los siguientes filtros:

- Top Talkers All Connections.
- All Connections Long Tail Analysis.
- Top Talkers Malicious.
- Malicious Long Tail Analysis

**Referirse al documento:**

DatasheetAugurio\_pag 7.pdf

La solución propuesta por **IQsec, S.A. de C.V.** presentará información de amenazas por país en un mapa de geolocalización por vertical con diversas categorías al menos con inteligencia de malware, troyanos, shellcode, p2p, TOR, reconocimiento, netbios, respuesta de ataques, amenazas en DNS, chat, y eventos disruptivos.

**Referirse al documento:**

DatasheetAugurio\_pag 7.pdf

La solución propuesta por **IQsec, S.A. de C.V.** se integrará y alineará al Sistema Integral de Gestión de Inteligencia



como parte de la habilitación estratégica de la tecnología a los procesos de negocio.

aplicado al ciber dominio como parte de la habilitación estratégica de la tecnología a los procesos de negocio.

**Referirse al documento:**

DatasheetAugurio\_pag 6.pdf

8.3.89. La solución deberá de integrarse y alinearse al Sistema de Gestión de Calidad de los Servicios de Soporte al Ciclo de Inteligencia aplicado al ciber dominio como parte de la habilitación estratégica de la tecnología a los procesos de negocio.

La solución propuesta por **IQsec, S.A. de C.V.** se integrará y alineará al Sistema de Gestión de Calidad de los Servicios de Soporte al Ciclo de Inteligencia aplicado al ciber dominio como parte de la habilitación estratégica de la tecnología a los procesos de negocio.

**Referirse al documento:**

DatasheetAugurio\_pag 6.pdf

8.3.90. La solución deberá de presentar información de los indicadores en la fase de explotación alineándolos con CVE, CPE, CWE, CAPEC, boletines de Microsoft, referenciación de exploits públicos relacionados con el intento de explotación, descripción, configuraciones vulnerables, referencias cruzadas con Metasploit, ExploitDB, Nessus, OVAL, Packetstorm, paquetes vulnerables de RedHat , SAINT, y Mitre.

La solución propuesta por **IQsec, S.A. de C.V.** presentará información de los indicadores en la fase de explotación alineándolos con CVE, CPE, CWE, CAPEC, boletines de Microsoft, referenciación de exploits públicos relacionados con el intento de explotación, descripción, configuraciones vulnerables, referencias cruzadas con Metasploit, ExploitDB, Nessus, OVAL, Packetstorm, paquetes vulnerables de RedHat , SAINT, y Mitre.





**Referirse al documento:**

DatasheetAugurio\_pag 4.pdf

8.3.91. La solución deberá contar con una API que permita obtener información operativa a través de consultas HTTP y la información deberá transmitirse por canales cifrados.

La solución propuesta por **IQsec, S.A. de C.V.** contará con una API que permita obtener información operativa a través de consultas HTTP y la información deberá transmitirse por canales cifrados.

**Referirse al documento:**

DatasheetAugurio\_pag 6.pdf

8.3.92. La solución deberá generar llaves de acceso para servidores y clientes que deseen realizar consultas a la API.

La solución propuesta por **IQsec, S.A. de C.V.** generará llaves de acceso para servidores y clientes que deseen realizar consultas a la API.

**Referirse al documento:**

DatasheetAugurio\_pag 6.pdf

8.3.93. La solución deberá poder modificar la cantidad de consultas diarias por cada cliente conectado a la API.

La solución propuesta por **IQsec, S.A. de C.V.** podrá modificar la cantidad de consultas diarias por cada cliente conectado a la API.

**Referirse al documento:**

DatasheetAugurio\_pag 6.pdf



8.3.94. La solución deberá poder modificar privilegios por cada cliente conectado a la API.

La solución propuesta por **IQsec, S.A. de C.V.** podrá modificar privilegios por cada cliente conectado a la API.

**Referirse al documento:**

DatasheetAugurio\_pag 6.pdf

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

Los artefactos contemplados en este esquema de solución propuesta por **IQsec, S.A. de C.V.** contendrán las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

**Referirse al documento:**

support-programs-at-a-glance.pdf

ForeScout\_ActiveCare-Maintenance-and-Support.pdf

Propuesta de mesa de ayuda\_pág 4.pdf





## 9. Servicio de Protección de Base de Datos

### 9.1 Descripción de Servicios

Implementar un esquema de fortalecimiento de seguridad informática, que evite que los datos en reposo sean explotados por aplicaciones o usuarios no autorizados. **IQsec, S.A. de C.V.**, asignará 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, implementará 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.

### 9.2 Descripción de Componentes

9.2.1. La solución deberá tener una capacidad mínima operativa por appliance de 500/1000/2000/5000/10000 Mbps de tráfico inspeccionado. La solución propuesta por **IQsec, S.A. de C.V.** tendrá una capacidad mínima operativa por appliance de 500/1000/2000/5000/10000 Mbps de tráfico inspeccionado.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

9.2.2. 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. La solución propuesta por **IQsec, S.A. de C.V.** soportará opciones de conectividad física como 1Gb Ethernet en UTP o



Fibra Óptica tipo SX, así como conectividad 10Gb en modos SR o LR.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

9.2.3. 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.

Las interfaces de conectividad a la red de la solución propuesta por **IQsec, S.A. de C.V.** serán 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.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

9.2.4. La solución deberá soportar el volumen de tráfico y deberá tener una latencia menor a 5ms, para no impactar el desempeño de las aplicaciones.

La solución propuesta por **IQsec, S.A. de C.V.** soportará el volumen de tráfico y deberá tener una latencia menor a 5ms, para no impactar el desempeño de las aplicaciones.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

9.2.5. La solución deberá tener al menos 1 GB de throughput.

La solución propuesta por **IQsec, S.A. de C.V.** tendrá al menos 1 GB de throughput.



9.2.6. La solución deberá tener de memoria al menos 30 GB DDR3.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

La solución propuesta por **IQsec, S.A. de C.V.** tendrá de memoria al menos 30 GB DDR3.

9.2.7. La solución deberá tener de almacenamiento en disco duro 2 TB.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

La solución propuesta por **IQsec, S.A. de C.V.** tendrá de almacenamiento en disco duro 2 TB.

9.2.8. La solución deberá contar con SSL Acceleration.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

La solución propuesta por **IQsec, S.A. de C.V.** contará con SSL Acceleration.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf





9.2.9. La solución deberá contar con Puerto serial, Puerto USB, Out-of-Band Port Management, Puerto IMPI.

La solución propuesta por **IQsec, S.A. de C.V.** contará con Puerto serial, Puerto USB, Out-of-Band Port Management, Puerto IMPI.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

9.2.10. La solución deberá contar con unidades de disco duro duales intercambiables (hot-swap).

La solución propuesta por **IQsec, S.A. de C.V.** contará con unidades de disco duro duales intercambiables (hot-swap).

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

9.2.11. La solución deberá mantener una latencia de <5ms.

La solución propuesta por **IQsec, S.A. de C.V.** mantendrá una latencia de <5ms.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

9.2.12. La solución deberá contar al menos con 5 segmentos de red.

La solución propuesta por **IQsec, S.A. de C.V.** contará al menos con 5 segmentos de red.

**Referirse al documento:**





DS\_SecureSphere\_Appliances - página 3.pdf

9.2.13. 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.

Cada consola de la solución propuesta por **IQsec, S.A. de C.V.** tendrá 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.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

9.2.14. Todos los elementos de la solución propuesta deben ser de la misma marca y fabricante.

Todos los elementos de la solución propuesta por **IQsec, S.A. de C.V.** serán de la misma marca y fabricante.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

9.2.15. La solución deberá tener como mínimo 12 GB de memoria.

La solución propuesta por **IQsec, S.A. de C.V.** tendrán como mínimo 12 GB de memoria.

**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

9.2.16. La solución deberá contar con 1 puerto serial, 2 interfaces de ethernet x 1GB, puerto IMPI de 1x10/100MB.

La solución propuesta por **IQsec, S.A. de C.V.** contará con 1 puerto serial, 2 interfaces de ethernet x 1GB, puerto IMPI de 1x10/100MB.



**Referirse al documento:**

DS\_SecureSphere\_Appliances - página 3.pdf

9.2.17. La solución deberá contar con administración mediante Secure Web, CLI, SOAP, REST.

La solución propuesta por **IQsec, S.A. de C.V.** contará con administración mediante Secure Web, CLI, SOAP, REST.

**Referirse al documento:**

Thales-eSecurity\_vormetric-data-security-platform-2\_pag 3.pdf

9.2.18. La solución deberá permitir dominios de administración.

La solución propuesta por **IQsec, S.A. de C.V.** permitirá dominios de administración.

**Referirse al documento:**

Thales-eSecurity\_vormetric-data-security-platform-2\_pag 4.pdf

9.2.19. La solución deberá soportar las API's, Microsoft Extensible Key Management (EKM), SOAP, REST.

La solución propuesta por **IQsec, S.A. de C.V.** soportará las API's, Microsoft Extensible Key Management (EKM), SOAP, REST.

**Referirse al documento:**



Thales-eSecurity\_vormetric-data-security-platform-2\_pag  
5.pdf

9.2.20. La solución deberá soportar administración mediante SNMP, NTP, Syslog-TCP.

La solución propuesta por **IQsec, S.A. de C.V.** soportará administración mediante SNMP, NTP, Syslog-TCP.

**Referirse al documento:**

Thales-eSecurity\_vormetric-data-security-platform-2\_pag  
5.pdf

9.2.21. La solución deberá permitir los formatos de syslogs CEF, LEEF and RFC 5424.

La solución propuesta por **IQsec, S.A. de C.V.** permitirá los formatos de syslogs CEF, LEEF and RFC 5424.

**Referirse al documento:**

Thales-eSecurity\_vormetric-data-security-platform-2\_pag  
5.pdf

9.2.22. La solución deberá cumplir con las certificaciones de FIPS 140-2 Level 1, FIPS 140-2 Level 2, FIPS 140-2 Level 3, Common Criteria (ESM PP PM V2.1).

La solución propuesta por **IQsec, S.A. de C.V.** cumplirá con las certificaciones de FIPS 140-2 Level 1, FIPS 140-2 Level 2, FIPS 140-2 Level 3, Common Criteria (ESM PP PM V2.1).

**Referirse al documento:**

Thales-eSecurity\_vormetric-data-security-platform-2\_pag  
5.pdf



9.2.23. La solución deberá contar con la capacidad de comprar el acceso de los usuarios por usuario y contraseña y por doble factor de autenticación.

La solución propuesta por **IQsec, S.A. de C.V.** contará con la capacidad de comprobar el acceso de los usuarios por usuario y contraseña y por doble factor de autenticación.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 17 de la empresa "IQSEC S.A. DE C.V." de la página 15 de 36 que a la letra dice:

*"Se le solicita amablemente a la convocante no ayude a precisar si la palabra "comprar" esta mal referenciada o si se refiere a la acción de garantizar el acceso?"*

*¿Es correcta nuestra apreciación?"*

**Es correcta su apreciación, el texto debé decir "comprobar" y esa deberá ser su entendimiento.**

**Referirse al documento:**

Thales-eSecurity\_vormetric-data-security-platform-2\_pag  
5.pdf

### 9.3 Descripción de Funcionalidades





9.3.1. 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.

La solución propuesta por **IQsec, S.A. de C.V.** contará 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.

**Referirse a los documentos:**

ImpervaSecureSphereAppliances- página 5.pdf

DS\_SecureSphere\_Data\_Security - página 4.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide\_página 426.pdf

Imperva Technical Brief - SecureSphere Platform Security - página 1.pdf"

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 428 a 432.pdf

9.3.2. 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.

La solución propuesta por **IQsec S.A. de C.V.**, proporcionará protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos,



actividad sospechosa o cualquier actividad específica a definir.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 31.pdf

9.3.3. 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.

La solución propuesta por **IQsec S.A. de C.V.**, soportará 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 visualizará alertas, ataques, errores de servidor y otra actividad no autorizada.
- En el modo de cumplimiento de políticas, la solución bloqueará ataques proactivamente.
- Respecto de algún ataque o alguna otra actividad no autorizada, la solución será capaz de tomar las acciones adecuadas. Las acciones deberán incluir la habilidad para





- 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.
- 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 será capaz de bloquear la dirección IP por un periodo de tiempo configurable.
  - En modo analizador de paquetes o sniffer, la solución será 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.

**Referirse a los documentos:**

Imperva-SecureSphere-v12.0-Administration-Guide-páginas 20 a 28.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 41.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 84.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 231.pdf



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

Imperva-SecureSphere-v12.0-Administration-Guide - página 21.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 500.pdf

La solución propuesta por **IQsec S.A. de C.V.** generará reportes y tendencias en tiempo real, así como permitirá la modificación de los mismos.

**Referirse a los documentos:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide- página 309.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 208.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 332- 333.pdf

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

La solución propuesta por **IQsec S.A. de C.V.**, contará con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente. Con referencia específica en el apartado del documento:

**Referirse al documento:**





Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 31.pdf

9.3.6. 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.

La solución propuesta por **IQsec S.A. de C.V.**, no requerirá el instalar agentes de software en los servidores a monitorear, pero si tendrá la opción en caso de ser necesario.

**Referirse al documento:**

DS\_SecureSphere\_Data\_Security-página 6.pdf

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

La solución propuesta por **IQsec S.A. de C.V.**, funcionará independiente a la activación de la auditoría nativa de la base de datos.

**Referirse a los documentos:**

Native\_Auditing\_Tools\_Performance.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 384.pdf

WP\_Imperva\_Hidden\_Costs\_Free\_DBAuditing - página 7.pdf

9.3.8. 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,

La solución propuesta por **IQsec S.A. de C.V.**, será transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen



configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.

cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.

**Referirse a los documentos:**

Imperva-SecureSphere-v12.0-Administration-Guide-página 22.pdf

Imperva-SecureSphere-v12.0-Administration-Guide - página 19.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 1180.pdf

9.3.9. 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.

El repositorio para el registro de la actividad en el appliance, propuesto por **IQsec S.A. de C.V.**, no será accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante o por medios administrativos debidamente asegurados.

**Referirse a los documentos:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 379.pdf

Imperva-SecureSphere-v12.0-Administration-Guide - página 226.pdf





9.3.10. 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.

9.3.11. 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

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 493.pdf

Imperva Technical Brief - SecureSphere Platform Security - página 2.pdf

La solución propuesta por IQsec S.A. de C.V., será 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.

**Referirse a los documentos:**

DS\_SecureSphere\_Data\_Security -página 2.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 241-242.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 53.pdf

La solución propuesta por IQsec S.A. de C.V., realizará 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.

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.

**Referirse a los documentos:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 40.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide- página 241-242.pdf

9.3.12. 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.

La solución propuesta por **IQsec S.A. de C.V.**, podrá 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.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 45.pdf

9.3.13. 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

La solución propuesta por **IQsec S.A. de C.V.**, tendrá la capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo con las políticas de negocio.





de tipo de dato deberán poder crearse de manera flexible y granular.

Las definiciones de tipo de dato podrán crearse de manera flexible y granular.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 58.pdf"

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 529 a 530.pdf"

9.3.14. 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.

La solución propuesta por **IQsec S.A. de C.V.**, proveerá 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.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 31.pdf

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

La solución propuesta por **IQsec S.A. de C.V.**, apoyará en los esfuerzos de detección e investigación de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y Control de cambios.



9.3.16. 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.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 31 a 33.pdf

La solución propuesta por **IQsec S.A. de C.V.**, monitoreará toda la actividad de las bases de datos, y almacenará los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.

**Referirse en los documentos:**

Imperva-SecureSphere-Datasheet-DBA.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 41.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide -página 1055.pdf

9.3.17. 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.

La solución propuesta por **IQsec S.A. de C.V.**, monitoreará e interactuará con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.

**Referirse al documento:**





Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 35.pdf

9.3.18. 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.

La solución propuesta por **IQsec S.A. de C.V.**, realizará 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.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 41.pdf

9.3.19. La solución deberá tener capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.

La solución propuesta por **IQsec S.A. de C.V.**, tendrá capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 137.pdf"

9.3.20. 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.

La solución propuesta por **IQsec S.A. de C.V.**, proveerá detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.



**Referirse a los documentos:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide-página 216

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 221.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide-página 222.pdf

9.3.21. 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.

La solución propuesta por **IQsec S.A. de C.V.**, manejará reglas y políticas tan amplias o granulares como se requieran y podrán ser construidas automáticamente o manualmente y podrán ser actualizadas, igualmente, de forma manual o automática.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 40.pdf

9.3.22. 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:

Las políticas granulares para control de acceso o generación de alertas propuestas por **IQsec S.A. de C.V.**, contarán 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 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
- 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, Instancia, Tabla y Columna accesada
  - Estado de autenticación de la sesión
  - Usuario y/o Grupo de Usuarios de Base de Datos conectado
  - Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB
  - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares)
  - Logins, Logouts, Queries
  - IPs de origen y destino
  - 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



- 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

- 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

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide – páginas 1041 a 1045.pdf

9.3.23. 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.

La solución propuesta por **IQsec S.A. de C.V.**, identificará 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.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide-página 434.pdf

28





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

La solución propuesta por **IQsec S.A. de C.V.**, posibilitará los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.

**Referirse al documento:**

DS\_SecureSphere\_Data\_Security-página 5.pdf

9.3.25. 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.

La solución propuesta por **IQsec S.A. de C.V.**, asociará y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son indicativos de una potencial violación de seguridad soportará e incluirá Geolocalización de direcciones IP.

**Referirse a los documentos:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide-página 274.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 1178.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 219.pdf

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

La solución propuesta por **IQsec S.A. de C.V.**, protegerá contra ataques SQL y no-SQL (como buffer overflow).



**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-  
página 291.pdf

9.3.27. 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.

La solución propuesta por **IQsec S.A. de C.V.**, correlacionará actividad en base de datos con actividad de aplicaciones web para entender detalladamente como los usuarios están accedendo datos privilegiados sin necesidad de alterar la aplicación web.

**Referirse a los documentos:**

Imperva-SecureSphere-v12.0-Database-Security-User-  
Guide -página 34.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-  
Guide-página 43.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-  
Guide- página 102.pdf

9.3.28. 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.

La solución propuesta por **IQsec S.A. de C.V.**, identificará ataques 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 desde una ubicación desconocida.
- Acceso a datos utilizando aplicaciones/herramientas no autorizadas.
- Acceso a datos inusual para cierta hora del día.
- Acceso a datos desde una ubicación desconocida.
- Acceso a datos utilizando aplicaciones/herramientas no autorizadas.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide-páginas 1009 a 1012.pdf

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

La solución propuesta por **IQsec S.A. de C.V.**, manejará una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide-página 348.pdf

9.3.30. 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).

La solución propuesta por **IQsec S.A. de C.V.**, tendrá facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP).

**Referirse al documento:**



Imperva-SecureSphere-v12.0-Database-Security-User-Guide- página 501. pdf

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

La solución propuesta por **IQsec S.A. de C.V.**, contará con Políticas, Reportes, Alertas, Objetos Sensibles y Transacciones preidentificadas y preconfiguradas para trabajar con las plataformas del Instituto FONACOT.

**Referirse a los documentos:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 35.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide- página 241 a 242.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide- página 295.pdf

9.3.32. 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.

La solución propuesta por **IQsec S.A. de C.V.**, tendrá la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.

**Referirse al documento:**



Imperva-SecureSphere-v12.0-Database-Security-User-Guide-página 233.pdf

9.3.33. 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.

La solución propuesta por **IQsec S.A. de C.V.**, analizará los eventos generados desde diferentes bases de datos. El análisis contemplará los siguientes criterios:

- Mostrará el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos.
- Contará 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.
- Realizará una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos.
- Ejecutará 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.
- Correlacionará eventos como número de errores inusuales de sentencias de SQL o al momento de hacer login a las bases de datos.

Referirse a los documentos:



Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 31.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 216 a 217.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 220

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 274.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 229.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 403 a 404.pdf

TB\_Universal\_User\_Tracking - página 1.pdf

TB\_Universal\_User\_Tracking -página 2.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 293.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 358.pdf

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

La solución propuesta por **IQsec S.A. de C.V.**, permitirá el manejo de alarmas y notificaciones –en tiempo real– para los eventos de correlación mencionados anteriormente.

**Referirse al documento:**





9.3.35. 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.

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 41.pdf

La solución propuesta por **IQsec S.A. de C.V.**, tendrá 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.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide- página 102.pdf

9.3.36. 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.

La solución propuesta por **IQsec S.A. de C.V.**, contará con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide- página 39.pdf

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

La solución propuesta por **IQsec S.A. de C.V.**, soportará y aplicará simultáneamente un modelo de seguridad positivo y negativo.

Handwritten signature or initials in blue ink.



**Referirse a los documentos:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 40.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 275.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 281.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 294.pdf

9.3.38. 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.

El modelo negativo de seguridad propuesto por **IQsec S.A. de C.V.**, define explícitamente las firmas de ataques conocidos y además cumplir con las siguientes especificaciones.

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





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

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

**Referirse a los documentos:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 40.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 275.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 281.pdf

Imperva-SecureSphere-v12.0-Database-Security-User-Guide - página 294.pdf

9.3.39. 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.

La solución propuesta por **IQsec S.A. de C.V.**, soportará 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.



**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide- página 779.pdf

9.3.40. 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.

La solución propuesta por **IQsec, S.A. de C.V.** proporcionará un proceso de instalación, actualización y gestión de cambios centralizada, seguro y ágil para los Agentes; el cual debe proporcionar una visión completa de todas las actualizaciones disponibles para los componentes de la solución de protección de Bases de Datos.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide- página 156.pdf

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

La solución propuesta por **IQsec S.A. de C.V.**, notificará cuando se encuentre disponible una nueva versión de Agente.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide- página 156.pdf

9.3.42. El despliegue y la instalación centralizada de parches y actualizaciones a componentes solo deberá ser realizada

El despliegue y la instalación centralizada de parches y actualizaciones a componentes propuestos por **IQsec S.A.**





por usuarios con los privilegios necesarios y administradores de la herramienta.

de C.V., serán realizadas por usuarios con los privilegios necesarios y administradores de la herramienta.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide-página 158.pdf

9.3.43. 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.

La solución propuesta por **IQsec S.A. de C.V.**, proporcionará 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.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide-página 742 y 743.pdf

9.3.44. 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.

La solución propuesta por **IQsec S.A. de C.V.**, contará con la opción de reducir el tráfico entre la comunicación entre el Agente y el Gateway utilizando métodos de comprensión de datos.

