Versión publica aprobada por el comité de Transparencia del instituto del Fondo Nacional para el Consumo de los Trabajadores, el día 9 de noviembre del 2022, en su Octava Sesión Ordinaria.

TRABAJO
SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL

INSTITUTO fonacot

CONTRATO No. FNCOT/AD/CAAS/005/2022

CONTRATO **ABIERTO PARA LA PRESTACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO, DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES**, QUE CELEBRAN, POR UNA PARTE, EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES REPRESENTADO POR LA C. ERIKA HELENA PSIHAS VALDÉS, EN SU CARÁCTER DE APODERADA LEGAL, EN ADELANTE **"EL INSTITUTO FONACOT"** Y, POR LA OTRA, LA EMPRESA DENOMINADA TECNOLOGIA EN SEGURIDAD Y COMUNICACIONES, S.A. DE C.V., EN LO SUCESIVO **"EL PRESTADOR"**, REPRESENTADA POR LA C. VICTORIA ISABEL MORALES AGUILAR, EN SU CARÁCTER DE APODERADA LEGAL, A QUIENES DE MANERA CONJUNTA SE LES DENOMINARÁ **"LAS PARTES"**, AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

- **DECLARACIONES**

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

I.1 Es un organismo público descentralizado de interés social, con personalidad jurídica y patrimonio propio, así como con autosuficiencia presupuestal y sectorizado en la Secretaría del Trabajo y Previsión Social, de conformidad con lo establecido en la Ley del Instituto del Fondo Nacional para el Consumo de los Trabajadores, publicada en el Diario Oficial de la Federación el 24 de abril del 2006.

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

I.3 De conformidad con numeral 8 inciso b)de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Instituto FONACOT, suscribe el presente instrumento el **C. Horacio Sánchez Tinoco**, en su calidad de Subdirector General de Tecnologías de la Información y Comunicación con R.F.C.SATH771010TB3 facultado para administrar el cumplimiento de las obligaciones que deriven del objeto del presente contrato, quien podrá ser sustituido en cualquier momento en su cargo o funciones, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, dirigido al representante de "EL PRESTADOR" para los efectos del presente contrato, encargados del cumplimiento de las obligaciones contraídas en el presente instrumento jurídico.

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

I.5 La adjudicación del presente contrato se realizó mediante el procedimiento de **Adjudicación Directa por excepción a la Licitación Pública**, realizado al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos y en los artículos **25**, **26 fracción III, 40, 41 fracción I** en lo referente a Derechos exclusivos **y 47** de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"LAASSP"**, y los correlativos de su Reglamento contando con el dictamen favorable por parte del Comité de Adquisiciones, Arrendamientos y Servicios del Instituto FONACOT, en su Cuarta Sesión Extraordinaria, celebrada el 1° de julio de 2022.

I.6 **"EL INSTITUTO FONACOT"** cuenta con recursos suficientes y con autorización para ejercerlos en el cumplimiento de sus obligaciones derivadas del presente contrato, en la partida presupuestal **31904,** denominada **Servicios Integrales de Infraestructura de Computo** con oficio número **DICP-SP-**

2022-052, de fecha **18 de mayo de 2022,** emitido por la Dirección de Integración y Control Presupuestal del Instituto FONACOT.

I.7 Para efectos fiscales las Autoridades Hacendarias le han asignado el Registro Federal de Contribuyentes **IFN060425C53**.

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

II. "EL PRESTADOR" declara que:

II.1 Es una persona **moral** legalmente constituida mediante, la escritura pública número 38,055, de fecha 31 de marzo de 2005, otorgada ante la fe del Lic. Francisco Xavier Arredondo Galván, notario público número 173 del entonces Distrito Federal, hoy Ciudad de México, cuyo primer testimonio quedó inscrito en el Registro Público de Comercio de la Ciudad de México, bajo el folio mercantil número 333048, de fecha 30 de mayo de 2005.

Eliminado CLAVE DE ELECTOR. Ubicada en el séptimo renglón del sexto párrafo. Fundamento Legal: Artículo 116 de la Ley General de Transparencia y Acceso a la Información Pública y 113 fracción I de la Ley Federal de Transparencia y Acceso a Información Pública, en relación con el artículo 3 fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el Lineamiento Trigésimo Octavo fracción I de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información. **Motivación:** Es una clave única e irrepetible, que por su estructura permite identificar al titular, su edad y fecha de nacimiento, por lo que es un dato personal de carácter confidencial.

II.2 La **C. Victoria Isabel Morales Aguilar**, en su carácter de apoderada legal, cuenta con poder suficiente para suscribir el presente contrato, de conformidad con lo establecido en la escritura pública número 13,383, de fecha 23 de julio del 2021, otorgada ante la fe del Lic. Juan Carlos Salazar Cajica, titular de la notaría pública número 49 de la Heroica Ciudad de Puebla de Zaragoza, facultades que bajo protesta de decir verdad, no le han sido revocadas ni modificadas a la presente fecha y en este acto se identifica con credencial para votar con clave de elector No. [redacted] expedida por el Instituto Nacional Electoral.

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

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

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

II.6 Cuenta con su Registro Federal de Contribuyentes **TSC050331163.**

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

II.8 Señala como su domicilio para todos los efectos legales el ubicado en Calle Patricio Sanz No. 526, Colonia del Valle, C.P. 03100, Demarcación Territorial Benito Juárez, Ciudad de México.

III. De "LAS PARTES":

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

CLÁUSULAS

PRIMERA. OBJETO DEL CONTRATO.

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

SEGUNDA. DE LOS MONTOS Y PRECIOS

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

El monto total mínimo del mismo es por la cantidad de $26,475,438.66 M.N. (Veintiséis Millones cuatrocientos setenta y cinco mil cuatrocientos treinta y ocho pesos, 66/100 M.N.) y el monto total máximo del mismo es por la cantidad de $30,446,754.46 (Treinta millones cuatrocientos cuarenta y seis mil setecientos cincuenta y cuatro pesos, 46/100 M.N.) ambas cantidades antes de IVA.

Los precios unitarios son considerados fijos y en moneda nacional (pesos mexicanos) hasta que concluya la relación contractual que se formaliza, incluyendo **"EL PRESTADOR"** todos los conceptos y costos involucrados en la prestación del servicio de Canales de Atención a clientes FONACOT, por lo que **"EL PRESTADOR"** no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

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

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

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

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

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

Los CFDI's (facturas) deberán contar con el visto bueno del administrador del contrato y con los requisitos fiscales vigentes señalados en los artículos 29 y 29-A del Código Fiscal de la Federación Aplicable en los Estados Unidos Mexicanos, por lo que deberán:

A. Presentar comprobantes fiscales digitales por Internet (CFDI), en archivo XML y la representación de dichos comprobantes en documento impreso en papel, que reúnan los requisitos fiscales respectivos, en la que indique el servicio prestado y el número de contrato que lo ampara. Dichos comprobantes serán enviados y entregados de conformidad con lo solicitado en el **Anexo 12 "Características Técnicas del Servicio"**, mismos que deberán de ser entregados en las oficinas centrales del Instituto FONACOT, ubicadas en Avenida Insurgentes Sur No. 452, 5to. Piso, Colonia Roma Sur, Código Postal 06760, Demarcación Territorial Cuauhtémoc, Ciudad de México, quinto piso, en la Subdirección General de Tecnologías de la Información y Comunicación, así mismo deberá ser enviada al correo electrónico horacio.sanchez@fonacot.gob.mx en un horario de labores de las 9:00 a las 18:00 horas de lunes a viernes.