**Referirse al documento:**



Imperva-SecureSphere-v12.0-Database-Security-User-Guide-página 742.pdf

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

La solución propuesta por **IQsec S.A. de C.V.**, proporcionará la opción de enmascarar la información personal que se despliega a través de la interfaz de administración, además deberá contar con la opción de desenmascarar esta información dependiendo los privilegios de cada usuario.

**Referirse al documento:**

Imperva-SecureSphere-v12.0-Database-Security-User-Guide-página 211.pdf

9.3.46. La solución deberá contar con la funcionalidad del cifrado, protección, monitoreo y administración de llaves de cifrado de los archivos de las bases de datos, así como la administración de la política de acceso a los mismos, tanto de los usuarios regulares (no privilegiados) mediante su integración con el servicio de directorio activo y LDAP, como de los usuarios privilegiados.

La solución propuesta por **IQsec, S.A. de C.V.** contará con la funcionalidad del cifrado, protección, monitoreo y administración de llaves de cifrado de los archivos de las bases de datos, así como la administración de la política de acceso a los mismos, tanto de los usuarios regulares (no privilegiados) mediante su integración con el servicio de directorio activo y LDAP, como de los usuarios privilegiados; considerando 15 servidores para la implementación de la solución.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 18 de la





empresa "IQSEC S.A. DE C.V." de la página 16 de 36 que a la letra dice:

*"Se le solicita amablemente a la convocante nos ayude a definir para cuantos servidores requiere el cifrado.*

*Lo anterior para precisar de mejor manera el dimensionamiento del servicio."*

**Se deberán considerar 15 servidores en los cuales se requiera el servicio de cifrado.**

**Referirse al documento:**

Vormetric Brochure pág. 1, 2, 8 y 9.pdf

9.3.47. La solución deberá minimizar la ocurrencia de incidentes internos de seguridad mediante monitoreo de la actividad de los usuarios privilegiados sobre los archivos de las bases de datos.

La solución propuesta por **IQsec, S.A. de C.V.** minimizará la ocurrencia de incidentes internos de seguridad mediante monitoreo de la actividad de los usuarios privilegiados sobre los archivos de las bases de datos.

**Referirse al documento:**

Vórmetric Brochure pág. 1 y 6.pdf

9.3.48. La solución deberá establecer control de acceso para diferentes tipos de usuarios, e identificar actividades sospechosas mediante la generación de bitácoras sobre los archivos.

La solución propuesta por **IQsec, S.A. de C.V.** establecerá control de acceso para diferentes tipos de usuarios, e identificar actividades sospechosas mediante la generación de bitácoras sobre los archivos.



**Referirse al documento:**

Plataforma de seguridad de datos de Vormetric pág 1, 2 y 3.pdf

9.3.49. La solución propuesta deberá establecer un esquema de protección a la información de tal forma de que la misma se encuentre debidamente cifrada en el sistema de archivos. De esta forma además de prevenir una extracción no autorizada, aun en el caso de una pérdida accidental de un archivo con los datos, los mismos no podrán ser accedidos fuera del ámbito de la plataforma de seguridad.

La solución propuesta por **IQsec, S.A. de C.V.** establecerá un esquema de protección a la información de tal forma de que la misma se encuentre debidamente cifrada en el sistema de archivos. De esta forma además de prevenir una extracción no autorizada, aun en el caso de una pérdida accidental de un archivo con los datos, los mismos no podrán ser accedidos fuera del ámbito de la plataforma de seguridad.

**Referirse al documento:**

Plataforma de seguridad de datos de Vormetric pág 1, 265, 266 y 267.pdf

9.3.50. La solución propuesta deberá establecer esquemas de prevención de infecciones o ataques en los archivos de las bases de datos o asociados relacionadas con código malicioso tipo malware, de ataques generados por el acceso no autorizado a las tablas de las bases de datos, modificaciones a librerías o cualquier.

La solución propuesta por **IQsec, S.A. de C.V.** establecerá esquemas de prevención de infecciones o ataques en los archivos de las bases de datos o asociados relacionadas con código malicioso tipo malware, de ataques generados por el acceso no autorizado a las tablas de las bases de datos, modificaciones a librerías o cualquier.





**Referirse al documento:**

Vormetric Enhances.pdf

9.3.51. La solución propuesta deberá contar con un esquema de protección de datos flexible y escalable, previsto para cumplimiento de normativas de seguridad del tipo PCI y el marco de la Ley de Protección de Datos Personales, que permita proteger dentro de los sistemas de archivos que contengan datos estructurados (bases de datos) y no estructurados (incluyendo archivos de aplicaciones Microsoft, voz, video, y texto en general) en un ambiente heterogéneo de sistemas operativos y plataformas de operación. Este entorno debe soportar al menos ambientes de operación de Microsoft Windows Server y Linux. Las bases de datos soportadas deben incluir Oracle, MS-SQL, MySQL, Mongo DB, y Hadoop Distributed File System. Todo esto con una sola consola de gestión para facilitar el proceso de administración y control de la solución.

La solución propuesta por **IQsec, S.A. de C.V.** contará con un esquema de protección de datos flexible y escalable, previsto para cumplimiento de normativas de seguridad del tipo PCI y el marco de la Ley de Protección de Datos Personales, que permita proteger dentro de los sistemas de archivos que contengan datos estructurados (bases de datos) y no estructurados (incluyendo archivos de aplicaciones Microsoft, voz, video, y texto en general) en un ambiente heterogéneo de sistemas operativos y plataformas de operación. Este entorno debe soportar al menos ambientes de operación de Microsoft Windows Server y Linux. Las bases de datos soportadas deben incluir Oracle, MS-SQL, MySQL, Mongo DB, y Hadoop Distributed File System. Todo esto con una sola consola de gestión para facilitar el proceso de administración y control de la solución.

**Referirse al documento:**

Vormetric Data Security Architecture pág 1 a la 6.pdf

Vormetric Brochure pág 1, 6 y 7.pdf

9.3.52. La solución propuesta deberá contar con una consola de administración que permita la gestión centralizada de todos los agentes de cifrado a ser instalados en los servidores de bases de datos, sus llaves de cifrado y la configuración,

La solución propuesta por **IQsec, S.A. de C.V.** contará con una consola de administración que permita la gestión centralizada de todos los agentes de cifrado a ser instalados en los servidores de bases de datos, sus llaves de cifrado y



publicación y gestión de políticas de acceso de los archivos a ser protegidos.

la configuración, publicación y gestión de políticas de acceso de los archivos a ser protegidos.

**Referirse al documento:**

Vormetric Brochure pág 1 y 3.pdf

Plataforma de seguridad de datos de Vormetric pág 1 y 116.pdf

9.3.53. La consola de la solución propuesta deberá poder configurarse en un esquema de alta disponibilidad teniendo una primaria y una secundaria.

La consola de la solución propuesta por **IQsec, S.A. de C.V.** estará configurada en un esquema de alta disponibilidad desde el inicio de contrato y durante toda su vigencia teniendo dos consolas una consola primaria y una secundaria.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 8 de la empresa "IQSEC S.A. DE C.V." de la página 13 de 36 que a la letra dice:

*"Se le solicita amablemente a la convocante nos ayude a precisar si es correcto entender que por las configuraciones mencionadas en los alcances del servicio y por el numeral 9.3.53 es correcto entender que la solución tecnológica ofertada para la prestación del servicio deberá ser instalada en alta disponibilidad desde el inicio el contrato ¿Es correcta nuestra apreciación?"*





**Respuesta de la Convocante: "Si es correcta su apreciación, la solución ofertada por el licitante deberá estar configurada e instalada en todo momento en HA desde el inicio del contrato y seguir durante toda la vigencia del contrato."**

**Referirse al documento:**

Plataforma de seguridad de datos de Vormetric pág 1, 107, 108 y 109.pdf

9.3.54. La solución propuesta deberá soportar la incorporación de múltiples consolas adicionales para efectos de configurar esquemas de tolerancia a fallas multi-nivel.

La solución propuesta por **IQsec, S.A. de C.V.** soportará la incorporación de múltiples consolas adicionales para efectos de configurar esquemas de tolerancia a fallas multi-nivel.

**Referirse al documento:**

Plataforma de seguridad de datos de Vormetric pág 1, 107, 108 y 109.pdf

9.3.55. Los agentes de la solución propuesta deberán operar de manera autónoma a la consola de gestión con excepción de las instancias de su inicialización (boot) en los servidores, cambio de políticas en la consola, o cambios en la llave de cifrado con el fin de maximizar su up-time. Estos deben operar de manera ininterrumpida incluso si las consolas son apagadas.

Los agentes de la solución propuesta por **IQsec, S.A. de C.V.** operara de manera autónoma a la consola de gestión con excepción de las instancias de su inicialización (boot) en los servidores, cambio de políticas en la consola, o cambios en la llave de cifrado con el fin de maximizar su up-time. Estos deben operar de manera ininterrumpida incluso si las consolas son apagadas.



**Referirse al documento:**

Arquitectura de seguridad de datos de Vormetric pág 1 y 6.pdf

9.3.56. El detalle de las llaves de cifrado de la solución propuesta no deberá ser publicado para los usuarios del sistema, de tal forma de que el algoritmo de cifrado no pueda ser conocido por los usuarios de la plataforma. Este debe ser almacenado de manera segura en un hardware dedicado a servicios de seguridad dentro de la consola.

El detalle de las llaves de cifrado de la solución propuesta por **IQsec, S.A. de C.V.** no será publicado para los usuarios del sistema, de tal forma de que el algoritmo de cifrado no pueda ser conocido por los usuarios de la plataforma. Este debe ser almacenado de manera segura en un hardware dedicado a servicios de seguridad dentro de la consola.

**Referirse al documento:**

Vormetric Brochure pág 1, 6, 11 y 14.pdf

9.3.57. La consola de la solución propuesta deberá tener la posibilidad de ser servidor de llaves bajo el estándar KMIP de OASIS.

La consola de la solución propuesta por **IQsec S.A de C.V** cuenta con la posibilidad de ser servidor de llaves bajo el estándar KMIP de OASIS.

**Referirse al documento:**

Vormetric Brochure pág 1 y 12.pdf

9.3.58. La solución propuesta deberá ser compatible con API PKCS#11 y administración extensible de claves de Microsoft.

La solución propuesta por **IQsec, S.A. de C.V.** será compatible con API PKCS#11 y administración extensible de claves de Microsoft.

Handwritten signature or initials.





9.3.59. La solución propuesta deberá poder soportar certificados digitales (X.509) PKCS#7, PKCS#8, y PKCS#12, claves de cifrado simétrico (algoritmos 3DES, AES128, AES256, ARIA128 y ARIA256) y asimétricas (algoritmos RSA1024, RSA2048, RSA4096).

**Referirse al documento:**

Vormetric Brochure pág 1 y 12.pdf

La solución propuesta por **IQsec, S.A. de C.V.** podrá soportar certificados digitales (X.509) PKCS#7, PKCS#8, y PKCS#12, claves de cifrado simétrico (algoritmos 3DES, AES128, AES256, ARIA128 y ARIA256) y asimétricas (algoritmos RSA1024, RSA2048, RSA4096).

9.3.60. La solución propuesta deberá ser escalable para soportar la gestión de múltiples agentes de múltiples servicios en una estructura multi-tenencia, y con soporte de configuración de múltiples dominios de seguridad. Para ello se deben poder configurar diferentes llaves de cifrado en función para cada área de operación de en el caso de ser requerido.

**Referirse al documento:**

Vormetric Brochure pág 1 y 12.pdf

La solución propuesta por **IQsec, S.A. de C.V.** será escalable para soportar la gestión de múltiples agentes de múltiples servicios en una estructura multi-tenencia, y con soporte de configuración de múltiples dominios de seguridad. Para ello se deben poder configurar diferentes llaves de cifrado en función para cada área de operación de en el caso de ser requerido.

9.3.61. La solución propuesta deberá habilitar la separación de funciones de tal forma de que el usuario del sistema pueda crear las llaves de cifrado, otro usuario distinto las pueda

**Referirse al documento:**

Vormetric Brochure pág 1, 4 y 5.pdf

La solución propuesta por **IQsec, S.A. de C.V.** habilitará la separación de funciones de tal forma de que el usuario del sistema pueda crear las llaves de cifrado, otro usuario distinto



aplicar, y otro distinto a los anteriores pueda monitorear los mismos.

las pueda aplicar, y otro distinto a los anteriores pueda monitorear los mismos.

**Referirse al documento:**

Plataforma de seguridad de datos de Vormetric pág 240,241 y 242.pdf

9.3.62. La consola de la solución propuesta deberá ser administrable vía interface web.

La consola de la solución propuesta por **IQsec, S.A. de C.V.** será administrable vía interface web.

**Referirse al documento:**

Vormetric Brochure pág 1 y 3.pdf

9.3.63. La solución propuesta deberá contar con autenticación por usuario y contraseña y opcionalmente de dos factores RSA.

La solución propuesta por **IQsec, S.A. de C.V.** contará con autenticación por usuario y contraseña y opcionalmente de dos factores RSA.

**Referirse al documento:**

Vormetric Brochure pág 1 y 5.pdf

9.3.64. La solución propuesta deberá poder configurar las copias de respaldo de su configuración de manera automática o manual.

La solución propuesta por **IQsec, S.A. de C.V.** podrá configurar las copias de respaldo de su configuración de manera automática o manual.

**Referirse al documento:**

Vormetric Brochure pág 1 y 5.pdf





9.3.65. El proceso de cifrado de la solución propuesta deberá llevar a cabo mediante agentes que se instalarán en los servidores de bases de datos.

El proceso de cifrado de la solución propuesta por **IQsec, S.A. de C.V.** llevará a cabo mediante agentes que se instalarán en los servidores de bases de datos.

**Referirse al documento:**

Plataforma de seguridad de datos de Vormetric pág 1, 11, 12 y 26.pdf

Arquitectura de seguridad de datos de Vormetric pág 1 y 6.pdf

9.3.66. Estos agentes de la solución propuesta deberán soportar sistemas operativos Microsoft, UNIX (IBM AIX) y/o Linux.

Estos agentes de la solución propuesta por **IQsec, S.A. de C.V.** soportará sistemas operativos Microsoft, UNIX (IBM AIX) y/o Linux.

**Referirse al documento:**

Vormetric Brochure pág 1 y 6.pdf

9.3.67. La solución propuesta deberá tener agentes compatibles con bases de datos estructuradas y no estructuradas, incluyendo MS-SQL Server, Oracle, NoSQL, MySQL, Mongo DB y Hadoop Distributed File System.

La solución propuesta por **IQsec, S.A. de C.V.** tendrá agentes compatibles con bases de datos estructuradas y no estructuradas, incluyendo MS-SQL Server, Oracle, NoSQL, MySQL, Mongo DB y Hadoop Distributed File System.

**Referirse al documento:**

Vormetric Brochure pág 1 y 6.pdf



9.3.68. Los agentes de la solución deberán poder se instalados tanto en servidores físicos como en versiones virtuales.

Los agentes de la solución propuesta por **IQsec, S.A. de C.V.** podrán se instalados tanto en servidores físicos como en versiones virtuales.

**Referirse al documento:**

Vormetric Brochure pág 1 y 6.pdf

9.3.69. La instalación de los agentes no deberá requerir cambio alguno en las aplicaciones o definición de campos de la base de datos.

La instalación de los agentes de la solución propuesta por **IQsec, S.A. de C.V.** no requerirán cambio alguno en las aplicaciones o definición de campos de la base de datos.

**Referirse al documento:**

Vormetric Brochure pág 1 y 6.pdf

9.3.70. Los agentes deberán utilizar las prestaciones de aceleración disponibles en los servidores, del tipo AES-NI. La implementación de los mismos no deberá generar una sobre carga típica incremental en los servidores de más del 5%.

Los agentes de la solución propuesta por **IQsec, S.A. de C.V.** utilizarán las prestaciones de aceleración disponibles en los servidores, del tipo AES-NI. La implementación de los mismos no deberá generar una sobre carga típica incremental en los servidores de más del 5%.

**Referirse al documento:**

Vormetric Brochure pág 1 y 6.pdf

9.3.71. Los agentes de la solución propuesta deberán poder cifrar cualquier archivo, volumen o directorio de los servidores donde se encuentren instalados de tal forma de que puedan proteger información estructurada y no-estructurada (por

Los agentes de la solución propuesta por **IQsec, S.A. de C.V.** podrán cifrar cualquier archivo, volumen o directorio de los servidores donde se encuentren instalados de tal forma de que puedan proteger información estructurada y no-





ejemplo: imágenes, videos, archivos digitalizados de voz, etc.)

estructurada (por ejemplo: imágenes, videos, archivos digitalizados de voz, etc.)

**Referirse al documento:**

Vormetric Brochure pág 1 y 3.pdf

9.3.72. Los agentes de la solución propuesta deberán registrar cualquier intento de acceso de los usuarios a los archivos, y tomar la decisión de permitir, rechazar o restringir el acceso de los usuarios a los mismos.

Los agentes de la solución propuesta por **IQsec, S.A. de C.V.** registraran cualquier intento de acceso de los usuarios a los archivos, y tomar la decisión de permitir, rechazar o restringir el acceso de los usuarios a los mismos.

**Referirse al documento:**

Vormetric Brochure pág 1 y 3.pdf

9.3.73. Las políticas de control de acceso de la solución propuesta deberán ser aplicadas aún hasta para los usuarios privilegiados del sistema.

Las políticas de control de acceso de la solución propuesta por **IQsec, S.A. de C.V.** serán aplicadas aún hasta para los usuarios privilegiados del sistema.

**Referirse al documento:**

Vormetric Brochure pág 1 y 6.pdf

9.3.74. Las políticas de la solución propuesta deberán estar basadas en el usuario, el proceso, el tipo de archivo y el horario.

Las políticas de la solución propuesta por **IQsec, S.A. de C.V.** estarán basadas en el usuario, el proceso, el tipo de archivo y el horario.

**Referirse al documento:**

38



9.3.75. Las políticas de la solución propuesta deberán poder ser aplicadas a usuarios locales, o también integradas al AD o LDAP.

Vormetric Brochure pág 1 y 6.pdf

Las políticas de la solución propuesta por **IQsec, S.A. de C.V.** podrán ser aplicadas a usuarios locales, o también integradas al AD o LDAP.

**Referirse al documento:**

Administrador de seguridad de datos de Vormetric pág 1 y 48.pdf

9.3.76. Los agentes de la solución propuesta deberán tener la capacidad de almacenar las llaves de cifrado en memoria de tal forma de no requerir tener conectividad con la consola asociada para poder aplicar los procesos de cifrado y descifrado.

Los agentes de la solución propuesta por **IQsec, S.A. de C.V.** tendrán la capacidad de almacenar las llaves de cifrado en memoria de tal forma de no requerir tener conectividad con la consola asociada para poder aplicar los procesos de cifrado y descifrado.

**Referirse al documento:**

Plataforma de seguridad de datos de Vormetric pág 1, 12, 49, 58, 197 y 461.pdf

9.3.77. Las bitácoras de la actividad de los usuarios de la solución propuesta deberán poder ser enviadas a una plataforma SIEM mediante un servidor de syslog o bien en formato CEF, en tiempo real de manera nativa.

Las bitácoras de la actividad de los usuarios de la solución propuesta por **IQsec, S.A. de C.V.** podrán ser enviadas a una plataforma SIEM mediante un servidor de syslog o bien en formato CEF, en tiempo real de manera nativa.

**Referirse al documento:**





9.3.78. La plataforma de la solución propuesta deberá integrar agentes que puedan ser incorporados en el futuro, permitiendo el enmascarado de datos y el cifrado columnas de las bases de datos, y que estos agentes sean gestionados por la misma consola. Los mismos que no generarán ningún costo adicional durante la vigencia del contrato para el Instituto FONACOT.

9.3.79. La solución propuesta deberá tener la capacidad de trabajar en ambientes de nube, soportando esquemas de operación con AWS, Azure, Rackspace e IBM de manera enunciativa más no limitativa.

9.3.80. La solución propuesta deberá tener la capacidad de integrarse con servicios de Key Management as a Service

Plataforma de seguridad de datos de Vormetric pág 1, 12, 49, 58, 197 y 461.pdf

La plataforma de la solución propuesta por **IQsec, S.A. de C.V.** integraran agentes que puedan ser incorporados en el futuro, permitiendo el enmascarado de datos y el cifrado columnas de las bases de datos, y que estos agentes sean gestionados por la misma consola. Los mismos que no generarán ningún costo adicional durante la vigencia del contrato para el Instituto FONACOT.

**Referirse al documento:**

Vormetric Brochure pág 1 y 6.pdf

Plataforma de seguridad de datos de Vormetric pág 1, 11, 12 y 26.pdf

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad de trabajar en ambientes de nube, soportando esquemas de operación con AWS, Azure, Rackspace e IBM de manera enunciativa más no limitativa.

**Referirse al documento:**

Socios Proveedores de Servicios en la Nube pág 2,6 y 7.pdf

La solución propuesta por **IQsec, S.A. de C.V.** tendrá la capacidad de integrarse con servicios de Key Management as a Service para dar servicios de manejo de llaves on premise o bien en la nube.



para dar servicios de manejo de llaves on premise o bien en la nube.

**Referirse al documento:**

Socios Proveedores de Servicios en la Nube pág 2,6 y 7.pdf

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

Los artefactos contemplados en este esquema de solución propuesta por **IQsec, S.A. de C.V.** contendrán las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

**Referirse al documento:**

Premium Plus Support Technical Support Thales e-Security.pdf

Imperva Support – Technical Assistance.pdf





## 10. Servicio de Ciberpatrullaje para protección y reputación de Identidad Institucional

### 10.1 Descripción del Servicio

**IQsec, S.A. de C.V.**, brindará el Servicio de aseguramiento de identidad institucional, el cual consiste en realizar actividades de inteligencia contra amenazas en tiempo real recopilando antes, durante y después de ataques cibernéticos.

El Servicio de aseguramiento de identidad institucional protegerá al Instituto FONACOT de los ataques de phishing con herramientas preventivas que abordan las amenazas antes de su lanzamiento. El servicio utilizará el dominio del Instituto para la protección del mismo para proporcionar prevención, detección y mitigación contra estafadores

El servicio se brindará mediante una solución tecnológica que ofrecerá una visibilidad profunda de las capas más oscuras y peligrosas de Internet, monitoreando e identificando automáticamente las amenazas, permitiendo tomar las medidas necesarias para limitar el daño.

### 10.2 Descripción de Funcionalidades

- |  |  |
|--|--|
| 10.2.1 El Servicio de aseguramiento de identidad institucional deberá proporcionar inteligencia contra amenazas en tiempo real recopilando antes, durante y después de ataques cibernéticos. | El Servicio de aseguramiento de identidad institucional propuesto por <b>IQsec, S.A. de C.V.</b> , proporcionará inteligencia contra amenazas en tiempo real recopilando antes, durante y después de ataques cibernéticos. |
|--|--|

#### Referirse en el documento

MarkMonitor\_Top5.Reasons.AntiFraud\_pag 3.pdf



- 10.2.2 La solución propuesta por el LICITANTE deberá ofrecer una visibilidad profunda de las capas más oscuras y peligrosas de Internet, monitoreando e identificando automáticamente las amenazas, permitiendo tomar las medidas necesarias para limitar el daño.
- La solución propuesta por **IQsec, S.A. de C.V.**, ofrecerá una visibilidad profunda de las capas más oscuras y peligrosas de Internet, monitoreando e identificando automáticamente las amenazas, permitiendo tomar las medidas necesarias para limitar el daño.
- Referirse en el documento**  
MarkMonitor\_Top5.Reasons.AntiFraud\_pag 3.pdf  
ds-MarkMonitor\_Dark\_Web\_Cyber\_Intelligence\_pag 3.pdf
- 10.2.3 La solución propuesta por el LICITANTE deberá monitorear en un formato de 24/7 a través de múltiples zonas de cibercrimen incluyendo el Dark Web, la Web profunda, redes sociales, sitios de chat IRC, foros y otros sitios. Con la finalidad de dar una visibilidad profunda de las amenazas inminentes para la organización.
- La solución propuesta por **IQsec, S.A. de C.V.**, monitoreará en un formato de 24/7 a través de múltiples zonas de cibercrimen incluyendo el Dark Web, la Web profunda, redes sociales, sitios de chat IRC, foros y otros sitios. Con la finalidad de dar una visibilidad profunda de las amenazas inminentes para la organización.
- Referirse en el documento**  
ds-MarkMonitor\_Dark\_Web\_Cyber\_Intelligence\_pag 3.pdf
- 10.2.4 La solución propuesta por el LICITANTE deberá monitorizar conversaciones en los medios sociales y otros canales digitales.
- La solución propuesta por **IQsec, S.A. de C.V.**, monitoreará conversaciones en los medios sociales y otros canales digitales.
- Referirse en el documento**  
MarkMonitor\_Top5.Reasons.AntiFraud\_pag 2.pdf  
ds-MarkMonitor\_Dark\_Web\_Cyber\_Intelligence\_pag 1.pdf
- 10.2.5 La solución propuesta por el LICITANTE deberá proporcionar inteligencia procesable y alertas para ayudar a la institución a tomar las medidas adecuadas
- La solución propuesta por **IQsec, S.A. de C.V.**, proporcionará inteligencia procesable y alertas para ayudar a la institución a





para proteger los activos financieros, marcas y reputación del instituto.

tomar las medidas adecuadas para proteger los activos financieros, marcas y reputación del instituto.

10.2.6 La solución propuesta por el LICITANTE deberá poder personalizar palabras clave de búsqueda en más de 150 idiomas proporcionan una idea de la actividad amenaza específica a través de múltiples canales.

**Referirse en el documento**

ds-MarkMonitor\_Dark\_Web\_Cyber\_Intelligence\_pag 1.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, podrá personalizar palabras clave de búsqueda en más de 150 idiomas proporcionan una idea de la actividad amenaza específica a través de múltiples canales.

10.2.7 La solución propuesta por el LICITANTE deberá contar con alternativa escalable para búsquedas manuales para el comportamiento criminal en el Dark Web utilizando tecnología de robots inteligentes. Dichos robots inteligentes tendrán que imitar el comportamiento humano para infiltrarse en las redes criminales de forma automática.

**Referirse en el documento**

ds-MarkMonitor\_Dark\_Web\_Cyber\_Intelligence\_pag 3.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, contará con alternativa escalable para búsquedas manuales para el comportamiento criminal en el Dark Web utilizando tecnología de robots inteligentes. Dichos robots inteligentes tendrán que imitar el comportamiento humano para infiltrarse en las redes criminales de forma automática.

10.2.8 La solución propuesta por el LICITANTE deberá estar conectada a un ecosistema de asociaciones y relaciones con motores de búsqueda, redes sociales, mercados en línea, grupos de defensa de la industria, registros y fuerzas del orden, así como a una red de bases de datos que funcionan con Thomson Reuters.

**Referirse en el documento**

ds-MarkMonitor\_Dark\_Web\_Cyber\_Intelligence\_pag 4.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, estará conectada a un ecosistema de asociaciones y relaciones con motores de búsqueda, redes sociales, mercados en línea, grupos de defensa de la industria, registros y fuerzas del orden, así como a una red de bases de datos que funcionan con Thomson Reuters.



10.2.9 La solución propuesta por el LICITANTE deberá contar con un motor de correlación basado en grandes datos utilizando aprendizaje automático para la detección automatizada, el cual deberá de garantizar una detección de hasta un 50% de incidentes de fraude para la institución.

10.2.10 La solución propuesta por el LICITANTE deberá ofrecer análisis en tiempo real de los registros de servidores web, para que pueda detectar los sitios de phishing antes de que se pueda lanzar ataques de fraude en nombre de la institución.

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

**Referirse en el documento**

ds-MarkMonitor\_Dark\_Web\_Cyber\_Intelligence\_pag 5.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, contará con un motor de correlación basado en grandes datos utilizando aprendizaje automático para la detección automatizada, el cual deberá de garantizar una detección de hasta un 50% de incidentes de fraude para la institución.

**Referirse en el documento**

MarkMonitor\_Top5.Reasons.AntiFraud\_pag 1.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, ofrecerá análisis en tiempo real de los registros de servidores web, para que pueda detectar los sitios de phishing antes de que se pueda lanzar ataques de fraude en nombre de la institución.

**Referirse al documento**

MarkMonitor\_Top5.Reasons.AntiFraud\_pag 4.pdf

Los artefactos contemplados en este esquema de solución propuesta por **IQsec, S.A. de C.V.**, contendrán las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

**Referirse al documento:**

Markmonitor-managed-services.pdf

Propuesta de mesa de ayuda\_pág 4.pdf





10.2.12 EL LICITANTE deberá anexar en su cotización un ejemplo de reporte ejecutivo, el cual deberá ser generado con la solución tecnológica ofertada para el Servicio de aseguramiento de identidad institucional descrito en el presente documento con el siguiente nivel de detalle:

Reporte Ejecutivo:

- Clasificación de Indicadores de ciber amenazas.  
Tipos de incidentes inferidos con base en los indicadores.
- Normatividad Relacionada Inferida por incumplimiento.
- Modelo de operación del análisis de compromiso, monitoreo y detección de amenazas recomendado.
- Ley de Seguridad Nacional.  
Mapa de Calor de la Cadena de Progresión de la Amenaza.
- Los 15 indicadores más populares.  
Línea de tiempo priorizada de los indicadores más populares.  
Descripción de los TTPs de las amenazas más populares.
- Reconocimiento alineado a Cyber Kill Chain (KC1)  
Línea de tiempo priorizada de la fase de Reconocimiento
- Armamentización alineada a Cyber Kill Chain (KC2)

**IQsec, S.A. de C.V.**, anexará en su cotización un ejemplo de reporte ejecutivo, el cual deberá ser generado con la solución tecnológica ofertada para el Servicio de aseguramiento de identidad institucional descrito en el presente documento con el siguiente nivel de detalle:

Reporte Ejecutivo:

- Clasificación de Indicadores de ciber amenazas.  
Tipos de incidentes inferidos con base en los indicadores.
- Normatividad Relacionada Inferida por incumplimiento.
- Modelo de operación del análisis de compromiso, monitoreo y detección de amenazas recomendado.
- Ley de Seguridad Nacional.  
Mapa de Calor de la Cadena de Progresión de la Amenaza.
- Los 15 indicadores más populares.  
Línea de tiempo priorizada de los indicadores más populares.  
Descripción de los TTPs de las amenazas más populares.
- Reconocimiento alineado a Cyber Kill Chain (KC1)  
Línea de tiempo priorizada de la fase de Reconocimiento
- Armamentización alineada a Cyber Kill Chain (KC2)  
Línea de tiempo priorizada de la fase de Armamentización.
- Entrega alineada a Cyber Kill Chain (KC3)  
Línea de tiempo priorizada de la fase de Entrega.

28

- Línea de tiempo priorizada de la fase de Armamentización.
  - Entrega alineada a Cyber Kill Chain (KC3)
    - Línea de tiempo priorizada de la fase de Entrega.
    - OWASP Top Ten.
  - Exploits con CVE Detalle de las vulnerabilidades con CVE.
  - Explotación alineada a Cyber Kill Chain (KC4)
    - Línea de tiempo priorizada de la fase de Explotación
    - Descripción de los TTPs de las amenazas encontradas durante la fase de Explotación.
  - Instalación alineada a Cyber Kill Chain (KC5)
    - Línea de tiempo priorizada de la fase de Instalación.
    - Descripción de los TTPs de las amenazas encontradas durante la fase de Instalación.
  - Comando y Control alineado a Cyber Kill Chain (KC6)
    - Línea de tiempo priorizada de la fase de Comando y Control
    - Descripción de los TTPs de las amenazas encontradas durante la fase de Comando y Control (C2).
  - Acciones y Objetivos alineado a Cyber Kill Chain (KC7)
    - Línea de tiempo priorizada de las Acciones y Objetivos.
- OWASP Top Ten.
  - Exploits con CVE Detalle de las vulnerabilidades con CVE.
  - Explotación alineada a Cyber Kill Chain (KC4)
    - Línea de tiempo priorizada de la fase de Explotación
    - Descripción de los TTPs de las amenazas encontradas durante la fase de Explotación.
  - Instalación alineada a Cyber Kill Chain (KC5)
    - Línea de tiempo priorizada de la fase de Instalación.
    - Descripción de los TTPs de las amenazas encontradas durante la fase de Instalación.
  - Comando y Control alineado a Cyber Kill Chain (KC6)
    - Línea de tiempo priorizada de la fase de Comando y Control
    - Descripción de los TTPs de las amenazas encontradas durante la fase de Comando y Control (C2).
  - Acciones y Objetivos alineado a Cyber Kill Chain (KC7)
    - Línea de tiempo priorizada de las Acciones y Objetivos.
  - Conclusiones.

**Referirse a los Documentos:**

ReporteEstratégicoAuguriiov1\_9\_pag 10.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 15.pdf





Descripción de los TTPs de las amenazas encontradas durante la fase de Acciones y Objetivos.

- Conclusiones.

ReporteEstratégicoAuguriiov1\_9\_pag 16.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 25.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 26.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 28-30.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 31-32.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 33-36.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 37-46.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 44-49.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 50-65.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 66-70.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 71-93.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 22-24.pdf  
ReporteEstratégicoAuguriiov1\_9\_pag 94.pdf



## 11. Servicio de Sensibilización de Tecnologías de la Información

### 11.1 Descripción del Servicio

**IQsec, S.A. de C.V.** proveerá al Instituto FONACOT, un mecanismo de sensibilización al interior del Instituto con el objeto de desarrollar una cultura de seguridad informática y acciones responsables que aporten valor en la reducción de riesgos institucionales.

### 11.2 Descripción de Componentes

- |  |   |
|--|---|
| <p>11.2.1 El servicio de sensibilización en seguridad informática deberá considerar una solución tecnológica, la cual deberá ser administrada por el prestador del servicio.</p>                         | <p>El servicio de sensibilización en seguridad informática que <b>IQsec, S.A. de C.V.</b> proveerá esta basado en una solución tecnológica que es administrada por <b>IQsec, S.A. de C.V.</b></p>                                   |
| <p><b>Referirse a los documentos:</b></p> <p>Propuesta_Programa de Concientización_pag 4.pdf</p>   |   |
| <p>11.2.2 La solución tecnológica para la prestación del servicio de sensibilización en seguridad informática deberá tener la capacidad de generar reportes de avances y resultados de evaluaciones.</p> | <p>La solución tecnológica propuesta por <b>IQsec, S.A. de C.V.</b> para la prestación del servicio de sensibilización en seguridad informática tiene la capacidad de generar reportes de avances y resultados de evaluaciones.</p> |





**Referirse a los documentos:**

Propuesta\_Programa de Concientización\_pag 6.pdf

11.2.3 El servicio de sensibilización en seguridad informática deberá considerar al menos los siguientes temas de seguridad informática:

- Contraseñas seguras.
- Ingeniería social.
- Confidencialidad, disponibilidad e integridad de almacenamiento.
- Phishing.
- Malware.
- Controles de seguridad de la información.
- Amenazas persistentes avanzadas.

El servicio de sensibilización en seguridad informática que **IQsec, S.A. de C.V.** proveerá y considerará al menos 1800 usuarios con acceso a la plataforma de concientización, teniendo acceso los siguientes temas de seguridad informática:

- Contraseñas seguras.
- Ingeniería social.
- Confidencialidad, disponibilidad e integridad de almacenamiento.
- Phishing.
- Malware.
- Controles de seguridad de la información.
- Amenazas persistentes avanzadas.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 10 de la empresa "IQSEC S.A. DE C.V." de la página 13 de 36 que a la letra dice:



*"Se le solicita amablemente a la convocante nos confirme el número de usuarios que podrán tener acceso a la plataforma y a los contenidos especificados en el numeral 11.2.3"*

**Respuesta de la Convocante: "El licitante deberá considerar al menos al acceso a la plataforma de concientización de 1800 usuarios durante la vigencia del contrato"**

**Referirse a los documentos:**

Propuesta\_Programa de Concientización\_pag 4.pdf

11.2.4 El servicio de sensibilización en seguridad informática deberá considerar las herramientas para informar, generar conciencia y la propagación de los puntos necesarios para el cuidado y custodia de la información.

El servicio de sensibilización en seguridad informática que **IQsec, S.A. de C.V.** proveerá, considerará las herramientas precisas para informar, generar conciencia y la propagación de los puntos necesarios para el cuidado y custodia de la información.

**Referirse a los documentos:**

Propuesta\_Programa de Concientización\_pag 4.pdf





11.2.5 El servicio de sensibilización en seguridad informática deberá los mecanismos para el diseño y la elaboración de instrumentos y evaluación.

El servicio de sensibilización en seguridad informática que **IQsec, S.A. de C.V.** proveerá, considerará los mecanismos para el diseño y la elaboración de instrumentos y evaluación.

**Referirse a los documentos:**

Propuesta\_Programa de Concientización\_pag 6.pdf

### 11.3 Descripción de Funcionalidades

11.3.1 La solución propuesta deberá establecer los mecanismos convenientes que permitan al personal del Instituto FONACOT desarrollar las habilidades como mínimo en los siguientes temas de seguridad informática:

- Contraseñas seguras.
- Ingeniería social.
- Confidencialidad, disponibilidad e integridad de almacenamiento.
- Phishing.
- Malware.
- Controles de seguridad de la información.

La solución propuesta por **IQsec, S.A. de C.V.** establecerá los mecanismos convenientes que permitan al personal del Instituto FONACOT desarrollar las habilidades como mínimo en los siguientes temas de seguridad informática:

- Contraseñas seguras.
- Ingeniería social.
- Confidencialidad, disponibilidad e integridad de almacenamiento.
- Phishing.
- Malware.
- Controles de seguridad de la información.

- Amenazas persistentes avanzadas.

- Amenazas persistentes avanzadas.

11.3.2 La solución propuesta deberá ejecutar el servicio de sensibilización del personal, considerando la elaboración de materiales impresos y digitales con información clara, precisa y sin tecnicismos complejos, respecto a los temas antes mencionados, los cuales están alineados a las políticas de seguridad de la información aplicables que serán acordadas entre el licitante ganador y el Instituto FONACOT.

**Referirse a los documentos:**

Propuesta\_Programa de Concientización\_pag 4 .pdf

La solución propuesta por **IQsec, S.A. de C.V.** ejecutará el servicio de sensibilización del personal, considerando la elaboración de materiales impresos y digitales con información clara, precisa y sin tecnicismos complejos, respecto a los temas antes mencionados, los cuales están alineados a las políticas de seguridad de la información aplicables que serán acordadas entre **IQsec, S.A. de C.V.** y el Instituto FONACOT.

11.3.3 El licitante ganador deberá elaborar y entregar a quién designe El Instituto FONACOT, un reporte detallado con los resultados de las pruebas de phishing ejecutadas.

**Referirse a los documentos:**

Propuesta\_Programa de Concientización\_pag 4-5 .pdf

**IQsec, S.A. de C.V.** elaborará y entregará a quién designe El Instituto FONACOT, un reporte detallado con los resultados de las pruebas de phishing ejecutadas.

**Referirse a los documentos:**

Propuesta\_Programa de Concientización\_pag 5-6 .pdf





11.3.4 El licitante ganador deberá realizar las dos pruebas de phishing conforme a la periodicidad que El Instituto FONACOT determine.

**IQsec, S.A. de C.V.** realizará las dos pruebas de phishing conforme a la periodicidad que El Instituto FONACOT determine.

**Referirse a los documentos:**

Propuesta\_Programa de Concientización\_pag 5.pdf

11.3.5 El licitante ganador utilizará todos los medios de difusión posibles, para aumentar el entendimiento general de la información en los receptores sin importar si se inclinan más por lo visual, lo auditivo, lo presencial o lo físico.

**IQsec, S.A. de C.V.** utilizará todos los medios de difusión posibles, para aumentar el entendimiento general de la información en los receptores sin importar si se inclinan más por lo visual, lo auditivo, lo presencial o lo físico.

**Referirse a los documentos:**

Propuesta\_Programa de Concientización\_pag 6.pdf

11.3.6 El licitante ganador deberá desarrollar la totalidad de sus materiales con lenguaje simple, utilizando los tecnicismos mínimos indispensables y en lo posible evitar definiciones o conceptos complejos que dificulten el desarrollo de la cultura informática del personal del Instituto FONACOT.

**IQsec, S.A. de C.V.** desarrollará la totalidad de los materiales que proveerá con lenguaje simple, utilizando los tecnicismos mínimos indispensables y en lo posible evitará definiciones o conceptos complejos que dificulten el desarrollo de la cultura informática del personal del Instituto FONACOT.

**Referirse a los documentos:**

Propuesta\_Programa de Concientización\_pag 6.pdf



- 11.3.7 La difusión de los materiales digitales se realizará a través de la infraestructura tecnológica del Instituto FONACOT. La difusión de los materiales digitales que **IQsec, S.A. de C.V.** proveerá, se realizará a través de la infraestructura tecnológica del Instituto FONACOT.
- Referirse a los documentos:**  
Propuesta\_Programa de Concientización\_pag 6.pdf
- 11.3.8 El licitante ganador deberá diseñar y elaborar instrumentos de evaluación que permitan identificar el nivel de sensibilización y cultura informática del personal del Instituto FONACOT. **IQsec, S.A. de C.V.** diseñará y elaborará los instrumentos de evaluación que permitan identificar el nivel de sensibilización y cultura informática del personal del Instituto FONACOT.
- Referirse a los documentos:**  
Propuesta\_Programa de Concientización\_pag 6.pdf
- 11.3.9 Los instrumentos de evaluación serán aplicados de manera trimestral conforme a la logística que determine El Instituto FONACOT. Los instrumentos de evaluación que **IQsec, S.A. de C.V.** proveerá serán aplicados de manera trimestral conforme a la logística que determine El Instituto FONACOT
- Referirse a los documentos:**  
Propuesta\_Programa de Concientización\_pag 6.pdf
- 11.3.10 El licitante ganador deberá asignar un recurso humano con perfil de consultor en seguridad informática con **IQsec, S.A. de C.V.** proveerá un recurso humano con perfil de consultor en seguridad informática con experiencia





experiencia comprobable, para la gestión y coordinación del programa de sensibilización del Instituto FONACOT.

comprobable, para la gestión y coordinación del programa de sensibilización del Instituto FONACOT.

**Referirse a los documentos:**

Propuesta\_Programa de Concientización\_pag 7.pdf

11.3.11 El licitante ganador, deberá entregar los accesos al licenciamiento correspondiente a los componentes del servicio de sensibilización en seguridad informática propuestos a favor del Instituto FONACOT.

**IQsec, S.A. de C.V.** entregará los accesos al licenciamiento correspondiente a los componentes del servicio de sensibilización en seguridad informática propuestos a favor del Instituto FONACOT.

**Referirse al documento:**

Propuesta de mesa de ayuda\_pag 4.pdf

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

Los artefactos contemplados en este esquema de solución por **IQsec, S.A. de C.V.** contendrán las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

**Referirse al documento:**

Standard Support by Wombat Security.pdf

Propuesta de mesa de ayuda\_pag 4.pdf



## 12. Servicio de Administración del SGSI

### 12.1 Descripción del Servicio

**IQsec, S.A. de C.V.**, actualizará y administrará el Sistema de Gestión de Seguridad de la Información (SGSI) en El Instituto FONACOT, alineado con sus objetivos estratégicos, evaluando la situación actual de la Institución. Dicho Sistema de Gestión de Seguridad de la Información asegurará el cumplimiento de los objetivos específicos de seguridad de la información, de acuerdo con lo establecido en el estándar ISO/IEC 27001.

**IQsec, S.A. de C.V.**, mediante el personal en sitio identificará los principales activos de información y realizará una evaluación de riesgos de los principales activos de información y su valoración a nivel cualitativo o cuantitativo.

**IQsec, S.A. de C.V.**, mediante el personal en sitio actualizará el Manual del Sistema de Gestión de Seguridad de la Información, conformado por las 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, de acuerdo con el Plan de Seguridad de la Información elaborado por la firma consultora, dentro del alcance definido por El Instituto FONACOT.

**IQsec, S.A. de C.V.**, establecerá y/o fortalecerá los controles adecuados de seguridad de la información a través de los controles seleccionados e indicadores para la medición efectiva de los controles.