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

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

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

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

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

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

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

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

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

CUARTA. VIGENCIA

El contrato comprenderá una vigencia considerada a partir del 02 de julio del 2022 y hasta el 31 de diciembre del 2022 **"LAS PARTES"** están de acuerdo en que por necesidades de **"EL INSTITUTO FONACOT"** podrá ampliarse, la prestación del servicio objeto del presente contrato, de conformidad con el artículo 52 de la **"LAASSP"**, siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) del monto o cantidad de los conceptos y volúmenes establecidos originalmente. Lo

anterior, se formalizará mediante la celebración de un Convenio Modificatorio del Contrato Principal. Asimismo, con fundamento en el artículo 91 del Reglamento de la **"LAASSP"**, **"EL PRESTADOR"** deberá entregar las modificaciones respectivas de las garantías, señaladas en la **CLÁUSULA SÉPTIMA** de este contrato.

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

QUINTA. GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.

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

La fianza deberá entregarse en la Dirección de Recursos Materiales y Servicios Generales del Instituto FONACOT cita en Insurgentes Sur 452, piso 1, colonia Roma Sur, Demarcación Territorial Cuauhtémoc, C.P. 06760, en los tiempos mencionados en el párrafo anterior.

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

- Expedirse a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores con domicilio en Avenida Insurgentes Sur número 452, Colonia Roma Sur, Demarcación Territorial Cuauhtémoc, Código Postal. 06760, Ciudad de México;
- La indicación del importe total garantizado con número y letra;
- La referencia de que la fianza se otorga atendiendo a todas las estipulaciones contenidas en el contrato y el anexo respectivo, así como la cotización y el requerimiento asociado a ésta;
- La información correspondiente al número de contrato, su fecha de firma, así como la especificación de las obligaciones garantizadas;
- El señalamiento de la denominación o nombre de **"EL PRESTADOR"** y de la institución afianzadora, así como sus domicilios correspondientes;
- La condición de que la vigencia de la fianza deberá quedar abierta para permitir que cumpla con su objetivo, y continuará vigente durante la sustanciación de todos los recursos legales o juicios que se interpongan hasta que se dicte resolución definitiva por la autoridad competente, de forma tal que no podrá establecerse o estipularse plazo alguno que limite su vigencia, lo cual no debe confundirse con el plazo para el cumplimiento de las obligaciones previstas en el contrato y actos administrativos garantizados;
- La indicación de que la fianza se hará efectiva conforme al procedimiento dispuesto en el artículo 282 de la Ley de Instituciones de Seguros y de Fianzas, el cual será aplicable también para el cobro de los intereses que en su caso se generen en los términos previstos en el artículo 283 del propio ordenamiento;
- La indicación de que la cancelación de la póliza de fianza procederá una vez que **"EL INSTITUTO FONACOT"** otorgue el documento en el que se señale la extinción de derechos y obligaciones, previo otorgamiento del finiquito correspondiente, o en caso de existir saldos a cargo de **"EL PRESTADOR"**, la liquidación debida;
- Para acreditar a la institución afianzadora el incumplimiento de la obligación garantizada, tendrá que cumplirse con los requisitos establecidos en las Disposiciones Generales a que se sujetarán las garantías otorgadas a favor del Gobierno Federal para el cumplimiento de obligaciones distintas de las fiscales que constituyan las dependencias y entidades en los actos y contratos que celebren, publicadas en el Diario Oficial de la Federación el 08 de septiembre de 2015; y
- El momento de inicio de la fianza y, en su caso, su vigencia.

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

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

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

La garantía de cumplimiento de ninguna manera será considerada como una limitación de la responsabilidad de **"EL PRESTADOR"**, derivada de sus obligaciones y garantías estipuladas en el presente instrumento jurídico, y de ninguna manera impedirá que **"EL INSTITUTO FONACOT"** reclame la indemnización o el reembolso por cualquier incumplimiento que pueda exceder el valor de la garantía de cumplimiento.

En caso de incremento al monto del presente instrumento jurídico o modificación al plazo, **"EL PRESTADOR"** se obliga a entregar a **"EL INSTITUTO FONACOT"** dentro de los diez días naturales siguientes a la formalización del mismo, de conformidad con el último párrafo del artículo 91 del Reglamento de la **"LAASSP"**, los documentos modificatorios o endosos correspondientes, debiendo contener en el documento la estipulación de que se otorga de manera conjunta, solidaria e inseparable de la garantía otorgada inicialmente.

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

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

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

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

SEXTA. RESPONSABILIDAD CIVIL.

"EL PRESTADOR" se obliga a proporcionar al administrador del contrato una póliza expedida por institución autorizada por las Leyes Mexicanas a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores, por un importe mínimo de $1,000,000.00 (Un millón de pesos 00/100 M.N.) que garantice la protección de daños y perjuicios que pudieran presentarse como resultado de las actividades propias de **"EL PRESTADOR"** por la ejecución de los servicios derivados del presente contrato, y de conformidad al Anexo Técnico, que como Anexo I se agrega al presente Contrato, el cual una vez rubricado por las partes formara parte integrante del mismo, .

SÉPTIMA. OBLIGACIONES DE "EL PRESTADOR"

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

OCTAVA. OBLIGACIONES DE "EL INSTITUTO FONACOT"

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

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

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

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

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

DÉCIMA. LICENCIAS

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

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

DÉCIMA PRIMERA. CALIDAD

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

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

DÉCIMA SEGUNDA. RESPONSABILIDAD

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

DÉCIMA TERCERA. IMPUESTOS Y DERECHOS

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

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

DÉCIMA CUARTA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES

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

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

"EL PRESTADOR" asume la responsabilidad total en caso de que, la prestación de los servicios, objeto del presente contrato, infrinja patentes, marcas o viole otros registros de derechos de propiedad industrial a nivel nacional e internacional, por lo que, se obliga a responder personal e ilimitadamente de los daños y perjuicios que pudiera causar a **"EL INSTITUTO FONACOT"** o a terceros.

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

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

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

DÉCIMA SEXTA. CONFIDENCIALIDAD

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

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

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

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

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

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

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

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

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

"EL INSTITUTO FONACOT" designa como responsable de administrar y vigilar el cumplimiento del presente contrato al C. Horacio Sánchez Tinoco en su calidad de Subdirector General de Tecnologías de la información y Comunicación con el objeto de verificar el óptimo cumplimiento del mismo, por lo que indicará a **"EL PRESTADOR"** las observaciones que se estimen pertinentes, quedando éste obligado a corregir las anomalías que le sean indicadas, así como deficiencias en la entrega de los servicios o de su personal.

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

Los servicios serán recibidos previa revisión del administrador del contrato.

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

DÉCIMA OCTAVA. DEDUCCIONES

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

Disponibilidad de servicios.