### 12.2 Características del Servicio

12.2.1 El LICITANTE adjudicado deberá realizar un análisis de riesgos que permita evaluar e identificar los requisitos de seguridad de la institución, definiendo las potenciales

**IQsec, S.A. de C.V.**, realizará un análisis de riesgos que permita evaluar e identificar los requisitos de seguridad de la institución, definiendo las potenciales amenazas a los





amenazas a los activos asociados a los procesos estratégico de la Institución y a los activos de información administrados o custodiados por la Dirección de Tecnologías de Información del Instituto FONACOT, su vulnerabilidad, la probabilidad de ocurrencia y su posible impacto. Para ello se debe tener en cuenta lo siguiente:

- En conjunto con el personal del Instituto FONACOT, el especialista en sistemas de gestión de seguridad de la información, deberán definir los procesos críticos dentro del alcance del SGSI de todo El Instituto FONACOT.
- El LICITANTE adjudicado deberá identificar los activos que es necesario proteger. 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.

activos asociados a los procesos estratégico de la Institución y a los activos de información administrados o custodiados por la Dirección de Tecnologías de Información del Instituto FONACOT, su vulnerabilidad, la probabilidad de ocurrencia y su posible impacto. Para ello se debe tener en cuenta lo siguiente:

- En conjunto con el personal del Instituto FONACOT, el especialista en sistemas de gestión de seguridad de la información, deberán definir los procesos críticos dentro del alcance del SGSI de todo El Instituto FONACOT.
- **IQsec, S.A. de C.V.**, identificará los activos que es necesario proteger. Se define como activo a la información, documentos, software, equipos de tecnología y servicios.
- **IQsec, S.A. de C.V.**, analizará 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.



**Referirse a los documentos:**

DOC-32915 Archer IT Risk Management\_pag 1.pdf

RSA Archer 6.3 Business Impact Analysis Use Case Guide\_pag 6.pdf

RSA Archer 6.1 IT Risk Mgt Guide\_pag 5.pdf

RSA Archer 6.1 IT Risk Mgt Guide\_pag 10-11.pdf

12.2.2 El licitante ganador deberá valorizar y ponderar las amenazas identificadas en el análisis de riesgos, con la finalidad de definir el alcance de aplicación en base al estándar ISO/IEC 27001, en coordinación con los representantes de la institución.

**IQsec, S.A. de C.V.**, valorizará y ponderará las amenazas identificadas en el análisis de riesgos, con la finalidad de definir el alcance de aplicación en base al estándar ISO/IEC 27001, en coordinación con los representantes de la institución.

**Referirse a los documentos:**

RSA Archer 6.1 IT Risk Mgt Guide\_pag 10.pdf

RSA Archer ISMS H15121 5-2016\_pag 1.pdf

12.2.3 El licitante ganador deberá revisar y en caso de ser necesario actualizar el estudio, denominado GAP análisis, con el que actualmente cuenta la institución a fin de determinar la brecha existente entre la realidad de la institución en temas de seguridad de la información (estado actual) y lo recomendado en el estándar ISO/IEC 27001 (estado deseado), con la

**IQsec, S.A. de C.V.**, revisará y en caso de ser necesario actualizará el estudio, denominado GAP análisis, con el que actualmente cuenta la institución a fin de determinar la brecha existente entre la realidad de la institución en temas de seguridad de la información (estado actual) y lo recomendado en el estándar ISO/IEC 27001 (estado





finalidad de identificar fallas y determinar mejoras posibles a sus prácticas de seguridad.

12.2.4 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. En base a este plan se definirán los controles necesarios que aseguren la reducción de los riesgos identificados, tanto los recomendados en la ISO 27001:2013 como de otro conjunto de nuevos controles diseñados para cubrir en forma adecuada las necesidades específicas de la institución.

12.2.5 El LICITANTE deberá elaborar las políticas, prácticas, estándares y procedimientos que conformen las actividades a corto plazo del Plan de Seguridad de la Información de la institución, que conduzcan a la implementación del Sistema de Gestión de Seguridad de la Información.

deseado), con la finalidad de identificar fallas y determinar mejoras posibles a sus prácticas de seguridad.

**Referirse a los documentos:**

RSA Archer ISMS H15121 5-2016\_pag 1.pdf

**IQsec, S.A. de C.V.**, elaborará 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. En base a este plan se definirán los controles necesarios que aseguren la reducción de los riesgos identificados, tanto los recomendados en la ISO 27001:2013 como de otro conjunto de nuevos controles diseñados para cubrir en forma adecuada las necesidades específicas de la institución.

**Referirse al documento:**

RSA Archer 6.2 Issues Mgt Use Case Guide\_pag 6.pdf

**IQsec, S.A. de C.V.**, elaborará las políticas, prácticas, estándares y procedimientos que conformen las actividades a corto plazo del Plan de Seguridad de la Información de la institución, que conduzcan a la implementación del Sistema de Gestión de Seguridad de la Información.



12.2.6 El LICITANTE deberá supervisar la ejecución del plan de trabajo y la calidad de los entregables generados. Esta tarea debe incluir el proveer de una metodología de seguimiento del proyecto, definir formas de control, evaluar la participación de las dependencias a cargo, usuarios líderes y personal informático involucrado en el proyecto.

12.2.7 El LICITANTE deberá realizar un simulacro de incidencias que puedan afectar la seguridad de la información, con la finalidad de comprobar la eficacia de los controles establecidos.

12.2.8 El LICITANTE deberá implementar el Sistema de Gestión de Seguridad de la Información, asesorando y

**Referirse al documento:**

RSA Archer IT and Security Policy Program Management\_pag 1.pdf

**IQsec, S.A. de C.V.** supervisará la ejecución del plan de trabajo y la calidad de los entregables generados. Esta tarea debe incluir el proveer de una metodología de seguimiento del proyecto, definir formas de control, evaluar la participación de las dependencias a cargo, usuarios líderes y personal informático involucrado en el proyecto.

**Referirse al documento:**

Servicio de soporte técnico y Mesa de Ayuda.pdf

**IQsec, S.A. de C.V.**, realizará un simulacro de incidencias que puedan afectar la seguridad de la información, con la finalidad de comprobar la eficacia de los controles establecidos.

**Referirse al documento:**

RSA Archer 6.3 Incident Mgt Use Case Guide\_pag 6.pdf

**IQsec, S.A. de C.V.**, implementara el Sistema de Gestión de Seguridad de la Información, asesorando y





controlando la implementación en base al Plan de Seguridad de la Información.

12.2.9 El servicio deberá tener la posibilidad de centralizar información de amenazas reportadas ya sea por analistas de seguridad o por servicios de suscripción vía correo electrónico, en un formato estructurado en una base de datos que facilite a los usuarios la ejecución de búsquedas.

Se requiere que la definición de amenazas en el servicio incluya:

- Vulnerabilidades.
- Código malicioso.
- Amenazas geopolíticas.
- Parches.

La herramienta propuesta por el LICITANTE deberá contar con las siguientes soluciones:

- Administración de Políticas.
- Administración de Riesgos.

controlando la implementación en base al Plan de Seguridad de la Información.

**IQsec, S.A. de C.V.**, dará la posibilidad centralizar información de amenazas reportadas ya sea por analistas de seguridad o por servicios de suscripción vía correo electrónico, en un formato estructurado en una base de datos que facilite a los usuarios la ejecución de búsquedas.

La definición de amenazas en el servicio incluirá:

- Vulnerabilidades.
- Código malicioso.
- Amenazas geopolíticas.
- Parches.

La herramienta propuesta por **IQsec, S.A. de C.V.**, contará con las siguientes soluciones:

- Administración de Políticas.
- Administración de Riesgos.
- Administración de Cumplimiento.



- Administración de Cumplimiento.
  - Administración de Incidentes.
  - Administración Empresarial.
  - Administración de Proveedores.
  - Administración de Amenazas.
  - Continuidad de Negocios.
  - Administración de Auditoría.
- Administración de Incidentes.
  - Administración Empresarial.
  - Administración de Proveedores.
  - Administración de Amenazas.
  - Continuidad de Negocios.
  - Administración de Auditoría.

Es importante que cuente con estos módulos completamente integrados entre sí; la herramienta propuesta por el LICITANTE ganador deberá tener la capacidad de integrarse por módulos, en esta fase del proyecto se implementarán las siguientes soluciones:

La solución propuesta contará con los módulos completamente integrados entre sí; la herramienta propuesta por **IQsec, S.A. de C.V.**, tendrá la capacidad de integrarse por módulos, en esta fase del proyecto se implementarán las siguientes soluciones:

- Administración de Políticas.
  - Administración de Riesgos.
  - Administración de Cumplimiento.
  - Administración de Incidentes.
  - Administración de Amenazas.
- Administración de Políticas.
  - Administración de Riesgos.
  - Administración de Cumplimiento.
  - Administración de Incidentes.
  - Administración de Amenazas.

**Referirse a los documentos:**

RSA Archer 6.1 IT Risk Mgt Guide \_pag 9.pdf





Sales Guide RSA Archer Use Case Reference Guide  
Rev\_pag 7.pdf

Sales Guide RSA Archer Use Case Reference Guide  
Rev\_pag 9.pdf

Sales Guide RSA Archer Use Case Reference Guide  
Rev\_pag 3.pdf

Sales Guide RSA Archer Use Case Reference Guide  
Rev\_pag 12.pdf

Sales Guide RSA Archer Use Case Reference Guide  
Rev\_pag 17.pdf

Sales Guide RSA Archer Use Case Reference Guide  
Rev\_pag 5.pdf

Sales Guide RSA Archer Use Case Reference Guide  
Rev\_pag 9.pdf

Sales Guide RSA Archer Use Case Reference Guide  
Rev\_pag 4.pdf

Sales Guide RSA Archer Use Case Reference Guide  
Rev\_pag 2.pdf

RSA Archer 6.3 Overview Guide\_pag 10.pdf

12.2.1( El servicio deberá incluir una solución para la automatización del Sistema de Gestión de Seguridad de la Información (SGSI).

El servicio **propuesto** por **IQsec, S.A. de C.V.**, incluirá una solución para la automatización del Sistema de Gestión de Seguridad de la Información (SGSI).



**Referirse al documento:**

RSA Archer 6.1 Information Security Management System (ISMS) Use Case Guide\_pag 7.pdf

### 12.3 Descripción de Componentes

12.3.1 La solución propuesta por el LICITANTE deberá poder instalarse en plataformas Windows server 2012 R2 o 2016 ediciones estándar o data center.

La solución propuesta por **IQsec, S.A. de C.V.**, podrá instalarse en plataformas Windows server 2012 R2 o 2016 ediciones estándar o data center.

**Referirse al documento:**

DELL - Servidor1 – Archer\_pag 2.pdf

RSA Archer 6.3 Platform Installation and Upgrade Guide\_pag 17.pdf

12.3.2 La solución propuesta por el LICITANTE deberá soportar Microsoft SQL server 2014 (64-bits) o 2016 (64-bits).

La solución propuesta por **IQsec, S.A. de C.V.**, soportará Microsoft SQL server 2014 (64-bits) o 2016 (64-bits).

**Referirse al documento:**

DELL - Servidor1 – Archer\_pag 3.pdf

RSA Archer 6.3 Platform Installation and Upgrade Guide\_pag 17.pdf





12.3.3 La solución propuesta por el LICITANTE deberá tener al menos 16 Cores de CPU.

La solución propuesta por **IQsec, S.A. de C.V.**, tendrá al menos 16 Cores de CPU.

**Referirse al documento:**

DELL - Servidor1 – Archer\_pag 1.pdf

12.3.4 La solución propuesta por el LICITANTE deberá tener al menos 96 Gb de RAM.

La solución propuesta por **IQsec, S.A. de C.V.**, tendrá al menos 96 Gb de RAM.

**Referirse al documento:**

DELL - Servidor1 – Archer\_pag 2.pdf

12.3.5 La solución propuesta por el LICITANTE deberá tener interfaces de red de al menos 1 Gbps.

La solución propuesta por **IQsec, S.A. de C.V.**, tendrá interfaces de red de al menos 1 Gbps.

**Referirse al documento:**

DELL - Servidor1 – Archer\_pag 2.pdf

12.3.6 La solución propuesta por el LICITANTE deberá tener al menos 1TB de almacenamiento.

La solución propuesta por **IQsec, S.A. de C.V.**, tendrá al menos 1TB de almacenamiento.

**Referirse al documento:**

DELL - Servidor1 – Archer\_pag 2.pdf



12.3.7 La solución propuesta por el LICITANTE deberá tener al menos 8 cores de CPU. La solución propuesta por **IQsec, S.A. de C.V.**, tendrá al menos 8 cores de CPU.

**Referirse al documento:**

DELL - Servidor1 – Archer\_pag 1.pdf

12.3.8 La solución propuesta por el LICITANTE deberá poder instalarse en plataformas Windows server 2012 o 2016. La solución propuesta por **IQsec, S.A. de C.V.**, podrá instalarse en plataformas Windows server 2012 o 2016.

**Referirse al documento:**

DELL - Servidor1 – Archer\_pag 2.pdf

RSA Archer 6.3 Platform Installation and Upgrade Guide\_pag 17.pdf

12.3.9 La solución propuesta por el LICITANTE deberá tener al menos 25 Gb de RAM. La solución propuesta por **IQsec, S.A. de C.V.**, tendrá al menos 25 Gb de RAM.

**Referirse al documento:**

DELL - Servidor1 – Archer\_pag 2.pdf

12.3.10 La solución propuesta por el LICITANTE deberá tener al menos 50GB de almacenamiento. La solución propuesta por **IQsec, S.A. de C.V.**, tendrá al menos 50GB de almacenamiento.





**Referirse al documento:**

DELL - Servidor1 – Archer\_pag 2.pdf

12.3.11 La solución propuesta por el LICITANTE deberá tener interfaces de red de al menos 1Gbps.

La solución propuesta por **IQsec, S.A. de C.V.**, tendrá interfaces de red de al menos 1Gbps.

**Referirse al documento:**

DELL - Servidor1 – Archer\_pag 2.pdf

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

Los artefactos contemplados en este esquema de solución propuesta por **IQsec, S.A. de C.V.**, contendrán las características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

**Referirse al documento:**

RSA.com-contact US.pdf

Propuesta de mesa de ayuda\_pág 4.pdf

## 12.4 Descripción de Funcionalidades



- 12.4.1 La solución propuesta por el LICITANTE deberá de contar con librerías y políticas mapeado a normas y procedimientos del Instituto que cumplen con el estándar ISO 27001:2013. La solución propuesta por **IQsec, S.A. de C.V.**, contará con librerías y políticas mapeado a normas y procedimientos del Instituto que cumplen con el estándar ISO 27001:2013.
- Referirse al documento:**
- RSA Archer 6.1 IT & Security Policy Prog Mgt Guide\_pag 10.pdf
- Sales Guide RSA Archer Use Case Reference Guide Rev\_pag 10.pdf
- 12.4.2 La solución propuesta por el LICITANTE deberá permite centralizar y normalizar políticas, estándares y procedimientos, además de mapearlos a objetivos del instituto. La solución propuesta por **IQsec, S.A. de C.V.**, permitirá centralizar y normalizar políticas, estándares y procedimientos, además de mapearlos a objetivos del instituto.
- Referirse al documento:**
- RSA Archer 6.1 IT & Security Policy Prog Mgt Guide\_pag 7.pdf
- 12.4.3 La solución propuesta por el LICITANTE deberá permitir comunicar adecuadamente las políticas a todo el instituto y promover la comprensión de las mismas entre los empleados del instituto, mediante campañas de capacitación específicas, ya sea mediante esta solución o incorporada a otra metodología de sensibilización. La solución propuesta por **IQsec, S.A. de C.V.**, permitirá comunicar adecuadamente las políticas a todo el instituto y promover la comprensión de las mismas entre los empleados del instituto, mediante campañas de capacitación específicas, ya sea mediante esta solución o incorporada a otra metodología de sensibilización.





12.4.4 La solución propuesta por el LICITANTE deberá poder rastrear o dar seguimiento a la aceptación de políticas, identificar brechas y monitorear excepciones a las políticas con informes en tiempo real.

**Referirse al documento:**

RSA Archer 6.3 Platform Administrator's Guide\_pag 667.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, podrá rastrear o dar seguimiento a la aceptación de políticas, identificar brechas y monitorear excepciones a las políticas con informes en tiempo real.

12.4.5 La solución propuesta por el LICITANTE deberá brindar la capacidad de crear contenido de políticas, comunicarlo a usuarios finales, realizar campañas de capacitación y ver excepciones, todo desde un solo portal web.

**Referirse a los documentos:**

RSA Archer 6.1 IT & Security Policy Prog Mgt Guide\_pag 7.pdf

RSA Archer 6.1 IT & Security Policy Prog Mgt Guide\_pag 12.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, brindará la capacidad de crear contenido de políticas, comunicarlo a usuarios finales, realizar campañas de capacitación y ver excepciones, todo desde un solo portal web.

**Referirse a los documentos:**

RSA Archer 6.1 IT & Security Policy Prog Mgt Guide\_pag 10-11.pdf



12.4.6 La solución propuesta por el LICITANTE deberá poder reducir el tiempo y el esfuerzo requeridos para crear y actualizar políticas, administrar excepciones y demostrando el cumplimiento de múltiples normas, mediante un portal web que contenga las métricas de tiempo.

La solución propuesta por **IQsec, S.A. de C.V.**, podrá reducir el tiempo y el esfuerzo requeridos para crear y actualizar políticas, administrar excepciones y demostrando el cumplimiento de múltiples normas, mediante un portal web que contenga las métricas de tiempo.

**Referirse a los documentos:**

RSA Archer 6.1 IT & Security Policy Prog Mgt Guide\_pag 10.pdf

RSA Archer 6.1 Policy Prog Mgt Guide\_pag 8.pdf

12.4.7 La solución propuesta por el LICITANTE deberá brindar una configuración de libre código, en dado caso que sea requerido por el instituto.

La solución propuesta por **IQsec, S.A. de C.V.**, brindará una configuración de libre código, en dado caso que sea requerido por el instituto.

**Referirse a los documentos:**

RSA Archer 6.3 Platform Administrator's Guide\_pag 21.pdf

12.4.8 La solución propuesta por el LICITANTE deberá permite crear vistas de las tecnologías e infraestructura del instituto, además de brindar su relación entre ellas.

La solución propuesta por **IQsec, S.A. de C.V.**, permitirá crear vistas de las tecnologías e infraestructura del instituto, además de brindar su relación entre ellas.

**Referirse al documento:**





12.4.9 La solución propuesta por el LICITANTE deberá permitir una integración con múltiples bases de datos y sistemas de registro de administración de configuración del instituto.

RSA Archer 6.3 Platform Administrator's Guide\_pag 1057.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, permitirá una integración con múltiples bases de datos y sistemas de registro de administración de configuración del instituto.

**Referirse al documento:**

12.4.10 La solución propuesta por el LICITANTE deberá contar con la capacidad para manejar múltiples lenguajes, incluyendo español.

RSA Archer 6.3 Platform Administrator's Guide\_pag 17.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, contará con la capacidad para manejar múltiples lenguajes, incluyendo español.

**Referirse al documento:**

12.4.11 La solución propuesta por el LICITANTE deberá consolidar e integrar nativamente información de las siguientes disciplinas:

RSA Archer 6.3 Platform Administrator's Guide\_pag 1079 .pdf

La solución propuesta por **IQsec, S.A. de C.V.**, consolidará e integrará nativamente información de las siguientes disciplinas:

- Gestión de Activos
- Gestión de Riesgos
- Gestión de Cumplimiento Normativo y Regulatorio

- Gestión de Activos
- Gestión de Riesgos
- Gestión de Cumplimiento Normativo y Regulatorio



- Gestión de Incidentes
  - Gestión de Proveedores y Contratos
  - Gestión de Vulnerabilidades y Amenazas
  - Gestión de Continuidad del Negocio
  - Gestión de Auditoría
- Gestión de Incidentes
  - Gestión de Proveedores y Contratos
  - Gestión de Vulnerabilidades y Amenazas
  - Gestión de Continuidad del Negocio.
  - Gestión de Auditoría

**Referirse a los documentos:**

RSA Archer 6.1 Information Security Management System Use Case Guide\_pag 11.pdf

RSA Archer 6.1 IT Risk Mgt Use Guide\_pag 11.pdf

RSA Archer 6.3 Incident Mgt Use Case Guide\_pag 6.pdf

RSA Archer Third Party Catalog 6.2 Use Case Guide\_pag 8.pdf

RSA Archer 6.1 IT Security Vulnerabilities Prog Guide\_pag 4.pdf

RSA Archer 6.3 Business Continuity & IT Disaster Recovery Planning Use Case Guide\_pag 8.pdf

RSA Archer 6.3 Overview Guide\_pag 10.pdf

12.4.12 La solución propuesta por el LICITANTE deberá actualizar los contenidos regulatorios mediante alimentación RSS.

La solución propuesta **IQsec, S.A. de C.V.**, actualizará los contenidos regulatorios mediante alimentación RSS.





12.4.13 La solución propuesta por el LICITANTE deberá tener la capacidad para el aislamiento de información por grupos de trabajo.

**Referirse al documento:**

RSA Archer 6.3 Platform Administrator's Guide\_pag 913.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, tendrá la capacidad para el aislamiento de información por grupos de trabajo.

12.4.14 La solución propuesta por el LICITANTE deberá contar con visibilidad de indicadores de riesgo y cumplimiento, con agregación automática, desde las distintas perspectivas del negocio ya sea por proceso, por unidad de negocio, por producto, por empresa, etcétera.

**Referirse al documento:**

RSA Archer 6.3 Platform Administrator's Guide\_pag 599.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, contará con visibilidad de indicadores de riesgo y cumplimiento, con agregación automática, desde las distintas perspectivas del negocio ya sea por proceso, por unidad de negocio, por producto, por empresa, etcétera.

12.4.15 La solución propuesta por el LICITANTE deberá contar con la capacidad para manejar múltiples escalas de medición del riesgo y presentar información consolidada y normalizada.

**Referirse al documento:**

RSA Archer 6.2 Key Indicator Mgt Guide\_pag 7.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, contará con la capacidad para manejar múltiples escalas de medición del riesgo y presentar información consolidada y normalizada.



12.4.16 La solución propuesta por el LICITANTE deberá contar con la capacidad para responder cuestionarios de evaluación de riesgos desde dispositivos móviles basados, sin necesidad de contar con conexión a Internet.

12.4.17 La solución propuesta por el LICITANTE deberá poder enviar automáticamente cuestionarios de evaluación de riesgos, con base en criterios específicos y reglas del instituto.

**Referirse al documento:**

RSA Archer Enterprise & Operational Risk Management\_pag 1-2.pdf

La solución propuesta por **IQsec, S.A. de C.V.** contará con la capacidad para responder cuestionarios de evaluación de riesgos desde dispositivos móviles basados, sin necesidad de contar con conexión a Internet.

**Referirse al documento:**

RSA Archer 6.3 Platform Administrator's Guide\_pag 584.pdf

La solución propuesta por **IQsec, S.A. de C.V.**, podrá enviar automáticamente cuestionarios de evaluación de riesgos, con base en criterios específicos y reglas del instituto.

**Referirse al documento:**

RSA Archer 6.3 Platform Administrator's Guide\_pag 118.pdf

**13. Servicio de Control y Gestión de Usuarios**





### 13.1 Descripción del Servicio

El servicio robustecerá la seguridad en los puestos de trabajo (endpoints) contra robo de información. La solución propuesta por **IQsec, S.A. de C.V.**, tendrá la capacidad de proteger las estaciones de trabajo del Instituto FONACOT contra ataques que tengan la intención de extraer información de manera no autorizada o en caso de presentarse la sustracción o robo de la estación de trabajo, protegerá el acceso a los documentos e información sensible que determine el instituto.

**IQsec, S.A. de C.V.**, en caso de ser el licitante ganador, en conjunto con Instituto FONACOT definirán las políticas y la estrategia de despliegue del "Servicio de protección de estaciones de trabajo", lo anterior, con la finalidad de realizar una dispersión del mismo de manera sincronizada con los objetivos del Instituto y lograr su total integración con los activos del Instituto.

El servicio que **IQsec, S.A. de C.V.** ofrece será capaz de garantizar que bajo ningún motivo en caso de robo físico de los equipos de puesto de trabajo se podrá tener acceso a la información sensible que el Instituto FONACOT maneja.

### 13.2 Descripción de Componentes

El servicio que **IQsec, S.A. de C.V.**, estará compuesto por hardware y/o software los cuales no serán de libre distribución y pueden ser integrados en todas las estaciones de trabajo con los que cuenta el Instituto FONACOT actualmente e incluso en el caso de que se integren nuevos puestos de trabajo la solución es fácilmente aplicable a estos elementos y será compatible.

La solución contará con las características limitativas mas no enunciativas siguientes:

- Ser compatible con sistemas operativos
  - Microsoft® Windows® 10
  - Microsoft® Windows® 8, 8.1



- Microsoft® Windows® 7
  - Microsoft® Windows® Vista
  - Microsoft® Windows® XP SP 3
  - Microsoft® Windows® Server 2003 – 2012
- Contará con los siguientes algoritmos y estándares
    - AES 256 bit
    - AES 128 bit
    - SHA 256 bit
    - SHA1 160 bit
    - RSA 1024 bit
    - Triple DES 112 bit
    - Blowfish 128 bit
  - **IQsec, S.A. de C.V.**, cuenta por lo menos con la certificación FIPS 140-2 nivel 1

Esto se referencia en la propuesta técnica de “**Propuesta de Servicios y Mesa de Servicios.pdf**”, expresada en los documentos adjuntados en este proceso licitatorio.

### 13.3 Descripción de Funcionalidades

13.3.1 La solución deberá permitir a las estaciones de trabajo cifrar datos sin tiempo de inactividad o cualquier interrupción a los equipos, aplicaciones o flujos de trabajo.

La solución propuesta por **IQsec, S.A. de C.V.**, permitirá a las estaciones de trabajo cifrar datos sin tiempo de inactividad o cualquier interrupción a los equipos, aplicaciones o flujos de trabajo.





**Referirse al documento:**

ESET\_Deslock\_Encryption\_pag 2.pdf

13.3.2 La solución deberá permitir realizar cifrado sólo los archivos y las carpetas deseadas.

La solución propuesta por **IQsec, S.A. de C.V.**, permitirá realizar cifrado sólo los archivos y las carpetas deseadas.

**Referirse al documento:**

ESET\_Deslock\_Encryption\_pag 2.pdf

13.3.3 La solución deberá permitir el cifrado de medios extraíbles. No se utilizará espacio adicional para el contenido cifrado, por lo que los usuarios del Instituto FONACOT podrán usar la capacidad total de los dispositivos.

La solución propuesta por **IQsec, S.A. de C.V.**, permitirá el cifrado de medios extraíbles. No se utilizará espacio adicional para el contenido cifrado, por lo que los usuarios del Instituto FONACOT podrán usar la capacidad total de los dispositivos.

**Referirse al documento:**

ESET\_Deslock\_Encryption\_pag 2.pdf

13.3.4 La solución deberá permitir integración con el Active Directory.

La solución propuesta por **IQsec, S.A. de C.V.**, permitirá integración con el Active Directory.

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.



13.3.5 La solución deberá realizar cifrado y gestión de claves y/o llaves. La solución propuesta por **IQsec, S.A. de C.V.**, realizará cifrado y gestión de claves y/o llaves.

**Referirse al documento:**

ESET\_Deslock\_Encryption\_pag 4.pdf

13.3.6 La solución deberá permitir políticas que se pueden aplicar para las estaciones de trabajo. La solución propuesta por **IQsec, S.A. de C.V.**, permitirá políticas que se pueden aplicar para las estaciones de trabajo.

**Referirse al documento:**

ESET\_Deslock\_Encryption\_pag 4.pdf

13.3.7 La solución deberá tener la capacidad de realizar Cifrado transparente de correo electrónico para Outlook. Sólo podrán descifrar el correo electrónico los destinatarios que compartan la misma clave que el remitente. La solución propuesta por **IQsec, S.A. de C.V.**, tendrá la capacidad de realizar Cifrado transparente de correo electrónico para Outlook. Sólo podrán descifrar el correo electrónico los destinatarios que compartan la misma clave que el remitente.

**Referirse al documento:**

ESET\_Deslock\_Encryption\_pag 2.pdf





13.3.8 La solución deberá realizar cifrado transparente de los archivos que sean enviados a la carpeta designada para tal funcionalidad de manera transparente e inmediata.

La solución propuesta por **IQsec, S.A. de C.V.**, realizará cifrado transparente de los archivos que sean enviados a la carpeta designada para tal funcionalidad de manera transparente e inmediata.

**Referirse al documento:**

ESET\_Deslock\_Encryption\_pag 2.pdf

13.3.9 La solución deberá tener capacidades de caza de amenazas para detectar y contrastar múltiples fuentes de información del punto final para buscar herramientas de hacking y actividades del adversario, portable, reglas yara, análisis de procesos, análisis de eventlog, análisis de registro, análisis de las conexiones activas de red, análisis de autoruns, verificación de archivos abiertos, persistencia en WMI, detección del perfil de directorios, escaneo del cache SHIM, escaneo de Shell bags, análisis del cache de DNS, verificación de configuración del firewall de punto final, verificación de rootkits, verificación de servicios, análisis de tareas calendarizadas, análisis del sistema de archivos, análisis de MFT, análisis de mutex, análisis de vulnerabilidades, y verificación de integridad de archivos.

La solución propuesta por **IQsec, S.A. de C.V.**, tendrá capacidades de caza de amenazas para detectar y contrastar múltiples fuentes de información del punto final para buscar herramientas de hacking y actividades del adversario, portable, reglas yara, análisis de procesos, análisis de eventlog, análisis de registro, análisis de las conexiones activas de red, análisis de autoruns, verificación de archivos abiertos, persistencia en WMI, detección del perfil de directorios, escaneo del cache SHIM, escaneo de Shell bags, análisis del cache de DNS, verificación de configuración del firewall de punto final, verificación de rootkits, verificación de servicios, análisis de tareas calendarizadas, análisis del sistema de archivos, análisis de MFT, análisis de mutex, análisis de vulnerabilidades, y verificación de integridad de archivos.

**Referirse al documento:**



- 13.3.10 La solución deberá de detectar llaves típicas que dejan los grupos o adversarios en APTs para mantener persistencia en el dispositivo. La solución propuesta por **IQsec, S.A. de C.V.**, detectará llaves típicas que dejan los grupos o adversarios en APTs para mantener persistencia en el dispositivo.
- 13.3.11 La solución deberá de analizar los elementos de autoruns de todos los procesos como plugins, controladores registrados, WMI, proveedores de LSA y aplicar IOCs. La solución propuesta por **IQsec, S.A. de C.V.**, analizará los elementos de autoruns de todos los procesos como plugins, controladores registrados, WMI, proveedores de LSA y aplicar IOCs.
- 13.3.12 La solución deberá de analizar archivos OBJECTS.DATA para enlistar elementos de listas registradas y alertar en caso de ser sospechosos. La solución propuesta por **IQsec, S.A. de C.V.**, analizará archivos OBJECTS.DATA para enlistar elementos de listas registradas y alertar en caso de ser sospechosos.

DatasheetAugurio\_pag 11.pdf.

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.





- 13.3.13 La solución deberá de identificar irregularidades en el perfil de usuario. La solución propuesta por **IQsec, S.A. de C.V.**, identificará irregularidades en el perfil de usuario.

**Referirse al documento:**

DatasheetAugurio\_pag11.pdf.

- 13.3.14 La solución deberá de detectar rastros de uso de herramientas maliciosas en Sysmon, Windows Defender, Applocker, Powershell y otras. La solución propuesta por **IQsec, S.A. de C.V.**, detectará rastros de uso de herramientas maliciosas en Sysmon, Windows Defender, Applocker, Powershell y otras.

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.

- 13.3.15 La solución deberá de hacer análisis de Shell bags loggeados que muestren la localidad de donde accedieron los usuarios. La solución propuesta por **IQsec, S.A. de C.V.**, hará análisis de Shell bags loggeados que muestren la localidad de donde accedieron los usuarios.

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.

- 13.3.16 La solución deberá de hacer análisis de procesos activos buscando anomalías en Hooks/File, Handles/Mutex, conexiones de red, cadenas en memoria, directorios e intentos de encubrimiento. La solución propuesta por **IQsec, S.A. de C.V.**, hará análisis de procesos activos buscando anomalías en Hooks/File, Handles/Mutex, conexiones de red, cadenas en memoria, directorios e intentos de encubrimiento.



13.3.17 La solución deberá de monitorizar rootkits usando Named Pipes o comunicaciones vía controles de Device IO.

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.

La solución propuesta por **IQsec, S.A. de C.V.**, monitoreará rootkits usando Named Pipes o comunicaciones vía controles de Device IO.

13.3.18 La solución deberá de verificar todas las sesiones LSA activas para la duración o conocimiento de nombres usados en casos adversarios o grupos de APTs

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.

La solución propuesta por **IQsec, S.A. de C.V.**, verificará todas las sesiones LSA activas para la duración o conocimiento de nombres usados en casos adversarios o grupos de APTs

13.3.19 La solución deberá de analizar todos los servicios locales para detectar configuraciones irregulares, localización de ejecutable de servicios, combinación de cuentas de usuario y tipo de inicialización, así como nombre de malwares en la ruta de imagen de servicios.

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.

La solución propuesta por **IQsec, S.A. de C.V.**, analizará todos los servicios locales para detectar configuraciones irregulares, localización de ejecutable de servicios, combinación de cuentas de usuario y tipo de inicialización, así como nombre de malwares en la ruta de imagen de servicios.





**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.

13.3.20 La solución deberá de verificar las llaves en RUN en búsqueda de código de ejecución poco común durante la inicialización.

La solución propuesta por **IQsec, S.A. de C.V.**, verificará las llaves en RUN en búsqueda de código de ejecución poco común durante la inicialización.

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.

13.3.21 La solución deberá de analizar los elementos enlistados en Startup a través de WMI.

La solución propuesta por **IQsec, S.A. de C.V.**, analizará los elementos enlistados en Startup a través de WMI.

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.

13.3.22 La solución deberá de analizar el Master File Table buscando archivos eliminados

La solución propuesta por **IQsec, S.A. de C.V.**, analizará el Master File Table buscando archivos eliminados

**Referirse al documento:**

DatasheetAugurio\_pag 11.pdf.



- 13.3.23 La solución detectará mutexes de programas maliciosos como RATs y otras piezas maliciosas usadas por adversarios o grupos de APTs. La solución propuesta por **IQsec, S.A. de C.V.**, detectará mutexes de programas maliciosos como RATs y otras piezas maliciosas usadas por adversarios o grupos de APTs.
- Referirse al documento:**  
DatasheetAugurio\_pag 11.pdf.
- 13.3.24 La solución detectará named pipes maliciosos comúnmente usados por adversarios o grupos de APTs. La solución propuesta por **IQsec, S.A. de C.V.**, detectará named pipes maliciosos comúnmente usados por adversarios o grupos de APTs.
- Referirse al documento:**  
DatasheetAugurio\_pag 11.pdf.
- 13.3.25 La solución deberá de verificar vulnerabilidades en el punto final que permiten movimientos laterales. La solución propuesta por **IQsec, S.A. de C.V.**, verificará vulnerabilidades en el punto final que permiten movimientos laterales.
- Referirse al documento:**  
DatasheetAugurio\_pag 11.pdf  
DatasheetAugurio\_pag 1.pdf
- 13.3.26 Los artefactos contemplados en este esquema de solución deberán contener las características y Los artefactos contemplados en este esquema de solución propuesta por **IQsec, S.A. de C.V.**, contendrán las



LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



especificaciones del soporte y pólizas de mantenimiento de los mismos

características y especificaciones del soporte y pólizas de mantenimiento de los mismos.

**Referirse al documento:**

[eset.com-Access ESET Premium Support assistance.pdf](#)

[Propuesta de mesa de ayuda\\_pág.4.pdf](#)



#### 14. Requerimientos de Seguridad de la Información

**IQsec, S.A. de C.V.**, en caso de resultar el licitante ganador contemplará 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. **IQsec, S.A. de C.V.**, en caso de resultar el licitante ganador realizará 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, **IQsec, S.A. de C.V.**, en caso de resultar el licitante ganador realizará 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 **IQsec, S.A. de C.V.**:

- Hará la colección y preservación de la imagen forense.
- Llevará 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 **IQsec, S.A. de C.V.** para brindar el Análisis Forense, contará con las siguientes funcionalidades y será realizado utilizando herramientas especializadas tales como:
  - i. Artefactos tecnológicos de análisis forense reconocidos 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 entregará **IQsec, S.A. de C.V.** en caso de resultar el licitante ganador al Instituto FONACOT cada vez que requiera este servicio como parte del análisis forense:

NOMBRE	DESCRIPCION	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 de 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



NOMBRE	DESCRIPCION	PERIODICIDAD
MEMORIA TÉCNICA DE ADQUISICIÓN DE INFORMACIÓN	Documento que detalla física y lógicamente los indicios de los que serán colectadas las imágenes forenses.	Por evento de análisis solicitado

IQsec, S.A. de C.V., considerará, 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 ser solicitado IQsec, S.A. de C.V. 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.

Esto se referencia en la propuesta técnica de "**Propuesta Análisis Forense.pdf**", expresada en los documentos adjuntados en este proceso licitatorio.

## 15. Administración de los Servicios

IQsec, S.A. de C.V. en caso de resultar el licitante ganador, contará 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 Administrador del proyecto de IQsec, S.A. de C.V. 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.

IQsec, S.A. de C.V. en caso de resultar el licitante ganador, asegurará la correcta implementación de todas las soluciones tecnológicas a través del personal cuyo rol esta 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, IQsec, S.A. de C.V., considerará la siguiente plantilla mínima de personal en su propuesta de servicio integral.



LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS  
 No. LA-014P7R001-E349-2018  
 RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



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).
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.	<ul style="list-style-type: none"> <li>AC Continuous Monitoring Certification (GMON); Y</li> <li>EC-Council Ethical Hacker; Y</li> <li>EC-Council Network Security Administrator v4.</li> </ul>
2	1	Especialista en sistemas de gestión de 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.	<ul style="list-style-type: none"> <li>GIAC Certified Windows Security Administrator (GCWN); Y</li> <li>GIAC Continuous Monitoring Certification (GMON); Y</li> <li>EC Council Network Security Administrator; Y</li> <li>EC Council Certified Ethical Hacker; Y</li> <li>EC Council Computer Hacking Forensic Investigator.</li> </ul>
3	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.	<ul style="list-style-type: none"> <li>CISA Certified Information Systems Auditor; Y</li> <li>CISM Certified Information Security Manager; Y</li> <li>GIAC Continuous Monitoring Certification (GMON); Y</li> <li>ITIL Foundation Certificate in IT Service.</li> </ul>
4	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,	<ul style="list-style-type: none"> <li>GCIA Certified Intrusion Analyst (GIAC); Y</li> <li>CCNA Certified Network Associate Routing and Switching.</li> </ul>

LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



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).
				Electrónica o afines a las actividades del proyecto.	
5	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.	<ul style="list-style-type: none"> <li>• EC Council Computer Hacking Forensic Investigator; y</li> <li>• EC Council Certified Ethical Hacker; y</li> <li>• GIAC Global Industry Cyber Security Professional (GICSP); y</li> <li>• SANS Assessing and exploiting control system (ICS security training).</li> </ul>
6	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.	<ul style="list-style-type: none"> <li>• CISSP Certified Information Systems Security Professional; y</li> <li>• Certified ISO/IEC 27001 Lead Implementer; y</li> <li>• Cobit Foundation Certificate; y</li> <li>• ITIL versión 3 foundation Examination.</li> </ul>
7	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.	<ul style="list-style-type: none"> <li>• Certificado vigente como especialista en alguna solución de validación de Identidad que tenga base instalada dentro de una dependencia de gobierno.</li> </ul>
8	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.	<ul style="list-style-type: none"> <li>• Certificación en alguna herramienta comercial de Análisis de Vulnerabilidades. Como, por ejemplo:                             <ul style="list-style-type: none"> <li>• Tenable</li> <li>• Acunetix</li> <li>• Etc</li> </ul> </li> </ul>
9	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.	<ul style="list-style-type: none"> <li>• GIAC Continuous Monitoring Certification (GMON); y</li> <li>• EC-Council Ethical Hacker; y</li> <li>• EC-Council Network Security Administrator v4.</li> </ul>



LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



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	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.	<ul style="list-style-type: none"> <li>• GIAC Certified Windows Security Administrator (GCWN); y</li> <li>• GIAC Continuous Monitoring Certification (GMON); y</li> <li>• EC Council Network Security Administrator; y</li> <li>• EC Council Certified Ethical Hacker; y</li> <li>• EC Council Computer Hacking Forensic Investigator.</li> </ul>
11	1	Consultor en tecnologías de la información.	2	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	<ul style="list-style-type: none"> <li>• CISA Certified Information Systems Auditor; y</li> <li>• CISM Certified Information Security Manager; y</li> <li>• GIAC Continuous Monitoring Certification (GMON); y</li> <li>• ITIL Foundation Certificate in IT Service.</li> </ul>
12	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.	<ul style="list-style-type: none"> <li>• Certificado PMP.</li> </ul>
13	1	Diseñador gráfico.	3	Cédula profesional a nivel licenciatura de carreras tales como: Diseño Gráfico, marketing y/o Mercadotecnia.	<ul style="list-style-type: none"> <li>• Certificación, constancia o documento de comprobación de una institución a nivel nacional o internacional sobre alguno de los siguientes temas:                             <ul style="list-style-type: none"> <li>• Marketing Digital.</li> <li>• Relaciones públicas.</li> <li>• Comunicación.</li> <li>• Diseño Editorial.</li> </ul> </li> </ul>
14	10	Personal en Sitio	3	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	<p>Cada uno del "Personal en Sitio", presentará al menos la siguiente certificación:</p> <p>Certificación en alguna de las tecnologías con las cuales se prestarán los servicios del presente Anexo Técnico.</p>



PLANTILLA DE PERSONAL					
No.	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).
15	10	Especialista Implementador	3	Cédula o título profesional a nivel Licenciatura de carreras tales como: Sistemas Computacionales, Informática, Telecomunicaciones, Electrónica o afines a las actividades del proyecto.	Cada uno de los "Especialistas Implementadores", presentará al menos la siguiente certificación:  Certificación en alguna de las tecnologías con las cuales se prestarán los servicios del presente Anexo Técnico.
	33				

### Reemplazo de Personal

En caso de que se requiera sustituir algún miembro del equipo por parte de IQsec, S.A. de C.V. 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, IQsec, S.A. de C.V. en caso de resultar el licitante ganador contará hasta con 5 (cinco) días hábiles para su sustitución. Será responsabilidad de IQsec, S.A. de C.V. en caso de resultar el licitante ganador involucrar al nuevo integrante, así como de ponerlo al tanto del estatus del proyecto.

Es responsabilidad de IQsec, S.A. de C.V. tener la capacidad del personal en sitio para atender picos de demanda de servicios de emergencia de 24x7x365. En caso de incumplimiento será aplicada la deductiva correspondiente. Los picos de demanda deberán ser atendidos a nivel nacional sin incurrir en costos adicionales para el Instituto Fonacot y durante toda la vigencia del contrato.





En cualquier evento de sustitución del personal de IQsec, S.A. de C.V. en caso de resultar el licitante ganador, entregará 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.

IQsec, S.A. de C.V. en caso de resultar el licitante ganador, no sustituirá 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.

## 16. Herramientas de Apoyo

### Equipo computacional.

Se requiere que IQsec, S.A. de C.V. en caso de resultar el licitante ganador proporcione el equipo computacional portátil personal, con las mismas características técnicas al del Instituto FONACOT o superiores, al personal en sitio que designe mientras éste se encuentre asignado al proyecto.

- Procesador Intel Core i7 o superior de cuarta generación.
- Memoria RAM de 16 Gb. DDR3, como mínimo.
- Disco duro de 500 Gb. o superior.
- Tarjeta de red Ethernet RJ45 10/100/1000 integrada en mother board
- Tarjeta de red inalámbrica integrada a la mother board, compatible con los estándares 802.11 a/b/g/n



### Equipo de comunicación Móvil.

Se requiere que IQsec, S.A. de C.V. en caso de resultar el licitante ganador, proporcione al personal en sitio equipo de telefonía móvil durante la vigencia del contrato, estos equipos deberán tener contemplado un plan de datos y llamadas suficientes para cubrir los requerimientos de comunicación necesarios entre el **Instituto Fonacot** e IQsec, S.A. de C.V. durante la vigencia del contrato.

### 17. Estándares

El Instituto FONACOT tiene definidos estándares (serán entregados a IQsec, S.A. de C.V. en caso de resultar el licitante ganador) que se deben considerar en todos los proyectos.

IQsec, S.A. de C.V. se apegará a los lineamientos que establece la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de los requerimientos de seguridad de la información (Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y en la de Seguridad de la Información, MAAGTICSI), publicados en el Diario Oficial de la Federación el 08 de mayo de 2014 y 04 de febrero de 2016, y en las versiones que se actualicen y estén vigentes durante la duración del presente contrato, y aquellas que se acuerden entre el Instituto FONACOT e IQsec, S.A. de C.V. en caso de resultar el licitante ganador.