La siguiente tabla muestra los porcentajes de deducción que se aplicarán sobre el costo mensual de los servicios correspondientes señalados en la propuesta económica:

Calidad de Servicios Lograda (Disponibilidad)		
Límite inferior	**Limite Superior**	**Porcentaje de la mensualidad a retener como deducción**
99.7%	100%	0%
99.3%	99.6999%	5%
99.1%	99.2999%	10%
98.9%	99.0999%	15%
98.7%	98.8999%	20%
98.5%	98.6999%	25%
98.3%	98.4999%	30%
98.1%	98.2999%	35%
97.9%	98.0999%	40%
97.7%	97.8999%	45%

D= Porcentaje de disponibilidad durante el periodo.

El área técnica de **"EL INSTITUTO FONACOT"** considerará de forma mensual la disponibilidad (D) de los servicios contemplando los tiempos establecidos en las coberturas limitada o amplia (TC) y Tiempos Fuera (TF) acumulados de acuerdo a la siguiente fórmula:

$$D = \frac{(TC - TF) \times 100}{TC}$$

Por falta de disponibilidad de un servicio que afecte u ocasione indisponibilidad o degradación de más servicios, se aplicara la deductiva correspondiente por cada uno de los servicios afectados o inaccesibles

Incidentes por fallas

La siguiente tabla muestra los porcentajes de deducción que se aplicarán sobre el costo total mensual del servicio Soporte Técnico considerando los costos señalados en la propuesta económica.

Calidad de Servicios Lograda (Cambio Estándar)		
Límite inferior	**Limite Superior**	**Porcentaje de deducción**
97%	100%	0%
94%	96.999%	10%
91%	93.999%	15%
88% o menor	90.999%	20%

El área técnica de **"EL INSTITUTO FONACOT"** considerará la siguiente fórmula para obtener el porcentaje de deducción mensual relacionado con la solución de incidentes por fallas que se encuentren fuera del nivel de servicio solicitado.

$$D = \frac{(ST - SF) \times 100}{ST}$$

D= Deducción.
ST= Solicitudes totales mensuales
SF= Solicitudes totales mensuales fuera de nivel de servicio

Cambios Estándar.

La siguiente tabla muestra los porcentajes de deducción que se aplicarán sobre el costo total mensual del servicio Soporte Técnico considerando los costos señalados en la propuesta económica

Calidad de Servicios Lograda (Cambio Estándar)		
Límite inferior	**Limite Superior**	**Porcentaje de deducción**
97%	100%	0%
94%	96.999%	10%
91%	93.999%	15%
88% o menor	90.999%	20%

El área técnica de **"EL INSTITUTO FONACOT"** considerará la siguiente fórmula para obtener el porcentaje de deducción mensual relacionado con las solicitudes de cambios estándar que se encuentren fuera del nivel de servicio solicitado.

$$D = \frac{(ST - SF) \times 100}{ST}$$

D= Deducción.
ST= Solicitudes totales mensuales
SF= Solicitudes totales mensuales fuera de nivel de servicio

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

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

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

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

al incumplimiento, el procedimiento de rescisión del contrato, considerando la gravedad del incumplimiento y los daños y perjuicios que el mismo pudiera ocasionar a los intereses del Estado, representados por **"EL INSTITUTO FONACOT"**.

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

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

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

VIGÉSIMA. PENAS CONVENCIONALES

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

INICIO DE OPERACIONES

Asignación de personal con perfil de Coordinador conforme a lo establecido en el punto SERVICIOS DE **COORDINACION del Anexo.**

Asignación de personal con perfil de soporte técnico conforme a lo establecido en el punto SOPORTE TECNICO para la administración de los servicios informáticos que se encuentran en operación en **"EL INSTITUTO FONACOT"**.

Considerando que el no contar con personal con perfil de coordinación y soporte técnico afectaría el inicio de operaciones del servicio, se aplicará una pena convencional por causa imputable a **"EL PRESTADOR"**, del 1% por cada día de atraso sobre el monto total del contrato considerando el costo señalado en la propuesta económica.

PUESTA A PUNTO DEL SERVICIO INTEGRAL ADMINISTRADO

- Switches de acceso.
- **Servicio de red inalámbrica en edificio Sede.**
- **Servicio de red inalámbrica en localidades.**
- Esquema de alta disponibilidad Tipo A.
- Esquema de alta disponibilidad Tipo B

Por atraso imputable a **"EL PRESTADOR"** en la puesta a punto de los servicios antes mencionados, se aplicará una pena convencional del 3% por cada día de atraso sobre el costo total mensual del servicio correspondiente, considerando los costos señalados en la propuesta económica.

- Archivos Compartidos en Red.
- Filtrado de contenidos Web.

Por atraso imputable a **"EL PRESTADOR"** en la puesta a punto de los servicios anteriores, se aplicará una pena convencional del 10% por cada día de atraso sobre el costo total mensual del servicio correspondiente, considerando los costos señalados en la propuesta económica.

- Herramienta de administración de la red.
- Servicio de administración de energía regulada (UPS).

Por atraso imputable a **"EL PRESTADOR"** en la puesta a punto de los servicios anteriores, se aplicará una pena convencional del 5% por cada día de atraso sobre el costo total mensual del servicio correspondiente, considerando los costos señalados en la propuesta económica.

- Cableado estructurado
  - Por atraso imputable a **"EL PRESTADOR"** en la entrega del plan de actividades, se aplicará una pena convencional del 3% por cada día de atraso sobre el costo total de la cantidad de nodos solicitados en el requerimiento.
  - Por atraso imputable a **"EL PRESTADOR"** en los tiempos establecidos en el plan de actividades que haya sido previamente autorizado por el personal técnico de **"EL INSTITUTO FONACOT"**, se aplicará una pena convencional del 5% por cada día de atraso sobre el costo total de la cantidad de nodos solicitados en el requerimiento
- Servicio bajo demanda.

  Por atraso imputable a **"EL PRESTADOR"** en la puesta a punto del servicio bajo demanda, se aplicará una pena convencional del 10% por cada día de atraso sobre el costo unitario correspondiente, tomando en consideración los costos establecidos en su propuesta económica.

- Solicitud de Cambio (RFCh).

Por atraso imputable a **"EL PRESTADOR"**, en el cumplimiento del plan de trabajo autorizado por el personal técnico del Instituto FONACOT, se aplicará una pena convencional del 1% diario sobre el costo mensual del servicio Soporte Técnicolicita, considerando el costo señalado en la propuesta económica.

SERCVICIO O EQUIPOS NO OTORGADOS

Cuando el servicio o el equipo no sea otorgado por causas imputables a **"EL PRESTADOR"**, no procederá pago alguno, asimismo, se aplicará una pena convencional del 5% por cada día de atraso del costo mensual del servicio, considerando los costos en la propuesta económica por los conceptos o bienes involucrados.

Lo anterior, de conformidad con el presente contrato y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta.

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

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

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

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

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

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

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

VIGÉSIMA PRIMERA. SANCIONES ADMINISTRATIVAS

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

VIGÉSIMA SEGUNDA. SANCIONES APLICABLES Y TERMINACIÓN DE LA RELACIÓN CONTRACTUAL

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

VIGÉSIMA TERCERA. RELACIÓN LABORAL

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

VIGÉSIMA CUARTA. EXCLUSIÓN LABORAL

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

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

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

VIGÉSIMA QUINTA. SUSPENSIÓN DE LA PRESTACIÓN DE LOS SERVICIOS.