### 18. Garantía de la Calidad de los Servicios

**IQsec, S.A. de C.V.**, proporcionará 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 a **IQsec, S.A. de C.V.**

IQsec, S.A. de C.V. en caso de resultar el licitante ganador, al terminar cada servicio integral mensual de: mantenimiento, soporte u operación de productos o servicios inherentes al presente, presentará una carta compromiso a la Subdirección General de Tecnologías de la Información y Comunicación, donde garantice:

#### **18.1 Solución de defectos.**

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

#### **18.2 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, serán cubiertas por IQsec, S.A. de C.V. en caso de resultar el licitante ganador sin cargo a las horas inicialmente pactadas ni costo adicional para el Instituto FONACOT.

#### **18.3 Atención de Fallas.**

IQsec, S.A. de C.V., documentará el mecanismo para la atención de incidentes.

Esto se referencia en la propuesta técnica de "**Propuesta de Servicios y Mesa de Servicios.pdf**", expresada en los documentos adjuntados en este proceso licitatorio.

#### **18.4 Levantamiento de garantías.**



IQsec, S.A. de C.V., presentará 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.

### 18.5 Atención a Garantías.

La solicitud podrá realizarse vía telefónica, por correo electrónico o de manera escrita al Director de Proyectos de IQsec, S.A. de C.V. en caso de resultar el licitante ganador (se confirmará vía correo electrónico y telefónico), describiendo el problema encontrado y el nivel de severidad, para que IQsec, S.A. de C.V. en caso de resultar 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.

### 18.6 Vigencia de la garantía.

**IQsec, S.A. de C.V.**, acepta que 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 del mismo, y cuyo formato y contenido será proporcionado por la Subdirección General de Tecnologías de la Información y Comunicación.

## 19. Garantizar los Niveles de Servicio (SLA'S)

### 19.1 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) hora, por lo que las instalaciones de las oficinas administrativas de IQsec, S.A. de C.V. están 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.

### 19.2 Mesa de servicio.

Interface de la mesa de ayuda de **IQsec, S.A. de C.V.** con la Mesa de Servicios del Instituto FONACOT para el control y administración de las incidencias.

## 20. PERFIL DEL LICITANTE DEL SERVICIO.

**IQsec, S.A. de C.V.**, es una empresa especializada en el robustecimiento de la seguridad de la información con experiencia en el mercado nacional que cuenta con instalaciones dentro de la Ciudad de México o área Metropolitana y con relacionamiento comercial y profesional en todas las soluciones tecnológicas propuestas para la prestación del servicio.



**IQsec, S.A. de C.V.**, tiene experiencia en contratos con el gobierno Federal y cuenta con los recursos financieros y materiales necesarios para llevar a cabo el objeto del presente Anexo Técnico.

## 21. CIERRE DEL SERVICIO.

Un mes antes de la finalización del contrato, **IQsec, S.A. de C.V.** realizará todas las labores de transferencia de recursos, conocimiento y documentación a un nuevo licitante o al **Instituto FONACOT** según sea el caso.

### 21.1 Transferencia de conocimientos de seguridad de la información.

IQsec, S.A. de C.V. en caso de resultar el licitante ganador, al cierre del servicio, proporcionará un Plan de transferencia de conocimiento al **Instituto FONACOT** con lo mínimo indispensable para mitigar los riesgos de transferencia y continuidad de la operación.

### 21.2 Cierre de solicitudes de servicio.

IQsec, S.A. de C.V. en caso de resultar el licitante ganador, para cerrar el contrato, presentará las cartas de aceptación de entrega del servicio a la Subdirección General de Tecnologías de la Información y Comunicación, debidamente firmadas por todas las partes involucradas en el servicio.

### 21.3 Cierre de contrato.

Una semana antes del término de la vigencia que abarca el contrato, todos los componentes del servicio que son objeto en este Anexo Técnico deberán estar terminados por parte de IQsec, S.A. de C.V. en caso de resultar el licitante ganador. El contrato podrá darse





por cerrado hasta que se atiendan en su totalidad los requerimientos de servicio turnados por el **Instituto FONACOT** dentro del período de vigencia del contrato, así como el periodo correspondiente a las garantías del servicio.

## 22. IDIOMAS.

Las propuestas de IQsec, S.A. de C.V. son presentadas en idioma español y en caso de encontrarse en otro idioma cuenta con su traducción simple al idioma español.

## 23. MANUALES, CATÁLOGOS Y FOLLETOS.

IQsec, S.A. de C.V., entregará en medio electrónico o impreso los manuales, folletos, catálogos, o aquella información que respalde las características técnicas de los equipos para la prestación del servicio conforme a lo solicitado en este Anexo Técnico.

IQsec, S.A. de C.V. en caso de resultar el licitante ganador entregará documentación que respalde las características técnicas de cada uno de los equipos ofertados en su propuesta. Esta documentación podrá conformarse por cualquiera de los siguientes puntos:

- Originales o copias fotostáticas de los manuales, folletos y/o catálogos en idioma español o traducción simple al español.
- Información impresa obtenida de Internet, la cual incluya la dirección URL en idioma español o traducción simple al español.

## 24. PATENTES, MARCAS Y DERECHOS.

No Aplica.

## 25. VIGENCIA, LUGAR Y HORARIO DE LA PRESTACIÓN DEL SERVICIO.



a. Vigencia.

El contrato que se derive del presente procedimiento tendrá una vigencia de a partir del día hábil siguiente al fallo y hasta el 31 de mayo de 2021.

De conformidad con lo establecido en el quinto párrafo del artículo 84 del **RLey**, la prestación del servicio se llevará a cabo de conformidad con lo solicitado en el **Anexo 13 "Características Técnicas del Servicio"**, sin perjuicio de que se cumpla con la obligación de formalizar el contrato dentro del plazo establecido en el numeral **III.4.5. FIRMA DEL CONTRATO** de la Convocatoria.

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 con 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 de **IQsec, S.A. de C.V.** en caso de resultar el licitante ganador prestará sus servicios en el edificio sede del Instituto FONACOT, sita en Avenida Insurgentes Sur No. 452, Colonia Roma



LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



Sur, Delegación Cuauhtémoc, CP. 06760, Ciudad de México, de acuerdo a las necesidades de la Convocante, el resto del personal prestará sus servicios en las oficinas de **IQsec, S.A. de C.V.**, en caso de resultar el licitante ganador, sin embargo, se presentarán 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 a 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.

DIRECTORIO DE SUCURSALES				
Dirección de Adscripción	Representación y/o Módulo*	Domicilio	Teléfono	Horario de Atención
<b>Región Metropolitana</b>				
Dirección de Plaza Mixcoac		Molinos esquina Santiago Rebull No. 61 Col. Mixcoac C.P. 3910 Del. Benito Juarez, Ciudad de México.	5273 5527 5271 6620 5273 9733	Lun a Vie 8:00 a 20:00
				Sábado 8:00 a 16:00
	Edificio Sede	Insurgentes Sur 452, Planta Baja, Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, Ciudad de México.	5265 7400	Lun a Vie 8:00 a 19:00
	Sede Alterna	Av. Plaza de la Republica 32, Col. Tabacalera, Deleg. Cuauhtémoc, C.P. 06030, Ciudad de México.	52657400 15553700	Lun a Vie 8:00 a 19:00
Dirección de Plaza Portales		Municipio Libre No. 83, Col. Portales, Del. Benito Juárez, C.P. 03300, México, Ciudad de México.	5672 9433 5674 3511 5674 3598	Lun a Vie 8:00 a 20:00
				Sábado 8:00 a 16:00
				Domingo 8:00 a 16:00
	*Módulo de atención SAT BANCEN	Av. Hidalgo 77, Col. Guerrero, Del. Cuauhtémoc, C.P. 06300, Ciudad de México.		Lun a Jue 10:00 a 18:00 Viernes 10:00 a 15:00
Dirección de Plaza Tlalnepantla		Sor Juana Inés de la Cruz No.22, despacho 106, Col. Centro Tlalnepantla, C.P. 54000, Tlalnepantla de Baz, Estado de México.	5565 0314 5565 1359	Lun a Vie 8:00 a 20:00
				Sábado 8:00 a 16:00
				Domingo 8:00 a 16:00
	Cuautitlán Izcalli	Av. Huhuetoca s/n, SORIANA, Loc. 6, Col. Claustro de San Miguel, Cuautitlán Izcalli, Estado de México.	5889 6836 5889 6075	Lun a Vie 9:00 a 17:00 Sábado 8:00 a 16:00

Patriotismo 399, San Pedro de los Pinos, 03800, CDMX.  
RFC: IQsec, S.A. De C.V. / IQS0708233C9

000238

LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



**DIRECTORIO DE SUCURSALES**

Dirección de Adscripción	Representación y/o Módulo*	Domicilio	Teléfono	Horario de Atención
Dirección de Plaza Vallejo		Norte 45 No. 853-B, Col. Industrial Vallejo, Del. Gustavo A. Madero, C.P. 02300, México, Ciudad de México.	5719 4012 5567 0473 5587 0031	Lun a Vie 8:00 a 19:00
				Sábado 8:00 a 16:00
	Ecatepec	Vía Morelos No. 24, Col. Jajalpa, C.P. 55090, Ecatepec, Estado de México.	5770 9005	Lun a Vie 9:00 a 18:00 Sábado 8:00 a 16:00
	Congreso del Trabajo	Av. Ricardo Flores Magón No. 44, Col. Guerrero, Del. Cuauhtémoc, C.P. 06300, México, Ciudad de México.	5583 8450 5597 6588 5782 5617	Lun a Vie 9:00 a 18:00 Sábado 8:00 a 16:00
	Plaza de la República	Plaza de la República No. 32, Planta Baja, Col. Tabacalera, Del. Cuauhtémoc, C.P. 06030, Ciudad de México.	5265 7400	Lun a Vie 9:00 a 18:00
Dirección de Plaza Zaragoza		Blvd. Puerto Aéreo No. 81, 1er piso, Col. Federal, Del. Venustiano Carranza, C.P. 15700, México, Ciudad de México.	5762 6583 2643 6785 2643 6783	Lun a Vie 8:00 a 20:00
				Sábado 8:00 a 16:00
				Domingo 8:00 a 16:00
	Chalco	Boulevard Cuauhtémoc, MZ. 53 LT. 6, Local 2, Col. Emiliano Zapata, Chalco de Covarrubias, Estado de México, C.P. 56608.	1734 1303 1734 1658 1734 1330	Lun a Vie 9:00 a 17:00 Sábado 8:00 a 16:00
	Texcoco	Prolongación 16 de Septiembre No. 310, Loc. 30, Col. Barrio de San Pablo Centro, C.P. 56116, Texcoco, Estado de México.	5954 0909 5925 1899	Lun a Vie 9:00 a 17:00 Sábado 8:00 a 16:00
Dirección de Plaza Coapa		Av. Canal de Miramontes 3280, locales 27, 28, 29, 30, Coaplaza, Col. Villacoapa, Del. Tlalpan, C.P. 14390	2652 2785 2652 3926	Lun a Vie 8:00 a 20:00
				Sábado 8:00 a 16:00
<b>Región Norte</b>				
Dirección Estatal Chihuahua		Calle Séptima y Allende No. 1002, Zona Centro, C.P. 31000, Chihuahua, Chihuahua.	415 3281 416 1660	Lun a Vie 8:00 a 20:00
				Sábado 8:00 a 16:00
				Domingo 8:00 a 16:00
	Delicias	Circuito Plaza de la Republica 4 Norte Colonia Centro Entre calle Central y calle 2da. Norte C.P. 33000	474 1376 467 5868	Lun a Vie 9:00 a 17:00
	Cd. Juárez	Paseo Triunfo de la Rep. No. 4450, Loc. 67 y 68, Cto. Comercial Río Grande, Col. Partido Escudero, C.P. 32330, Ciudad Juárez, Chihuahua.	613 6527 613 6752	Lun a Vie 8:00 a 18:00
				Sábado 8:00 a 16:00
Dirección Estatal Mexicali		Av. Reforma No. 692, sección primera de la Ciudad de Mexicali, Baja California Norte.	552 5678 552 5961 552 6076	Lun a Vie 8:00 a 20:00
				Sábado 8:00 a 16:00
				Domingo 8:00 a 16:00
Dirección Estatal Tijuana			661 6305	Lun a Vie 8:00 a 20:00



LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



**DIRECTORIO DE SUCURSALES**

Dirección de Adscripción	Representación y/o Módulo*	Domicilio	Teléfono	Horario de Atención
		Blvd. Díaz Ordaz No.14910, Col. Las Brisas, Plaza Las Brisas, Tijuana, Baja California Norte.	661 6207	Sábado 8:00 a 16:00 Domingo 8:00 a 16:00
	Ensenada	Av. Delante fracción A y B, Lt. 007, Mza. 025, Col. Carlos Pacheco, C.P. 22890, Municipio de Ensenada, Baja California Norte.	152 1920	Lun a Vie 9:00 a 17:00
Dirección Estatal Hermosillo		Blvd. Luis Donald Colosio No. 323, Col. Valle Grande, C.P. 83205, Hermosillo, Sonora.	213 4345 216 5628 217 1593	Lun a Vie 8:00 a 20:00 Sábado 8:00 a 16:00 Domingo 8:00 a 16:00
	Cd. Obregón	Durango No. 245 Sur, Col. Centro, C.P. 85000, Ciudad Obregón, Sonora.	413 5040 414 1041	Lun a Vie 9:00 a 18:00 Sábado 8:00 a 16:00
	Empalme	Plaza Reforma, Loc.5, Col. Moderna, C.P.85330, Empalme, Sonora.	113 1429	Lun a Vie 9:00 a 17:00 Sábado 8:00 a 16:00
	Nogales	Av. de los Nogales No. 277, Loc. 3 y 4, Plaza Coyoacán, Col. Colinas del Yaqui, C.P. 84093, Nogales, Sonora.	209 6621 209 5434	Lun a Vie 9:00 a 18:00 Sábado 8:00 a 16:00
Dirección Estatal Culiacán		Gral. José Aguilar Barraza No. 1297 Poniente, Col. Centro, C.P. 80029, Culiacán, Sinaloa.	714 7152 717 0342 761 5771	Lun a Vie 8:00 a 20:00 Sábado 8:00 a 16:00 Domingo 8:00 a 16:00
	Mazatlán	Av. Ejército Mexicano No. 1401-A, Col. Ferrocarrilera, C.P. 82010, Mazatlán, Sinaloa.	982 0203 982 3008 982 7158	Lun a Vie 9:00 a 18:00 Sábado 8:00 a 16:00
	Los Mochis	Av. Cuauhtémoc No. 201 Poniente, Col. Bienestar, C.P. 81280, Los Mochis, Sinaloa.	818 2656 818 5779 818 1772	Lun a Vie 9:00 a 18:00 Sábado 8:00 a 16:00
Dirección Estatal La Paz		Calz. Forjadores de Sudcalifornia No. 286, Col. Bellavista, C.P. 23078, La Paz, Baja California Sur.	122 4111 125 6136	Lun a Vie 8:00 a 18:00 Sábado 8:00 a 16:00
	San José del Cabo	Carretera Transpeninsular Km. 34.5, Col. Guaymitas, Plaza Guaymitas, Loc. 2, C.P. 2340, San José del Cabo, Baja California Sur.	123 5962	Lun a Vie 9:00 a 17:00
<b>Región Noreste</b>				
Dirección Estatal Monterrey		Av. Manuel L. Barragán No. 325 Norte, Col. Residencial Anáhuac, Plaza Fiesta Anahuac, C.P. 66457, San Nicolás de los Garza Monterrey, NL	343 5075 343 5069 343 5061	Lun a Vie 8:00 a 20:00 Sábado 8:00 a 16:00 Domingo 8:00 a 16:00
	Monterrey II	Av. Ruiz Cortines y General Bonifacio Salinas 600, Col. León XIII, C.P. 67120 Guadalupe N.L. Sucursal Soriana Lindavista	394 6521 334 6676 394 7369	Lun a Vie 9:00 a 17:00 Sábado de 8:00 a 16:00



LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



DIRECTORIO DE SUCURSALES				
Dirección de Adscripción	Representación y/o Módulo*	Domicilio	Teléfono	Horario de Atención
	Nuevo Laredo	Calle Héroe de Nacataz y Reynosa s/n, anexo al Centro Cívico, Zona Centro, CP 88000, Nuevo Laredo, Tamaulipas.	713 6666	Lun a Vie 9:00 a 17:00
Dirección Estatal San Luis Potosí		Independencia No. 1630, Col. Barrio San Miguelito, C.P. 78339, San Luis Potosí, San Luis Potosí.	812 5207	Lun a Vie 8:00 a 20:00
			812 5466	Sábado 8:00 a 16:00
			812 6290	Domingo 8:00 a 16:00
Zacatecas		Blvd. José López Portillo No. 303, edificio STPS, Col. Dependencias Federales, C.P. 98618, Zacatecas, Zacatecas.	923 3947	Lun a Vie 9:00 a 18:00
			923 8964	Sábado 8:00 a 16:00
			927 9015	
Cd. Valles		Carranza No. 53 Sur, Zona Centro, C.P. 79000, Ciudad Valles, San Luis Potosí.	882 4428	Lun a Vie 9:00 a 17:00
			381 0319	
Fresnillo		Paseo del Mineral No. 1018, Col. Luis Donald Colosio, C.P. 99000, Fresnillo, Zacatecas.	931 3357	Lun a Vie 9:00 a 17:00
Dirección Estatal Durango		Aquiles Serdán No. 954, planta alta, Zona Centro, C.P. 34000, Durango, Durango.	811 5721	Lun a Vie 8:00 a 20:00
			811 5644	Sábado 8:00 a 16:00
				Domingo 8:00 a 16:00
Dirección Estatal Saltillo		Blvd. Isidro López Zertuche No. 2567-A, Col. Universidad, C.P. 25260, Saltillo, Coahuila.	416 4142	Lun a Vie 8:00 a 20:00
			416 7510	Sábado 8:00 a 16:00
			416 7570	Domingo 8:00 a 16:00
Cd. Acuña		Libramiento Emilio Mendoza Cisneros No. 1315, centro comercial MERCO, Col. Benjamín Canales, C.P. 26236, Cd. Acuña, Coahuila.	773 0988	Lun a Vie 9:00 a 18:00
			773 1933	
Monclova		Calle de la Fuente No. 221, Loc. 4 y 5, Plaza Blanca, Col. Telefonistas, C.P. 25700, Monclova, Coahuila.	633 6695	Lun a Vie 9:00 a 18:00
			633 6690	
Piedras Negras		Blvd. Eliseo Mendoza Berrueto s/n, Plaza Comercial, Loc. 5, Col. San Felipe Norte, C.P. 26070, Piedras Negras, Coahuila.	782 4344	Lun a Vie 9:00 a 17:00
			782 4653	
Dirección Estatal Torreón		Av. Morelos No. 138 Poniente, Col. Centro, C.P. 27000, Torreón, Coahuila.	711 9738	Lun a Vie 8:00 a 20:00
			711 9758	Sábado 8:00 a 16:00
			712 3000	Domingo 8:00 a 16:00
Gómez Palacio		Av. Hidalgo No. 113 Sur, Loc. 4, Col. Centro, Gómez Palacio, Durango.	714 0032	Lun a Vie 8:00 a 16:00
			714 9718	
Dirección Estatal Tampico		Av. Hidalgo No. 2401, Col. Reforma, C.P. 89140, Tampico, Tamaulipas.	213 6550	Lun a Vie 8:00 a 19:00
			213 6580	Sábado 8:00 a 16:00
			213 8139	
Reynosa		Aldama No. 1100, Loc. 26, Centro Comercial Río Grande, Col. Centro, C.P. 88500, Reynosa, Tamaulipas.	922 0168	Lun a Vie 9:00 a 17:00
			922 0244	Sábado 8:00 a 16:00

Patriotismo 399, San Pedro de los Pinos, 03800, CDMX.

RFC: IQsec, S.A. De C.V. / IQS0708233C9

000241



LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



DIRECTORIO DE SUCURSALES

Dirección de Adscripción	Representación y/o Módulo*	Domicilio	Teléfono	Horario de Atención
			922 6686	
	Cd. Victoria	Matamoros No. 237, oficinas de la STPS, Col. Centro, C.P. 87000, Ciudad Victoria, Tamaulipas.	315 3941	Lun a Vie 9:00 a 17:00
	Matamoros	Ave. Prolongación González No. 2035 Col. Parque Industrial, Plaza Comercial Soriana Laguneta, C.P. 87479, Matamoros, Tamaulipas.	149 1284 813 3243	Lun a Vie 9:00 a 17:00
Región Sureste				
Dirección Estatal Mérida		Paseo Montejo No. 492-A por la 43, Col. Centro, C.P. 97000, Mérida, Yucatán.	928 0821 923 5428	Lun a Vie 8:00 a 20:00
	Campeche	Av. 16 de Septiembre s/n, Palacio Federal, Col. Centro, C.P. 24000, Campeche, Campeche.	924 7002 811 3880 816 0692 816 5793	Sábado 8:00 a 16:00 Domingo 8:00 a 16:00 Lun a Vie 9:00 a 17:00 Sábado 8:00 a 16:00
Dirección Estatal Cancún		Av. Tulum, Retorno 1, Lote 3, Manzana 1, Super manzana 22, Col. Centro, C.P. 77500, Benito Juárez, Quintana Roo.	883 9701 884 0192 884 1915 883 9621 884 0746 883 9800	Lun a Vie 8:00 a 20:00 Sábado 8:00 a 16:00
	Chetumal	Av. Othón Pompeyo Blanco No. 204, 1er piso, Col. Centro, C.P. 77000, Chetumal, Quintana Roo.	285 3937	Mar a Vie 9:00 a 17:00
	Cozumel	Plaza del Sol, Mercado de Artesanía, Local Planta Alta 8 Andador 5ta. Avenida Sur No. 1 Col. Centro C.P. 77600	869 0134	Lun a Vie 9:00 a 17:00
	Playa del Carmen	Av. Benito Juárez, Lt. 3, Loc. 12, Plaza Papagayos, Col. Centro, C.P. 77710, Playa del Carmen, Quintana Roo.	879 3855	Lun a Vie 9:00 a 17:00
Dirección Estatal Tuxtla Gutiérrez		3a Norte Poniente No. 1395, entre la 12 y 13 Poniente Norte, Col. Moctezuma, C.P. 29030, Tuxtla Gutiérrez, Chiapas.	611 4703 611 7061 611 0983	Lun a Vie 8:00 a 20:00 Sábado 8:00 a 16:00
	Tapachula	4a calle Ote. No. 6, Col. Centro, C.P. 30700, Tapachula, Chiapas.	626 3226	Lun a Vie 9:00 a 17:00
Dirección Estatal Veracruz		Av. Independencia No. 787-D, P.B., Col. Centro, C.P. 91700, Veracruz, Veracruz.	955 0257 955 0338 932 9187	Lun a Vie 8:00 a 20:00 Sábado 8:00 a 16:00 Domingo 8:00 a 16:00
	Córdoba	Calle 5 No. 308, despacho 2, Col. Centro, C.P. 94500, Córdoba, Veracruz.	405 2504 405 2503	Lun a Vie 9:00 a 17:00

## DIRECTORIO DE SUCURSALES

Dirección de Adscripción	Representación y/o Módulo*	Domicilio	Teléfono	Horario de Atención
	Xalapa	Diego Leño s/n, Palacio Federal, Col. Centro, C.P. 91000, Xalapa, Veracruz.	841 5359 812 2950	Lun a Vie 9:00 a 17:00
	Poza Rica	Av. 20 de noviembre No. 110, Local 4 en Plaza Fuente, Col. Cazonas, C.P. 93230. Poza Rica, Veracruz,	826 9932	Lun a Vie 9:00 a 17:00
Dirección Estatal Villahermosa		Benito Juárez No. 118-120, Col. Centro, C.P. 86000, Villahermosa, Tabasco.	314 5804	Lun a Vie 8:00 a 20:00
			314 5767	Sábado 8:00 a 16:00
			312 5878	Domingo 8:00 a 16:00
	Cd. del Carmen	Av. 10 de Julio No. 117 Col. Francisco y Madero CP. 24190 Cd. Del Carmen, Campeche	111 3366	Lun a Vie 9:00 a 17:00 Sábado 8:00 a 16:00
	Coatzacoalcos	Av. Juárez No. 511, Col. Centro, C.P. 96400, Coatzacoalcos, Veracruz.	212 3051	Lun a Vie 9:00 a 17:00
			213 1207	
<b>Región Occidente</b>				
Dirección Estatal Guadalajara Abastos		Av. Lázaro Cárdenas No. 2305, edificio H, Loc. 102, Plaza Comercial Abastos, Col. Las Torres, C.P. 44920, Guadalajara, Jalisco.	658 3168	Lun a Vie 8:00 a 19:00
			658 4070	Sábado 8:00 a 16:00
	Federalismo	Av. Federalismo Norte 696 Sector Hidalgo, Entre Calle Cardenal y Alondra, Col. Artesanos, C.P. 44200, Guadalajara, Jalisco.	658 4070	Lun a Vie 8:00 a 19:00
			658 3112	Sábado 8:00 a 16:00
			613 2711	
			614 0913	
	Manzanillo	Blvd. Lázaro Cárdenas No. 1721, Col. Playa Azul las Brisas, C.P. 28218, Manzanillo, Colima.	333 7526	Lun a Vie 9:00 a 17:00
			333 7527	Sábado 8:00 a 16:00
			333 7528	
	Colima	Av. Ignacio Sandoval No. 350 Loc. 3,4,6 Col. Lomas de Circunvalación C.P. 28010	330 6647	Lun a Vie 9:00 a 17:00
				Sábado 8:00 a 16:00
Dirección Estatal Aguascalientes		Av. López Mateos Oriente No. 520, Zona Centro, C.P. 20000, Aguascalientes, Aguascalientes.	916 6869	Lun a Vie 8:00 a 20:00
			918 0335	Sábado 8:00 a 16:00
			918 1032	Domingo 8:00 a 16:00
Dirección Estatal Tepic		Av. Tecnológico No. 3983, Loc. 8, 9 y 10, Practiplaza Oriente, C.P. 63175, Tepic, Nayarit.	214 5828	Lun a Vie 8:00 a 19:00
			214 0444	Sábado de 8:00 a 16:00
			210 6024	
	Puerto Vallarta	Av. Francisco Villa No. 1474, P.B., Col. Los Sauces, C.P. 48328, Puerto Vallarta, Jalisco.	224 9822	Lun a Vie 8:00 a 18:00
			225 3214	Sábado de 8:00 a 16:00
			225 9137	
Dirección Estatal León			119 5315	Lun a Vie 8:00 a 20:00





**DIRECTORIO DE SUCURSALES**

Dirección de Adscripción	Representación y/o Módulo*	Domicilio	Teléfono	Horario de Atención
		Juan José Torres Landa Oriente 1007, Loc. 14 y 15, Col. Puerta San Rafael, León, Guanajuato.	119 5092 707 9893	Sábado 8:00 a 16:00 Domingo 8:00 a 16:00
	Celaya	Blvd. Adolfo López Mateos No. 932 Poniente, Col Centro, C.P. 38000, Celaya, Guanajuato.	609 1999 615 4199	Lun a Vie 9:00 a 17:00
	Irapuato	Av. Guerrero No. 1871, Local 2, (entre Orquídea y Jazmín), Col. Gámez, C.P. 36650.	624 1286 624 0443	Lun a Vie 9:00 a 17:00
Dirección Estatal Morelia		Av. Lázaro Cárdenas No. 2000, Col. Chapultepec Sur, C.P. 58260, Morelia, Michoacán.	324 1154 314 4096 314 5567	Lun a Vie 8:00 a 18:00 Sábado 8:00 a 16:00
	Lázaro Cárdenas	Av. Melchor Ocampo No. 73-A Altos, Col. 2o Sector FIDELAC, C.P. 60950, Lázaro Cárdenas, Michoacán.	537 6000 532 2343 532 2363	Lun a Vie 9:00 a 17:00
	Uruapan	Emilio Carranza No. 14- 4, Plaza Paraíso, C.P. 60000, Uruapan, Michoacán.	523 7744 524 4396	Lun a Vie 9:00 a 17:00
	Zamora	Amado Nervo Poniente No. 70, Col. Centro, C.P. 59600, Zamora, Michoacán.	515 7711 515 5093	Lun a Vie 9:00 a 17:00
Dirección Estatal Querétaro		Av. Universidad Oriente No. 142, Col. Centro, C.P. 76000, Querétaro, Querétaro.	212 3579 212 9532 212 7697	Lun a Vie 8:00 a 20:00 Sábado 8:00 a 16:00 Domingo 8:00 a 16:00
	San Juan del Río	16 Septiembre No. 8, Loc. 1, Col. Centro, C.P. 76800, San Juan del Río, Querétaro.	274 9675	Lun a Vie 9:00 a 17:00
<b>Región Centro</b>				
Dirección Estatal Pachuca		Carr. Pachuca- Tulancingo No. 1000, Loc. D9 al D12, Plaza Universidad, Col. Abundio Martínez, C.P 42184, Mineral de la Reforma, Hidalgo.	7142 783 7134 831	Lun a Vie 8:00 a 20:00 Sábado 8:00 a 16:00
	Tizayuca	Carretera México- Pachuca Km. 50, oficina de CANACINTRA Tizayuca, Zona Industrial Tizayuca, C.P. 43800, Tizayuca, Hidalgo.	100 7612	Mar a Vie 10:00 a 17:00
Dirección Estatal Cuernavaca		Plan de Ayala No. 1200, Col. Chapultepec, C.P. 62450, Cuernavaca, Morelos.	315 5251 315 6653 316 2690	Lun a Vie 8:00 a 20:00 Sábado 8:00 a 16:00
	Cuautla	Galeana No. 33, Loc. 101, planta alta, Col. Centro, C.P. 62740, Cuautla, Morelos.	108 0292 354 7739	Lun a Vie 9:00 a 17:00

LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



DIRECTORIO DE SUCURSALES

Dirección de Adscripción	Representación y/o Módulo*	Domicilio	Teléfono	Horario de Atención
	Acapulco	Av. Costera Miguel Alemán No. 1803, Frac. Magallanes, C.P. 39690, Acapulco, Guerrero.	485 2802	Lun a Vie 9:00 a 18:00
			485 0191	Sábado 8:00 a 16:00
			485 3833	
	Chilpancingo	Priv. de Jacarandas S/N, P.B., puerta 4 STPS, Col. Burócratas, C.P. 39090, Chilpancingo, Guerrero.	116 1030	Lun a Vie 9:00 a 17:00
Dirección Estatal Puebla		Calle 9 Norte No. 208, Col. Centro, C.P. 72000, Puebla, Puebla.	246 6777	Lun a Vie 8:00 a 20:00
			246 1071	Sábado 8:00 a 16:00
			246 6688	Domingo 8:00 a 16:00
	*Módulo de atención CIS	Centro Integral de Servicios (CIS), Edificio SUR, Vía Atlixcayotl No. 1101.	303 4600	Martes a Viernes 10:00 a 15:00
	*Módulo de atención VW	Servicenter de Volkswagen. Autop. Méx. - Puebla Km. 116.5 San Lorenzo Almecatla	S/N	Mar y Vie 12:00 a 17:00
	Tlaxcala	Av. Ocotlán No. 15, Col. Ocotlán, C.P. 90100, Tlaxcala, Tlaxcala.	462 1946 4622	Lun a Vie 8:00 a 18:00
			431 4621 446 4621 767	Sábado 8:00 a 16:00
	*Módulo de atención Teziutlán	El Encanto, entrada al Hospital General Sección 3ra. No. 20, C.P. 73954, Chignautla, Puebla.		Jue y Vie 11:00 a 15:00
	Tehuacán	Calle 1 Norte No. 618, Loc. 8, 9 y 10, Plaza Montecarlo, Col. Francisco Sarabia, C.P. 75730, Tehuacán, Puebla.	371 8940	Lun a Vie 9:00 a 17:00
Dirección Estatal Oaxaca		Carbonera No. 902, Esquina González Ortega, Col. Barrio Trinidad de las Huertas, C.P. 68120, Oaxaca, Oaxaca.	514 2655	Lun a Vie 8:00 a 20:00
			514 6954	Sábado 8:00 a 16:00
			514 8588	
	Salina Cruz	Av. Manuel Ávila Camacho No. 50, Palacio Federal, Salina Cruz, Oaxaca.	133 8311	Lun a Vie 9:00 a 17:00
	Tuxtepec	Av. 20 de Noviembre s/n, Col. La Piragua, C.P. 68300, Tuxtepec, Oaxaca.	871 0442	Lun a Vie 9:00 a 17:00
			871 0443	
Dirección Estatal de Toluca		Ignacio Allende Sur No. 116, Col. Centro, C.P. 50000, Toluca, Estado de México.	213 6336	Lun a Vie 8:00 a 20:00
			214 2468	Sábado 8:00 a 16:00
			214 2466	Domingo 8:00 a 16:00

26. PLAZO PARA LA SUSPENSIÓN DEL SERVICIO.

Patriotismo 399, San Pedro de los Pinos, 03800, CDMX.  
RFC: IQsec, S.A. De C.V. / IQS0708233C9

000245





**IQsec, S.A. de C.V.**, acepta que 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.

## 27. FORMA DE PAGO

**IQsec, S.A. de C.V.**, acepta que con fundamento en el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el pago se realizará en pagos mensuales, **excepto el primer mes, el cual se pagará, si fuera el caso, de manera proporcional a partir del siguiente día hábil del fallo y hasta el final de este mes en cuestión**, de acuerdo a los servicios devengados debidamente soportado y acompañado con los entregables que apliquen de acuerdo al numeral "29 ENTREGABLES", del presente Anexo Técnico.

El pago mensual 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 **Dirección de Tecnologías de la Información**, así mismo deberán ser



enviados al correo electrónico a [angel.gascon@fonacot.gob.mx](mailto:angel.gascon@fonacot.gob.mx) con copia a [javier.jimenez@fonacot.gob.mx](mailto:javier.jimenez@fonacot.gob.mx), en un horario de labores de las 9:00 a las 15:00 horas de lunes a viernes en días hábiles.

- b. Los comprobantes fiscales deben emitirse por los actos o actividades que se realicen, dichos comprobantes deben de cumplir con las especificaciones que determine el Servicio de Administración Tributaria (SAT), considerando el **Anexo 20 "Guía de llenado de los comprobantes fiscales digitales por Internet"**, y de ser posible el número de contrato que ampara dicha factura.

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 **IQsec, S.A. de C.V.**, acepta 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**.

En caso de que **IQsec, S.A. de C.V.** resulte el licitante ganador presentará sus facturas con errores o deficiencias, el plazo de pago se ajustará en términos de los artículos 89 y 90 del **RLey**.

**IQsec, S.A. de C.V. 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.

## 28. NIVELES DE SERVICIO (SLA's).

### 28.1 Tiempos de respuesta.





IQsec, S.A. de C.V. considerará 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.

CONCEPTO	Atención y solución de las incidencias o problemas con base a su complejidad			
	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.
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

## 29. ENTREGABLES.

**IQsec, S.A. de C.V.** considerará 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.

**IQsec, S.A. de C.V.**, acepta que 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, así mismo se considera lo que se expresa a continuación y las modificaciones que se acuerden en el plan de trabajo en común acuerdo no serán motivo de penalización.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 11 de la empresa "**IQsec S.A. DE C.V.**" de la página 13 de 36 que a la letra dice:



*"Se le solicita amablemente a la convocante nos ayude a precisar si se podrán realizar modificaciones a las fechas de implementación del plan de trabajo de acuerdo con las operaciones del día al día del INSTITUTO, en caso de ser afirmativa la respuesta no aplicaría la pena convencional en caso de que el atraso sea imputable a los tiempos de implementación del INSTITUTO".*

**"Se acepta su solicitud, se podrán realizar modificaciones al plan de trabajo en conjunto entre el licitante ganador y el Instituto. Siempre y cuando ambas partes esten de acuerdo."**

#### Entregables de Inicio del proyecto:

- Minuta de la Reunión de Kick Off.
- Plan de Trabajo General.
- Plan de Trabajo detallado por Servicio a Implementar
- Memoria Técnica de cada servicio implementado

#### 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 Cyberpatrullaje e integridad de imagen institucional. (dark web y deep web)
- Reporte de disponibilidad de recursos.
- 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 estadísticas e indicadores de concientización.
- Reporte de histórico de políticas de cifrado de archivos.
- Reporte de trazabilidad de SVI.
- Reporte de dependencia lógica de los servicios críticos.
- Reporte de afectaciones de activos.
- Reporte de implementación de SGSI.

IQsec, S.A. de C.V. en caso de resultar el licitante ganador proporcionará 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 a IQsec, S.A. de C.V. en caso de resultar el 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.

### 30. PENAS CONVENCIONALES Y DEDUCTIVAS.

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

PENAS CONVENCIONALES		
No.	Descripción	Monto
1	<u>Minuta de la Reunión de Kick Off</u> de este con el numeral 29. ENTREGABLES Anexo 13 "Características Técnicas del Servicio".	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 IQsec, S.A. de C.V., la cual deberá entregarse <u>a más tardar a los cinco días hábiles de haberse llevado a cabo la referida reunión.</u>
2	Atraso en la <u>entrega del Plan de Trabajo General</u> de conformidad con el numeral 29. ENTREGABLES Anexo 13 "Características Técnicas del Servicio".	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 <u>a más tardar a los cinco días hábiles después de firmado el Contrato.</u>
3	Atraso en la entrega del <u>Plan de Trabajo Detallado por Servicio a Implementar</u> , de acuerdo con las necesidades del servicio integral de conformidad con el numeral 29 ENTREGABLES Anexo 13 "Características Técnicas del Servicio".	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	<u>Memoria Técnica</u> de cada Servicio Implementado de conformidad con el numeral 29 ENTREGABLES del Anexo 13 "Características Técnicas del Servicio".	1% del monto total mensual del mes en cuestión, por día natural de atraso en la <u>entrega de la Memoria Técnica</u> , la cual deberá entregarse <u>a más tardar a los cinco días de concluido la implementación respectiva del servicio correspondiente.</u>
5	Atraso en los tiempos establecidos en la <u>implementación</u> de los servicios objetos de conformidad con el numeral 29 ENTREGABLES del Anexo 13 "Características Técnicas del Servicio".	3% del monto total mensual del mes en cuestión, por día natural de atraso en la <u>implementación</u> de cada uno de los servicios objeto del presente, de acuerdo a su plan de trabajo detallado correspondiente.

#### DEDUCTIVAS.

De acuerdo con lo previsto por los artículos 53 BIS de La Ley y 97 de El Reglamento, el Instituto FONACOT aplicará a IQsec, S.A. de C.V., en caso de ser el licitante ganador, deductivas de conformidad con lo siguiente:



DEDUCTIVAS		
No.	Descripción	Monto
1	Incumplimiento parcial o entrega mal realizada o incompleta en los <u>niveles de servicio</u> establecidos en el numeral 28. <b>NIVELES DE SERVICIO (SLA's), del Anexo 13 "Características Técnicas del Servicio",</b>	3% del monto total mensual del mes en cuestión, por incumplimiento parcial o entrega mal realizada o incompleta a los <u>niveles de servicio</u> .
2	Incumplimiento en la <u>entrega total</u> de cada uno de los servicios, ya sea por mala realización o entrega incompleta, de cualquiera de los servicios plasmados en el numeral 4. <b>DESCRIPCIÓN GENERAL DEL SERVICIO del Anexo 13 "Características Técnicas del Servicio",</b>	3% del monto total mensual del mes en cuestión, por incumplimiento en la <u>entrega total</u> 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 parcial o entrega mal realizada o incompleta en los tiempos establecidos en la <u>implementación</u> de los servicios establecidos en el 4. <b>DESCRIPCIÓN GENERAL DEL SERVICIO del Anexo 13 "Características Técnicas del Servicio".</b>	3% del monto total mensual del mes en cuestión, por día natural por incumplimiento parcial o entrega mal realizada o incompleta en la <u>implementación</u> de cada uno de los servicios.
4	Incumplimiento en el tiempo de asignación o reemplazo de los recursos humanos, establecidos en el numeral 15. <b>ADMINISTRACIÓN DE LOS SERVICIOS del Anexo 13 "Características Técnicas del Servicio.</b>	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.
5	Incumplimiento parcial o entrega mal realizada o incompleta por cada uno de los entregables mensuales, establecidos en el numeral 15. <b>ADMINISTRACIÓN DE LOS SERVICIOS del Anexo 13 "Características Técnicas del Servicio".</b>	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.

### 31. GARANTÍA DE CUMPLIMIENTO DE CONTRATO PLURIANUAL.

IQsec, S.A. de C.V. en caso de resultar el licitante adjudicado garantizará 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** y el artículo 87 del **RLey**, 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 **RLey**, 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 se redactará en la forma y términos establecidos en el **Anexo 16** de esta convocatoria.
- **La no entrega de la garantía es motivo de rescisión del contrato.**

### 32. GARANTÍA DE RESPONSABILIDAD CIVIL

**IQsec, S.A. de C.V.** en caso de resultar 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 de **IQsec, S.A. de C.V.**, en caso de ser el licitante ganador, por la ejecución de los servicios que se contraten derivados de este procedimiento. La cual será entregada dentro de los 5 días hábiles posteriores al Acto de Fallo en la Dirección de Tecnologías de la Información sitó 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 válida la garantía por responsabilidad civil que IQsec, S.A. de C.V. en caso de resultar el licitante ganador se obliga a presentar al Administrador del Contrato.

En caso de que algún siniestro supere el monto de la Póliza requerida, IQsec, S.A. de C.V. en caso de resultar el licitante ganador se hará cargo de la totalidad de los gastos que este llegue a generar.





### 33. GARANTÍA DE RESPONSABILIDAD LABORAL.

Queda expresamente estipulado que el personal de IQsec,S.A. de C.V. en caso de resultar el 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 a IQsec, S.A. de C.V. en caso de resultar el 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.

### 34. 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 CERT (COMPUTER EMERGENCY RESPONSE TEAM, EQUIPO DE RESPUESTA ANTE EMERGENCIAS INFORMÁTICAS)

### 35. CONFIDENCIALIDAD.

Con motivo de la prestación del servicio el Instituto FONACOT proporcionará a IQsec, S.A. de C.V. en caso de resultar el licitante ganador toda la información y documentación necesaria para el debido desempeño de sus funciones, misma que IQsec, S.A. de C.V. en caso de resultar 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 a IQsec, S.A. de C.V. en caso de resultar el licitante ganador, así como toda la información que IQsec, S.A. de C.V. en caso de resultar 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 IQsec, S.A. de C.V. en caso de resultar el licitante ganador, 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 IQsec, S.A. de C.V. en caso de resultar 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 IQsec, S.A. de C.V. en caso de resultar el licitante ganador sea constitutiva de delito, en perjuicio del Instituto FONACOT, ésta podrá proceder a 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.

### 36. ADMINISTRACIÓN DEL CONTRATO

El administrador del contrato será el titular de la **Subdirección General de Tecnologías 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 a lo descrito en este Anexo Técnico.

### 37. GLOSARIO

Es un documento que define los principales términos usados en el proyecto. Permite establecer una terminología consensuada.



Elemento	Descripción
Certificación CEH	Certified Ethical Hacker
Certificación CHFI	Computer Hacking Forensic Investigator
CRISC	Certified Risk Information System Control.
ITIL	(Information Technology Infrastructure Library). Biblioteca de infraestructura de Tecnologías de Información.
ITIL Expert	Certificación de ITIL nivel Expert.
PMI.	(Project Management Institute), Instituto de Administración de Proyectos que emite las mejores prácticas de gestión de proyectos.
PMP.	(Project Management Professional). Es una certificación de experiencia en gestión de proyectos ofrecida por el Project Management Institute.
DTI.	Dirección de Tecnologías de Información del Instituto FONACOT.
SGDTI.	Subdirección General de Tecnologías de la Información del Instituto FONACOT.
Instituto FONACOT	El Instituto del Fondo Nacional para el Consumo de los Trabajadores (Instituto FONACOT), a través de la Dirección de Recursos Materiales y Servicios Generales, en adelante el Instituto FONACOT.
TIC'S.	(Technology Information Communication). Tecnologías de información y comunicaciones.
SLA'S.	(Service Level Agreement). Niveles de servicio acordados por el negocio.
LAASSP	Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
MAAGTIC-SI.	Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI).
ORDEN DE SERVICIO	Documento procesado por una herramienta de software para la administración y control de servicios o productos específicos requeridos



Elemento	Descripción
	por el Instituto FONACOT al licitante ganador, estableciéndose puntualmente el esfuerzo y plan de trabajo detallado.
PLAN DE TRABAJO DEL PROYECTO.	Es un instrumento documental donde el licitante ganador deberá de describir las actividades, la asignación de sus recursos y los tiempos y movimientos del trabajo a realizar la construcción de la solución, por lo cual, la principal función de este artefacto es formalizar la ejecución de un proyecto específico.