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

Cuando la suspensión obedezca a causas imputables a **"EL INSTITUTO FONACOT"**, a solicitud escrita de **"EL PRESTADOR"**, cubrirá los gastos no recuperables, durante el tiempo que dure esta suspensión, para lo cual **"EL PRESTADOR"** deberá presentar dentro de los 30 (treinta) días naturales siguientes de la

notificación del término de la suspensión, la factura y documentación de los gastos no recuperables en que haya incurrido, siempre que estos sean razonables, estén debidamente comprobados y se relacionen directamente con el contrato.

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

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

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

VIGÉSIMA SÉXTA. RESCISIÓN

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

a) Si incurre en responsabilidad por errores u omisiones en su actuación;
b) Si incurre en negligencia en la prestación de los servicios objeto del presente contrato, sin justificación para **"EL INSTITUTO FONACOT"**;
c) Si transfiere en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual;
d) Si cede los derechos de cobro derivados del contrato, sin contar con la conformidad previa y por escrito de **"EL INSTITUTO FONACOT"**;
e) Si suspende total o parcialmente y sin causa justificada la prestación de los servicios del presente contrato o no les otorga la debida atención conforme a las instrucciones de **"EL INSTITUTO FONACOT"**;
f) Si no suministra los servicios en tiempo y forma conforme a lo establecido en el presente contrato y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta;
g) Si no proporciona a **"EL INSTITUTO FONACOT"** o a las dependencias que tengan facultades, los datos necesarios para la inspección, vigilancia y supervisión de los servicios del presente contrato;
h) Si cambia de nacionalidad e invoca la protección de su gobierno contra reclamaciones y órdenes de **"EL INSTITUTO FONACOT"**;
i) Si es declarado en concurso mercantil por autoridad competente o por cualquier otra causa distinta o análoga que afecte su patrimonio;
j) Si no acepta pagar penalizaciones o no repara los daños o pérdidas, por argumentar que no le son directamente imputables, sino a uno de sus asociados o filiales o a cualquier otra causa que no sea de fuerza mayor o caso fortuito;
k) Si no entrega dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato, la garantía de cumplimiento del mismo;
l) Si la suma de las penas convencionales excede el monto total de la garantía de cumplimiento del contrato y/o de las deducciones alcanzan el 20% (veinte por ciento) del monto total de este instrumento jurídico;
m) Si **"EL PRESTADOR"** no presta los servicios objeto de este contrato de acuerdo con las normas, la calidad, eficiencia y especificaciones requeridas por **"EL INSTITUTO FONACOT"** conforme a las cláusulas del presente contrato y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta;
n) Si divulga, transfiere o utiliza la información que conozca en el desarrollo del cumplimiento del objeto del presente contrato, sin contar con la autorización de **"EL INSTITUTO FONACOT"** en los términos de lo dispuesto en la cláusula DÉCIMA NOVENA del presente instrumento jurídico;
o) Si se comprueba la falsedad de alguna manifestación contenida en el apartado de sus declaraciones del presente contrato;

p) Cuando **"EL PRESTADOR"** y/o su personal, impidan el desempeño normal de labores de **"EL INSTITUTO FONACOT"**, durante la prestación del servicio, por causas distintas a la naturaleza del objeto del mismo;
q) Cuando exista conocimiento y se corrobore mediante resolución definitiva de autoridad competente que **"EL PRESTADOR"** incurrió en violaciones en materia penal, civil, fiscal, mercantil o administrativa que redunde en perjuicio de los intereses de **"EL INSTITUTO FONACOT"** en cuanto al cumplimiento oportuno y eficaz en la entrega de los servicios del presente contrato; y
r) En general, incurra en incumplimiento total o parcial de las obligaciones que se estipulen en el presente contrato o de las disposiciones de la **"LAASSP"** y su Reglamento.

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

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

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

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

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

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

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

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

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

Los intereses se calcularán sobre el monto de los pagos progresivos efectuados y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de **"EL INSTITUTO FONACOT"**.

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

VIGÉSIMA SÉPTIMA. TERMINACIÓN ANTICIPADA

"EL INSTITUTO FONACOT" podrá dar por terminado anticipadamente el presente contrato, cuando concurran razones de interés general o bien cuando por causas justificadas se extinga la necesidad de requerir los servicios originalmente contratados, y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas, se ocasionaría algún daño o perjuicio a **"EL INSTITUTO FONACOT"**, o se determine la nulidad total o parcial de los actos que dieron origen al contrato con motivo de una resolución de una inconformidad o intervención de oficio emitida por la Secretaría de la Función Pública, lo que bastará sea comunicado a **"EL PRESTADOR"** con 30 (treinta) días naturales anteriores al hecho. En este caso, **"EL INSTITUTO FONACOT"** a solicitud escrita de **"EL PRESTADOR"** cubrirá los gastos no recuperables, siempre que estos sean razonables estén debidamente comprobados y relacionados directamente con el contrato.

VIGÉSIMA OCTAVA. DISCREPANCIAS

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

VIGÉSIMA NOVENA. CONCILIACIÓN.

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

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

TRIGÉSIMA. DOMICILIOS

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

TRIGÉSIMA PRIMERA. LEGISLACIÓN APLICABLE

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

TRIGÉSIMA SEGUNDA. JURISDICCIÓN

"LAS PARTES" convienen que, para la interpretación y cumplimiento de este contrato, así como para lo no previsto en el mismo, se someterán a la jurisdicción y competencia de los Tribunales Federales en la

Ciudad de México, renunciando expresamente al fuero que pudiera corresponderles en razón de su domicilio actual o futuro.

Por lo anteriormente expuesto, tanto **"EL INSTITUTO FONACOT"** como **"EL PRESTADOR"**, declaran estar conformes y bien enterados de las consecuencias, valor y alcance legal de todas y cada una de las estipulaciones que el presente instrumento jurídico contiene, por lo que lo ratifican y firman por triplicado en la Ciudad de México, el día 15 de julio de 2022.

POR "EL INSTITUTO FONACOT"

C. ERIKA HELENA PSIHAS VALDÉS
APODERADA LEGAL Y ÁREA CONTRATANTE

POR "EL PRESTADOR"

C. VICTORIA ISABEL MORALES AGUILAR
APODERADA LEGAL

ADMINISTRADOR DEL CONTRATO

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

ANEXO I
ANEXO TÉCNICO

SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES

Anexo técnico

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

Contenido

1. INFORMACION GENERAL 4
1.1. ANTECEDENTES 4
1.2. OBJETIVO DEL SERVICIO 4

2. DESCRIPCIÓN DEL SERVICIO INTEGRAL ADMINISTRADO 5
2.1. ALCANCE DEL SERVICIO 5
2.2. IMPLEMENTACIÓN DEL SERVICIO 5
2.2.1. CONTINUIDAD OPERATIVA 5
2.3. ESPECIFICACIONES DEL SERVICIO 6
2.3.1. Servicio de Monitoreo de Infraestructura 6
2.3.2. Servicio de Switching 9
2.3.3. Switches de acceso 31
2.3.4. Red Inalámbrica 70
2.3.5. Archivos Compartidos en Red. 84
2.3.6. Servicio de Contención Perimetral. 86
2.3.7. CABLEADO ESTRUCTURADO 98
2.3.8. SERVICIO DE ADMINISTRACIÓN DE ENERGÍA REGULADA (UPS) 99
2.3.9. SOPORTE TÉCNICO 104
2.3.10. SERVICIOS BAJO DEMANDA 108
2.4. PLAN DE RETORNO 109
2.5. POLÍTICAS 109
2.6. GESTIÓN DEL SERVICIO. 110
2.6.1. ESCRITORIO DE SERVICIO. 110
2.6.2. ADMINISTRACIÓN DE INCIDENTES 111
2.6.3. ADMINISTRACIÓN DE PROBLEMAS 112
2.6.4. ADMINISTRACIÓN Y CAMBIOS DE LA CONFIGURACIÓN 112
2.6.5. SERVICIOS DE COORDINACIÓN. 112
2.7. ASPECTOS GENERALES 114
3. MANUALES, CATALOGOS Y FOLLETOS 115
4. PATENTES, MARCAS Y DERECHOS 115

5. MUESTRAS 115

6. PRUEBAS Y DESARROLLO A EFECTUAR A LAS MUESTRAS 115

7. LUGAR, PLAZO Y HORARIO DE LA PRESTACIÓN DEL SERVICIO 115

8. PLAZO PARA LA SUSPENSIÓN DEL SERVICIO 116

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 5351 52 05 74 00 www.fonacot.gob.mx

9. PAGO 116

10. ENTREGABLES 116
10.1. ENTREGABLES INICIALES 116
10.2. ENTREGABLES MENSUALES 117
10.3. ENTREGABLES FINALES 118
10.3.1. Memoria técnica 118

11. NIVELES DE SERVICIO 118
11.1. inicio de operaciones 118
11.2. PUESTA A PUNTO DEL SERVICIO INTEGRAL ADMINISTRADO 118
11.3. Cableado estructurado 119
11.4. Servicios bajo demanda 120
11.5. Incidentes por fallas 120
11.6. Cambios Estándar 121
11.7. Solicitud de Cambio (RFCh) 122

12. GARANTÍA DE CUMPLIMIENTO DEL CONTRATO 122

13. GARANTÍA DE RESPONSABILIDAD CIVIL 122

14. PENA CONVENCIONAL Y DEDUCTIVA 122
14.1. pena convencional 122
14.1.1. INICIO DE OPERACIONES 123
14.1.2. PUESTA A PUNTO DEL SERVICIO INTEGRAL ADMINISTRADO 123
14.1.3. SERCVICIO O EQUIPOS NO OTORGADOS 124
14.2. deductivas 125
Disponibilidad de servicios. 125
Incidentes por fallas 126
Cambios Estándar. 126

15. NORMAS APLICABLES 127

16. CONFIDENCIALIDAD 127

17. ADMINISTRADOR DEL CONTRATO 128
17.1. MODIFICACIONES QUE SE RESERVA EL ADMINISTRADOR DEL CONTRATO . 128

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

1. INFORMACION GENERAL

1.1. ANTECEDENTES

Actualmente el Instituto FONACOT dispone de un universo aproximado de 1,700 usuarios, de los cuales el 30% es personal de estructura, el 50 % operativo y el 20% externo. Este personal se encuentra distribuido en las Oficinas Centrales de Insurgentes, Edificio Plaza de la República, Direcciones Regionales, Estatales, Representaciones y/o Módulos ubicadas en distintas entidades federativas a nivel nacional, todos interconectados mediante una red VPN MPLS y en algunos casos mediante enlaces ADSL.
Asimismo, el Instituto FONACOT, cuenta con un centro de datos que soporta los servicios sustantivos, los cuales también se encuentran integrados a la red VPN MPLS.
Los elementos de infraestructura que conforman el prototipo de una localidad del Instituto FONACOT son los siguientes:

- Switch
- Access Points
- Equipo de energía ininterrumpible
- Cableado estructurado

1.2. OBJETIVO DEL SERVICIO

Gestionar, monitorear y en su caso suministrar los elementos necesarios de infraestructura de telecomunicaciones para la adecuada operación de las redes de área local, y los servicios informáticos del Instituto FONACOT, a fin de garantizar que las oficinas del Instituto FONACOT se encuentren intercomunicadas de manera óptima.

Los objetivos específicos a cubrir son los siguientes:

- Monitorear la disponibilidad y desempeño de la infraestructura tecnologica y servicios informáticos involucrados en el otorgamiento del servicio solicitado en este anexo tecnico.
- Administrar y operar los servicios solicitados, basándose en estándares internacionales como ITIL, para atender de manera oportuna los incidentes de administración y soporte tecnico.
- Atender cualquier eventualidad relacionada con los elementos de administración y seguridad propuesta, de acuerdo a los niveles de servicio.
- Operar el monitoreo, la administración de los servicios y redes en un esquema 7 x 24.
- Brindar el soporte técnico de manera remota preferentemente o en sitio, cumpliendo con los niveles de servicio establecidos.
- Brindar asesoría proactiva en el tratamiento de incidentes que involucran la aparición y/o detección de nuevas vulnerabilidades sobre los componentes de seguridad involucrados en el servicio solicitado.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Coordinar con el escritorio de servicio y con los diferentes grupos resolutores del Instituto FONACOT para dar respuesta a los incidentes relacionados con la administración del monitoreo de la infraestructura de red.
- Proporcionar los reportes de comprobación del cumplimiento de los niveles de servicio establecidos y de análisis de incidencias.

2. DESCRIPCIÓN DEL SERVICIO INTEGRAL ADMINISTRADO

2.1. ALCANCE DEL SERVICIO

En términos generales el servicio comprende los siguientes elementos, las características de cada uno de los servicios se expresa en el punto 2.4 ESPECIFICACIONES DEL SERVICIO

2.2. IMPLEMENTACIÓN DEL SERVICIO

2.2.1. CONTINUIDAD OPERATIVA

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

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

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

A continuación, se enlistan los servicios requeridos por el Instituto FONACOT:

SERVICIO INTEGRAL ADMINISTRADO

SERVICIO DE MONITOREO DE INFRAESTRUCTURA
SERVICIO DE SWITCHING.

- Herramienta de Administración de la Red
- Esquema de Alta Disponibilidad en Switches CORE Tipo A.
- Esquema de Alta Disponibilidad en Switches CORE Tipo B
- Switches de acceso
  - Switch de acceso Tipo1
  - Switch de acceso Tipo2
  - Switch de acceso Tipo 3
  - Switch de acceso Tipo4
  - Switch de acceso Tipo 5

RED INALÁMBRICA

- Servicio de red Inalambrica en edificio SEDE
- Servicio de red inalambrica en localidades

ARCHIVOS COMPARTIDOS EN RED

- FILESERVER
- FTP

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

GESTIÓN DE LA SEGURIDAD

- Servicio de Contención Perimetral
  - Firewall Tipo 1
  - Firewall Tipo 2

FILTRADO DE CONTENIDOS

- Filtrado de contenido Web

SERVICIO DE ADMINISTRACIÓN DE ENERGÍA REGULADA (UPS)

- UPS tipo 1, 3 KVA
- UPS tipo 2, 5 KVA
- UPS tipo 3, 8 KVA
- UPS tipo 4, 10 KVA
- UPS tipo 5, 16 KVA
- UPS tipo 6, 20 KVA
- UPS tipo 7, 30 KVA
- UPS tipo 8, 40 KVA
- UPS tipo 9, 100 KVA

CABLEADO ESTRUCTURADO

- Instalación de nodos nuevos
- Reubicación de nodos existentes
- Mantenimiento de nodos de red
- Instalación de Fibra Óptica
- Movimientos de infraestructura.