### 38. REQUISITOS Y CARACTERÍSTICAS MÍNIMAS.

IQsec, S.A. de C.V. cumplirá los siguientes requisitos mínimos para ser objeto de evaluación por puntos y porcentajes. El incumplimiento de alguno de éstos, será motivo de no evaluación a través de puntos y porcentajes.

Las siguientes características mínimas, serán evaluadas en las visitas que la Convocante realizará a las instalaciones de **IQsec, S.A. de C.V.**, Anexo 13-A "Visita a las Instalaciones".

**IQsec, S.A. de C.V.** presentará en su propuesta mapa de ubicación (en un radio no mayor a 20 kilómetros del edificio Sede de la Convocante) y escrito (firmado por el representante legal, en el que manifieste el domicilio de **IQsec, S.A. de C.V.** donde se llevará a cabo la Visita a las instalaciones, adicionalmente deberá señalar que cumple con los siguientes requisitos y características mínimas:

#### 38.1 Conectividad.





Conectividad entre la Convocante e **IQsec, S.A. de C.V.** en caso de resultar el licitante ganador para proporcionar el servicio el "**Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones**".

**a. Enlace dedicado.**

**IQsec, S.A. de C.V.** contará con la infraestructura de telecomunicaciones necesaria para lograr la comunicación con la Convocante, ya que es requisito que el **IQsec, S.A. de C.V.** en caso de resultar el licitante ganador provea un enlace dedicado como medio de comunicación y los mecanismos de seguridad de acceso a la infraestructura tecnológica de la Convocante.

Los costos derivados por la conectividad deberán estar inmersos en los precios unitarios o precios por servicio en la propuesta económica, sin hacer diferencia alguna o proporcionar el detalle de dicho costo.

**b. El ancho de banda.**

Deberá ser al menos de 4mbps, para brindar un servicio aceptable. La utilización del enlace no deberá sobrepasar el 70% de su capacidad, si fuera éste el caso, **IQsec, S.A. de C.V.** en caso de resultar el licitante ganador realizará las actividades necesarias para mantener la capacidad del enlace conforme a lo solicitado. La relación con el proveedor de dicho enlace será responsabilidad de **IQsec, S.A. de C.V.** en caso de resultar el licitante ganador.

**c. Disponibilidad.**

El enlace que se utilice para comunicar la red de datos de **IQsec, S.A. de C.V.** en caso de resultar el licitante ganador con la de la Convocante, tendrá al menos una disponibilidad del 97% mensual. **IQsec, S.A. de C.V.** en caso de resultar el licitante ganador entregará un reporte que detalle la disponibilidad mensualmente.

**d. Seguridad en la conectividad.**



La administración, configuración y monitoreo de la infraestructura de comunicaciones (firewalls, routers, IDS, etc.) que brinden la seguridad en la conectividad entre las instalaciones de la Convocante e **IQsec, S.A. de C.V.** en caso de resultar el licitante ganador, será responsabilidad de este último.

Las especificaciones de las políticas de seguridad (físicas y lógicas) que se deberán manejar serán indicadas **IQsec, S.A. de C.V.**, en caso de ser el licitante ganador,

### 38.2 Elementos o características de las instalaciones de los licitantes participantes.

Las instalaciones de **IQsec, S.A. de C.V.** tienen como mínimo las siguientes características:

38.2.1 Cuentan con el espacio suficiente para albergar cómo mínimo a 50 personas, así como también el personal requerido para llevar a cabo este Anexo 13 "Características Técnicas del Servicio", además de contar con seguridad perimetral.

38.2.2 Cuarto de comunicaciones.

El cual cuenta con un área exclusiva para este fin, donde estarán albergados todos los equipos y dispositivos de red y comunicaciones.

38.2.3 UPS's (por sus siglas en inglés: uninterruptible power supply).

Baterías almacenadores de energía para soportar la operación del personal asignado al proyecto objeto de la presente licitación.

38.2.4 Seguridad de accesos.

El área para el desarrollo de las actividades de seguridad destinada a los proyectos de la Convocante deberá tener Seguridad de accesos físicos, lógicos y de comunicaciones.





- a. Será un área exclusiva para la Convocante dentro de las instalaciones de IQsec, S.A. de C.V. en caso de resultar el licitante ganador, la cual atenderá en su totalidad los requerimientos objeto de este **Anexo 13 "Características Técnicas del Servicio"**.
- b. Contará con los equipos de cómputo de los ingenieros de soporte para realizar los trabajos objeto de este **Anexo 13 "Características Técnicas del Servicio"**, y en su caso, estos estarán preparados de modo que se impida la extracción de información hacia medios magnéticos, ópticos y por internet; dicha funcionalidad no generará un costo adicional al Instituto FONACOT.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 8 de la empresa "INFOSOLUCIONES S.A. DE C.V." de la página 20 de 36 que a la letra dice:

*"Se le solicita amablemente a la Convocante permita que para cumplir con el punto antes referido se puedan presentar los equipos de cómputo con lo que cuenta la licitante como parte de su equipo operativo y que estos cuenten con su solución de seguridad de end point actualizada y vigente para el cumplimiento de la seguridad solicitada en el numeral b.*

*¿Se acepta nuestra propuesta?"*

**Respuesta de la Convocante: Se acepta su propuesta siempre y cuando como parte del servicio en caso de ser adjudicado se integre a los equipos de cómputo de los ingenieros de soporte la solución solicitada por el Instituto para protección de estaciones de trabajo son que esto genere un costo adicional al instituto.**

- c. Contará con una red de datos independiente y segura.
- d. Contará con acceso físico controlado mediante un mecanismo personalizado y automatizado (ej. Tarjeta de acceso, lector biométrico o claves).
- e. Esquema de accesos controlados (ej. Bitácoras, monitoreo, etc.).
- f. Todos y cada uno de los recursos asignados al proyecto tendrán dominio y fluidez del idioma español (México).

### 38.3 VISITA A LAS INSTALACIONES



La Convocante realizará la visita a las instalaciones de IQsec, S.A. de C.V. con la finalidad de evaluar lo establecido en este **numeral 38. REQUISITOS Y CARACTERÍSTICAS MÍNIMAS** del **Anexo 13 "Características Técnicas del Servicio"** y lo solicitado en el **Anexo 13-A "Visita a las Instalaciones"**.

**IQsec, S.A. de C.V.** cumplirá con las condiciones especificadas, para tal efecto, el Instituto FONACOT a través de la Subdirección General de Tecnologías de la Información y Comunicación, levantará y llenará el **Anexo 13-A "Visita a las Instalaciones"**, el cual formara parte de su evaluación y estará validado por ambas partes con la firma autógrafa de IQsec, S.A. de C.V. y del Área Técnica y Requirente.

**IQsec, S.A. de C.V.**, en caso de ser el licitante ganador, acepta que el no cumplir con los requerimientos establecidos en el **Anexo 13-A "Visita a las Instalaciones"**, será motivo para no ser evaluado a través de puntos y porcentajes.

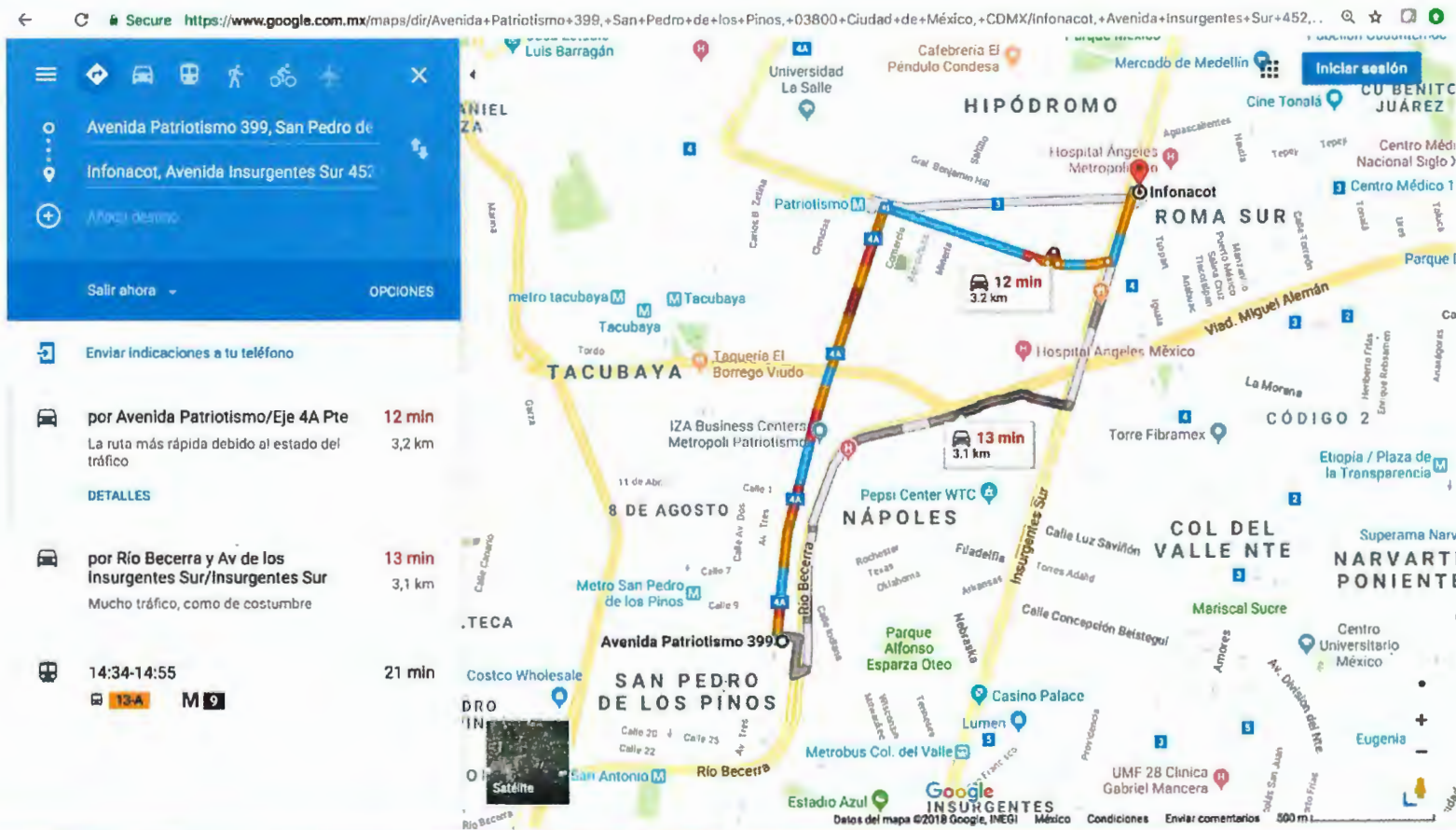
**IQsec, S.A. de C.V.** a continuación presenta mapa de ubicación (en un radio no mayor a 20 kilómetros del edificio Sede de la Convocante) y escrito (firmado por el representante legal, en el que manifieste el domicilio de **IQsec, S. A. de C.V.** donde se llevará a cabo la Visita a las instalaciones, de conformidad con lo solicitado en el inciso **D.** del numeral **V.1. PROPOSICIÓN TÉCNICA.**



## Mapa de Ubicación

### III.4.2.1. Visita a las instalaciones.

Párrafo 4. Mapa de ubicación. La distancia entre el edificio Sede de la Convocante e IQsec, S.A. de C.V., corresponde a 3.2 km. Aproximadamente, lo cual se muestra de manera gráfica en la siguiente imagen extraída de la aplicación web denominada Google Maps.



Patriotismo 399, San Pedro de los Pinos, 03800, CDMX.  
RFC: IQsec, S.A. De C.V. / IQS0708233C9

LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



Ciudad de México, a 5 de julio de 2018.

**Instituto del Fondo Nacional para el Consumo de los Trabajadores**

**Presente.**

Yo C. Yolanda Saldaña Tavera en mi carácter de Aproderado Legal de la empresa IQsec, S.A de C.V., según se acredita en el Testimonio Notarial No. 96,546 de fecha 18 de febrero de 2014 otorgado ante la fe del Notario Público No. 140 de la Ciudad de México, manifiesto que el domicilio donde se llevará a cabo la Visita a las Instalaciones de IQsec, S.A. de C.V. corresponde a:

**Domicilio:** Avenida Patriotismo Núm. 399.

**Colonia:** San Pedro de los Pinos.

**Delegación:** Benito Juárez.

**Código Postal:** 03800.

**Entidad Federativa:** Ciudad de México.

**Telefonos:** (55) 4163-1700.

Patriotismo 399, San Pedro de los Pinos, 03800, CDMX.  
RFC: IQsec, S.A. De C.V. / IQS0708233C9

000263





Así mismo, señalo que IQsec, S.A. de C.V., cumple con los siguientes requisitos y características mínimas:

**1.1. Conectividad.**

Conectividad entre la Convocante e IQsec, S.A. de C.V. en caso de resultar el licitante ganador para proporcionar el **Servicio Integral de Fortalecimiento en la Gestión, Administración y Control de la Seguridad de las Tecnologías de la Información y Comunicaciones.**

**a. Enlace dedicado.**

IQsec, S.A. de C.V. cuenta con la infraestructura de telecomunicaciones necesaria para lograr la comunicación con la Convocante, ya que es requisito que IQsec, S.A. de C.V. en caso de resultar el licitante ganador provea un enlace dedicado como medio de comunicación y los mecanismos de seguridad de acceso a la infraestructura tecnológica de la Convocante.

Los costos derivados por la conectividad estarán inmersos en los precios unitarios o precios por servicio en la propuesta económica, sin hacer diferencia alguna o proporcionar el detalle de dicho costo.

**b. El ancho de banda.**

Será al menos de 4mbps, para brindar un servicio aceptable. La utilización del enlace no sobrepasará el 70% de su capacidad, si fuera éste el caso, IQsec, S.A. de C.V. en caso de resultar el licitante ganador realizará las actividades necesarias para mantener la capacidad del enlace conforme a lo solicitado.

La relación con el proveedor de dicho enlace será responsabilidad de IQsec, S.A. de C.V.

**c. Disponibilidad.**

El enlace que se utilice para comunicar la red de datos de IQsec, S.A. de C.V. en caso de resultar el licitante ganador con la de la Convocante, tendrá al menos una disponibilidad del 97% mensual.



**d. Seguridad en la conectividad.**

La administración, configuración y monitoreo de la infraestructura de comunicaciones (firewalls, routers, IDS, etc.) que brinden la seguridad en la conectividad entre las instalaciones de la Convocante e IQsec, S.A. de C.V., será responsabilidad de este último.

Las especificaciones de las políticas de seguridad (físicas y lógicas) que se deberán manejar serán indicadas a IQsec, S.A. de C.V. en caso de resultar el licitante ganador.

**1.2. Elementos o características de las instalaciones de los licitantes participantes.**

Las instalaciones de IQsec, S.A. de C.V. tienen como mínimo las siguientes características:

Cuenta con el espacio suficiente para albergar como mínimo a 50 personas, así como también el personal requerido para llevar a cabo los servicios detallados en el **Anexo 13 "Características Técnicas del Servicio"**, además de contar con seguridad perimetral.

**1.2.1. Cuarto de comunicaciones.**

El cual cuenta con un área exclusiva para este fin, donde están albergados todos los equipos y dispositivos de red y comunicaciones.

**1.2.2. UPS's (por sus siglas en inglés: uninterruptible power supply).**

Baterías almacenadores de energía para soportar la operación del personal asignado al proyecto objeto de la presente licitación.

**1.2.3. Seguridad de accesos.**

El área para el desarrollo de las actividades de seguridad destinada a los proyectos de la Convocante tiene Seguridad de accesos físicos, lógicos y de comunicaciones.





- a. Será un área exclusiva para la Convocante dentro de las instalaciones de IQsec, S.A. de C.V. en caso de resultar el licitante ganador, la cual atenderá en su totalidad los requerimientos objeto de este **Anexo 13 "Características Técnicas del Servicio"**.
- b. Contará con los equipos de cómputo necesarios para realizar los trabajos objeto de este **Anexo 13 "Características Técnicas del Servicio"**, y en su caso, estos estarán preparados de modo que se impida la extracción de información hacia medios magnéticos, ópticos y por internet. dicha funcionalidad no generará un costo adicional al Instituto FONACOT.

De acuerdo con la junta de aclaraciones de bases y considerando la respuesta a la pregunta número 8 de la empresa "INFOSOLUCIONES S.A. DE C.V." de la página 20 de 36 que a la letra dice:

*"Se le solicita amablemente a la Convocante permita que para cumplir con el punto antes referido se puedan presentar los equipos de cómputo con lo que cuenta la licitante como parte de su equipo operativo y que estos cuenten con su solución de seguridad de end point actualizada y vigente para el cumplimiento de la seguridad solicitada en el numeral b.*

*¿Se acepta nuestra propuesta?"*

**Respuesta de la Convocante: Se acepta su propuesta siempre y cuando como parte del servicio en caso de ser adjudicado se integre a los equipos de cómputo de los ingenieros de soporte la solución solicitada por el Instituto para protección de estaciones de trabajo sin que esto genere un costo adicional al instituto.**

- c. Cuenta con una red de datos independiente y segura.
- d. Cuenta con acceso físico controlado mediante un mecanismo personalizado y automatizado (ej. Tarjeta de acceso, lector biométrico o claves).
- e. Esquema de accesos controlados (ej. Bitácoras, monitoreo, etc.).
- f. Todos y cada uno de los recursos asignados al proyecto tendrán dominio y fluidez del idioma español (México).

LICITACIÓN PÚBLICA ELECTRÓNICA NACIONAL CON REDUCCIÓN DE PLAZOS

No. LA-014P7R001-E349-2018

RELATIVA A LA:

"Contratación plurianual del servicio integral de fortalecimiento en la gestión, administración y control de la seguridad de las tecnologías de la información y comunicaciones".



**Atentamente,**

**Yolanda Saldaña Tavera.**  
**Apoderado Legal**

**IQsec, S.A. de C.V.**

El calendario de visitas se dará a conocer en el acto de apertura de propuestas, una vez que se hayan recibido las propuestas técnicas y económicas de los licitantes y será en el orden en que fueron recibidas sus propuestas. Se levantará una constancia de evaluación de la visita de acuerdo con el **Anexo 13-A "Visita a las Instalaciones"**.



## ANEXO II PROPUESTA ECONÓMICA

El presente Anexo consta de 2 páginas, el cual una vez rubricado por las partes, formará parte integrante del Contrato I-SD-2018-114.

Visto Bueno del Área Requirente \_\_\_\_\_

*[Handwritten signature]*

Ciudad de México, a 2 de julio de 2018.

**ANEXO 11**  
**FORMATO PARA LA PRESENTACIÓN DE LA PROPUESTA ECONÓMICA**

IQsec, S.A. de C.V. a fin de integrar su cotización considerará lo establecido en el **Anexo 13 "Características Técnicas del Servicio"**.

IQsec, S.A. de C.V. presenta sus precios en moneda nacional, la vigencia de la cotización es por los ejercicios fiscales 2018, 2019, 2020 y 2021, los precios son fijos e inalterables durante la vigencia del contrato, así como nuestra conformidad a las condiciones de pago establecidas en esta convocatoria. IQsec, S.A. de C.V. acepta que en caso de alguna suspensión del procedimiento por parte de la Secretaría de la Función Pública, la propuesta permanecerá vigente hasta en tanto quede sin efecto la suspensión.

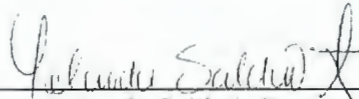
No.	Concepto	P. Unitario Mensual (A)	Cantidad de Meses (B)	Total 35 meses (A*B)
1.	Servicio de Gestión, Seguimiento y Control de Incidentes	\$ 566,909.13	35	\$ 19,841,819.55
2.	Servicio de Validación de Identidad	\$ 614,516.37	35	\$ 21,508,072.95
3.	Servicio de detección e investigación de vulnerabilidades y prueba de penetración.	\$ 499,055.14	35	\$ 17,466,929.90
4.	Servicio de Control y Gestión de Usuarios	\$ 519,849.11	35	\$ 18,194,718.85
5.	Servicio de Protección de Base de Datos	\$ 653,532.41	35	\$ 22,873,634.35
6.	Servicio de Protección y reputación de identidad institucional.	\$ 540,451.55	35	\$ 18,915,804.25
7.	Servicio de sensibilización de tecnologías de la Información	\$ 435,578.83	35	\$ 15,245,259.05
8.	Servicio Administrado del SGSI	\$ 699,333.85	35	\$ 24,476,684.75
9.	Servicio de Protección de Estaciones de Trabajo	\$ 418,615.34	35	\$ 14,651,536.90
10.	10 Recursos en Sitio (El licitante deberá considerar para su propuesta económica al menos 10 recursos en sitio de manera mensual que cuenten con el perfil de "Personal en Sitio".	\$ 524,226.79	35	\$ 18,347,937.65
Subtotal antes de IVA				\$ 191,522,398.20
IVA				\$ 30,643,583.71
Costo Total del Servicio				\$ 222,165,981.91

Importe con letra (Antes de IVA): Ciento noventa y un millones quinientos veintidos mil trescientos noventa y ocho pesos 20/100 M.N.





**Atentamente,**



**Yolanda Saldaña Tavera.**

**Apoderado Legal  
IQsec, S.A. de C.V.**

**Notas:**

- El pago se realizará en pagos mensuales, excepto el primer mes, el cual se pagará, si fuera el caso, de manera proporcional a partir del siguiente día hábil del fallo y hasta el final de este mes en cuestión, de acuerdo a los servicios devengados debidamente soportado y acompañado con los entregables que apliquen de acuerdo al numeral "29 ENTREGABLES", del Anexo 13 "Características Técnicas del Servicio".
- El precio ofertado ya considera todos los costos hasta la conclusión total de la prestación del servicio conforme a las especificaciones técnicas solicitadas por la convocante.
- El importe deberá expresarse con **dos decimales. (0.00)**, en caso de que algún importe sea expresado con tres o más decimales, la convocante considerará los dos primeros decimales del referido precio.
- El licitante, en términos de lo establecido en el **inciso F. del numeral VI.1.1.** de la convocatoria acepta, que la convocante, de ser el caso realice las correcciones a los errores aritméticos que pudieran detectarse en su propuesta, siempre y cuando ésta no afecte precios unitarios. Y que de no estar de acuerdo contará con 24 horas posteriores al fallo para comunicarlo por escrito a la convocante, a fin de que ésta proceda, conforme a lo establecido en el segundo párrafo del artículo 46 de **La Ley**.
- El presente documento podrá ser reproducido por cada licitante en el modo que estime conveniente, debiendo respetar su contenido, preferentemente en el orden indicado.