SOPORTE TÉCNICO.

SERVICIOS BAJO DEMANDA

TRANSFERENCIA DEL CONOCIMIENTO

PLAN DE RETORNO

- Políticas

GESTIÓN DEL SERVICIO.

Escritorio de servicio.

- Administración de incidentes
- Administración de problemas
- Administración y cambios de la configuración

Servicios de coordinación.

ASPECTOS GENERALES

2.3. ESPECIFICACIONES DEL SERVICIO

A continuación, se describen las especificaciones que el licitante deberá cumplir para proveer el Servicio Integral Administrado:

2.3.1. Servicio de Monitoreo de Infraestructura

El licitante deberá realizar el monitoreo de la disponibilidad, capacidad y rendimiento de la infraestructura de comunicaciones, servidores, bases de datos, aplicaciones y transacciones basadas en Java, a fin de que su utilización permita mantener la supervisión

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. +55 1 52 65 74 00 www.fonacot.gob.mx

ininterrumpida de la infraestructura, aplicaciones que soportan los sistemas institucionales y servicios informáticos del Instituto FONACOT.
El licitante deberá realizar el monitoreo de toda la infraestructura utilizando herramientas especializadas que cumpla al menos con las siguientes características técnicas:

- Debe soportar SNMP versión 1, 2 y 3. Deberá contener protocolos para monitoreo de ancho de banda además de SNMP: WMI, Netflow, jFlow, sFlow, Packet Sniffing.
- Deberá poseer un acceso HTML puro y debe ser accesible vía http o SSL.
- Deberá poseer un acceso a través de una aplicación nativa de Windows y una aplicación para dispositivos móviles que puedan ser utilizadas simultáneamente.
- Deberá ser capaz de realizar el monitoreo sin agentes.
- La herramienta deberá poder realizar monitoreo al menos de los siguientes aspectos: ancho de banda, aplicaciones, servidores virtuales, SLA, LAN, VPN, WAN y sitios distribuidos, monitoreo de QoS (para VoIP)
- Deberá soportar IPv6
- Deberá ser capaz de enviar notificaciones vía correo electrónico, y los recipientes deberán ser configurables por cada cuenta de usuario de la herramienta de forma independiente.
- Las notificaciones deben ser flexibles a modo de que la arquitectura sea tolerante a fallos (email, alertas en las aplicaciones móviles, Syslog, acciones HTTP o notificaciones en tecnologías externas a través de un EXE)
- La herramienta deberá proveer la opción de trabajar con un nodo Failover en cluster.
- Escalado de alertas que envíe una notificación extra cada cierto tiempo, durante el período de caída del dispositivo.
- Deberá existir una característica jerárquica en las notificaciones adjuntas e integradas a la jerarquía entre dispositivos, de modo que, si un dispositivo principal falla y esta característica está activa, las alarmas de todos los dispositivos que están jerárquicamente bajo el fallido sean silenciadas.
- Interfaz única para el monitoreo de dispositivos y aplicaciones.
- Proveer muestreo vía SNMP para dispositivos capa 2 y capa 3
- Al detectar alguna falla en algún dispositivo, deberá suprimir las alarmas dependientes de modo que solo la alarma de más alto nivel se reciba.
- Tener la capacidad de ejecutar comandos al recibir una alerta.
- Debe permitir la configuración personalizada de umbrales para las alarmas.
- Deber permitir la configuración de múltiples condiciones para desencadenar una alerta
- Deberá ser capaz de monitorear varias redes en diferentes localidades
- La interfaz del producto debe estar disponible en idioma español
- La documentación y manuales deberán estar disponibles al menos en idioma inglés
- Soportar distintos intervalos de muestreo dependiendo de la variable que se está interrogando.
- Debe ser compatible con plataforma Windows Server 2008 o superior.
- Debe permitir realizar búsquedas de los dispositivos por dirección IP, modelo, grupos, tecnologías.
- Deberá ser capaz de realizar un descubrimiento automático de la red
- Deberá contar con módulos integrados para el monitoreo de bases de datos SQL mediante un agente SNMP

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

EDP

- Deberá generar reportes en tiempo real enfocados a análisis de fallas, y acuerdos de calidad de servicio (SLA). Los reportes deberán ser generados mediante la recolección automática de datos y eventos de los diferentes dispositivos. De igual manera los reportes deberán ser generados bajo demanda o programados en esquema diario, semanal, mensual y enviados vía correo electrónico a la dirección o direcciones que el area técnica del Instituto FONACOT defina.
- Deberá tener la capacidad de generar tableros de control de acuerdo con lo siguiente:
    - Mapas y tableros de control. Deberá proveer tableros de control con información de rendimiento en tiempo real
    - Los tableros de control deberán ser diseñables de forma interactiva, ofreciendo diversos objetos gráficos y la posibilidad de importar imágenes para ser mostradas dentro del dashboard.
    - Deberá ser capaz de generar tableros de control por proceso, de acuerdo con las métricas de los dispositivos involucrados en cada proceso
- Reportes Detallados
    - Entregar reportes en HTML o PDF
    - Programar las tareas de los informes o hacerse ad-hoc
    - Posibilidad de exportar datos históricos de monitoreo para análisis, en formatos XML, CSV o HTML
    - Ofrecer gráficos con gran nivel de detalle, además de presentar los datos de forma tabular por métrica de los dispositivos
    - Mostrar tiempo productivo e improductivo, en segundos y en porcentaje
    - Mostrar un análisis top del uso de ancho de banda
    - Mostrar análisis top del uso de CPU
- Debe recolectar métricas de desempeño de redes, aplicaciones, servidores y servicios en tiempo real.
- Detección y notificación de fallas en tiempo real de redes, aplicaciones, servidores y servicios.
- Asegure la disponibilidad del servicio soportada por la infraestructura tecnológica.
- Debe realizar monitoreo proactivo para evitar la afectación de los niveles de servicio, alertando posibles fallos de acuerdo con los umbrales personalizables
- Debe ser capaz de realizar un análisis estadístico para detectar comportamientos inusuales de acuerdo con la información histórica del dispositivo
- Debe permitir a los usuarios la consulta de reportes a través de un navegador Web.
- Debe soportar encripción SSL para el envío de información entre redes monitoreadas en múltiples sitios
- Debe soportar HTTPS para Web y Windows
- Debe soportar control de acceso de usuarios de acuerdo a los siguientes puntos:
    - Manejar perfiles de usuario.
    - Que sea capaz de limitar a qué dispositivos puede acceder el usuario.
    - Que sea capaz de limitar los derechos de lectura/escritura, para sólo lectura
    - Debe permitir agendar mantenimientos de manera programada.
- Debe permitir configurar el tiempo límite de respuesta de un dispositivo.
- Debe utilizar una base de datos.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 65 74 00 www.fonacot.gob.mx

- Toda la información histórica debe ser almacenada en una base de datos única, a prueba de ataques SQL injection
- Debe ser auto administrable, de forma que no sea necesario la intervención humana para su administración.
- Debe ser fácilmente configurable y contar una GUI visual
- Los reportes y la interfaz web deberán ser personalizables para el del área técnica del Instituto FONACOT
- Debe ser capaz de importar archivos MIB para monitorear dispositivos de múltiples fabricantes
- Deberá contar con una API que permita crear, borrar y editar objetos de monitoreo

Como parte del servicio, el licitante ganador será responsable de proporcionar el licenciamiento necesario para que el personal autorizado del área técnica del Instituto FONACOT acceda a las consolas de monitoreo.

Como parte de este servicio, el licitante ganador durante toda la vigencia del servicio se obliga a realizar sin costo adicional para la convocante, todas las modificaciones, adecuaciones y/o cambios en los tableros (dashboards), contenedores, vistas, topologías, y cualquier actividad que permita optimizar la visualización de la información colectada por las diferentes herramientas de monitoreo consideradas en este rubro.

Es responsabilidad del licitante ganador mantener el licenciamiento vigente y efectuar las actualizaciones hacia las nuevas versiones disponibles e incorporando nuevas funcionalidades de las mismas durante toda la vigencia del contrato, sin costo adicional para la convocante.

El licitante ganador deberá presentar la información de disponibilidad, capacidad y rendimiento de la infraestructura monitoreada a través de una pantalla que deberá ubicarse en las oficinas centrales del Instituto FONACOT.

El licitante ganador deberá contemplar todos los accesorios necesarios para el montaje de la pantalla en el lugar que designe el área técnica del Instituto FONACOT, así como los componentes o elementos (cables e interfaces, etc.) que sean obligados para su operación.

El servicio de monitoreo deberá operar en infraestructura del licitante ganador, por lo que es responsabilidad del licitante mantener la configuración, parametrización y puesta a punto de las herramientas de monitoreo involucradas en el servicio solictado.

2.3.2. Servicio de Switching.

2.3.2.1. Herramienta de Administración de la Red

El licitante deberá llevar a cabo las actividades de administración de la infraestructura de switches propuestos, utilizando el software especializado Netsight Console, Policy Manager, Inventory Manager y NAC Manager propiedad del Instituto FONACOT. Este software cuenta con mantenimiento vigente hasta el 31 de mayo de 2022, por lo que es responsabilidad del licitante ganador mantenerlo vigente durante toda la vigencia del

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 5241 65 74 00 www.fonacot.gob.mx

servicio, así como, realizar lo necesario para dar continuidad al uso de estas herramientas actualizándolas a las nuevas versiones disponibles e incorporando las nuevas funcionalidades cubriendo al menos los siguientes puntos:

- Deberá permitir la administración centralizada de parámetros de todos los switches que suministre el licitante ganador para otorgar el servicio de Switching.
- Deberá permitir la aplicación de reglas de clasificación de tráfico de capas 2, 3 y 4, a usuarios, con el fin de asegurar el acceso de los mismos a los recursos de red que les corresponden.
- Deberá permitir mediante una interfaz Web tener visibilidad completa y un cierto nivel de control sobre todos los switches que conforman este servicio a fin de proporcionar la siguiente información:

o Dashboards, reportes, graficas, tablas y estadísticas interactivas que muestren los principales parámetros de la red, tales como: estado de los elementos de red, alarmas, eventos, desplegado de puertos, uso de CPU, SSIDs, así como de los usuarios conectados a la red, identificación de dispositivos de acuerdo al sistema operativo, tipo de autenticación y perfil.
o Búsqueda de dispositivos por dirección IP, dirección MAC o nombre de usuario.
o Diagramas de conexión lógica de los dispositivos y elementos de red.
o Datos provenientes de la solución de Control de Acceso a la Red y gestión de funciones de dicha solución, tales como dar de baja usuarios y/o dispositivos, re autenticación de los mismos, movimiento de usuarios y/o dispositivos a diferentes grupos de trabajo que proporcione la solución de Control de Acceso a la Red.
o Generación de reportes.
o Guardar un histórico de la información hasta por 6 meses.

- Deberá contar con un visor de flujos basado en NetFlow para efectos de diagnóstico y soporte.
- Deberá identificar diferentes tipos de equipos como PC's, Servidores, Impresoras, Cámaras IP, Teléfonos IP conectados a la red e identificar las vulnerabilidades asociadas a ellos.
- Deberá interactuar con los equipos propuestos para localizar ubicación exacta de los eventos de seguridad que sean notificados vía SNMP v3 por el dispositivo de análisis de comportamiento de la red y detener el ataque en forma automática desde el puerto donde se genere la anomalía o en el punto de ingreso a la red, a través de implementación dinámica de políticas de control de tráfico, que deshabiliten el puerto y/o bloqueen el flujo origen de la anomalía de seguridad sin intervención manual.
- Capacidad de administrar controladoras y Access Points del mismo fabricante.
- Capacidad de detectar alguna las siguientes amenazas:

o AP intrusos (rogue)
o Dispositivos en modo Ad-Hoc.
o Ataques de Denial of Service (DoS)
o Fuentes de interferencia
o Intentos de password Cracking

- Capacidad de habilitar la captura de información en tiempo real en un Access Point de la red.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 05 74 00 www.fonacot.gob.mx

- Capacidad de reportar fuentes de interferencia
- Capacidad de desplegar información sobre cada controlador inalámbrico

o Listado de Access Point conectados por canal
o Clientes
o Uso de ancho de banda

- Capacidad de listar los Access Point del sistema y desplegar información individual sobre:

o Controlador al que está conectado
o Ancho de banda
o Clientes conectados
o Alarmas

- Capacidad de listar los clientes del sistema y desplegar información individual sobre:

o Horarios de inicio y fin de sesión
o Historial de roaming entre Access Point
o Cambios de dirección IP
o Cambios de estado de autenticación

- Clientes conectados
- Capacidad de listar las amenazas detectadas mediante WiDS/Wips

El licitante se obliga a mantener la continuidad de los servicios que se encuentran implementados actualmente en la red del Instituto FONACOT, por lo que las configuraciones, reglas y políticas de acceso a usuarios, deberán ser migradas de manera transparente a los equipos propuestos con el LICITANTE.

Durante toda la vigencia del contrato, la herramienta de administración deberá mantenerse a la última versión de software estable liberada por el fabricante.

Se deberán considerar al menos 3 accesos concurrentes a la herramienta de administración para personal del area técnica del Instituto FONACOT independientes a los que el LICITANTE requiera para la operación del servicio.

Este servicio deberá operar en la infraestructura del LICITANTE.

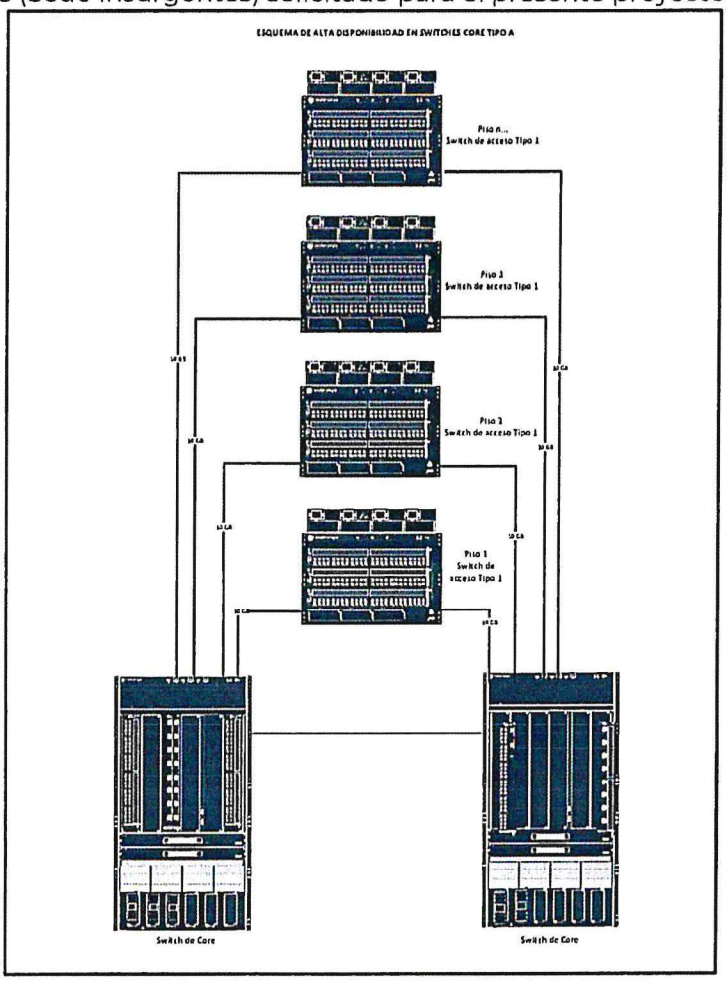
2.3.2.2. Esquema de Alta Disponibilidad en Switches CORE Tipo A.

El LICITANTE deberá implementar un esquema de alta disponibilidad en las Oficinas Centrales del Instituto FONACOT (Sede Insurgentes), basado en dos Switches CORE de última generación con la finalidad de contar con redundancia a nivel backbone de fibra óptica. Es responsabilidad del LICITANTE considerar el dimensionamiento adecuado en cuanto a hardware, licenciamiento, actualizaciones, componentes y cualquier otro elemento que se requiera para la adecuada operación de los equipos que conformen este esquema.

Es responsabilidad del LICITANTE, garantizar que el esquema de alta disponibilidad implementado mantenga la configuracion, niveles de seguridad y control de tráfico por servicio y por usuario que actualmente tiene definidas el área técnica Instituto

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

FONACOT. La implementación de los equipos CORE deberá integrarse nativamente con la herramienta de administración de la Red, propiedad del Instituto FONACOT.
A continuación, se muestra el esquema de alta disponibilidad de switches core en oficinas centrales (Sede Insurgentes) solicitado para el presente proyecto.



Los Switches CORE que conformen el esquema de alta disponibilidad en las Oficinas Centrales del Instituto FONACOT (Sede Insurgentes), deberán cumplir con al menos las siguientes características tecnicas:

- El equipo deberá proveer al menos 06 ranuras para la inserción de tarjetas y crecimientos en un futuro.
- El equipo debe ser capaz de soportar las siguientes densidades de puertos:
  - 432 puertos 10/100/1000 Base-TX o 1000Base-X SFP
  - 168 puertos 10GBase-X SFP+
  - 36 puertos 40GBase-X QSFP+
- Soportar voltaje de Alimentación 100-240 VCA, a una frecuencia de 50-60 Hz
- Incluirá Ventiladores y Fuentes de alimentación de tipo Hot-swappable
- Proveer la facilidad de insertar, remover o reemplazar módulos, sin interrumpir la operación del sistema.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- El equipo deberá incluir al menos 2 fuentes de poder internas en modo redundante, para garantizar la total operación de la unidad, aun cuando una fuente de poder haya fallado. Las fuentes de poder redundantes deberán de realizar balanceo de carga.
- Debe soportar la funcionalidad de "Virtual Chassis", "Chassis Bonding", "Virtual Switching System" o similar. Con la finalidad de poder realizar configuraciones de alta disponibilidad a nivel de L2, sin que existan los problemas y tiempo de re-convergencia por los protocolos de Spanning Tree, permitiendo la Administración de dos switches como uno sólo.
- Acorde a la arquitectura del equipo, deberá incluir redundancia en tarjetas supervisoras (controladoras) o en su defecto un esquema de procesamiento distribuido
- Debe incluir al menos para los 2 equipos de Oficinas Centrales:

o 96 Puertos 10/100/1000Base-TX RJ45 PoE+
o 10 puertos Ethernet 10GBase-X

- Soportar auto-mdi/mdix, auto-sensing y auto-negotiation en todos los puertos 10/100/1000 Base-TX
- Contar con puerto serial USB y RJ45 para configuración del equipo y carga de firmware, así como de carga y descarga de archivos.
- Soportar Power over Ethernet con estándares 802.3af/802.3at
- La capacidad de conmutación o switching capacity del chasis deberá ser de al menos 96 Gbps
- Un Throughput IPv4 por chasis de al menos 720 Mpps
- Soportar un desempeño mínimo por cada tarjeta de servicio (tarjeta I/O) de 160 Gbps
- Contar con al menos 10 colas de prioridad (Queues) por puerto
- Soportar al menos 65000 MAC Address
- Soportar al menos 4000 VLANs
- Deberá soportar e incluir Netflow v9.
- Contar con el soporte de Jumbo frames de 9,216 bytes
- Soportar SNMP v1/v2c/v3
- Soportar al menos 15 mirrors por chasis, los cuales pueden ser de:

o Uno a uno
o Uno a muchos
o Muchos a uno
o Mirror de Vlans

- Soportar Remote Port Mirror
- Soportar CDP v1/2
- Incluirá la funcionalidad Proxy ARP
- Incluir la funcionalidad Bi-directional Forwarding Detection (BFD)
- Contar con la funcionalidad Q-in-Q
- Ser capaz de implementar NTP (Network Time Protocol) ó SNTP (Simple Network Time Protocol).
- Incluirá la funcionalidad de NAT

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Con el sistema operativo base, deberá proveer la función de balanceo de servicios, de tal forma que se puedan generar gateways virtuales de servicios como WEB, SMTP o algún otro aplicativo, sin la necesidad de agregar módulos especiales y licenciamiento para este propósito.
- Soportar la funcionalidad DHCP Server / Relay
- Soportar la funcionalidad Unidirectional Link Detection
- Incluirá la funcionalidad de Supresión de Broadcast
- Soportar el estándar 802.1ak MVRP
- Incluir la funcionalidad Generic VLAN Registration Protocol (GVRP)
- Soportar IGMP v1/v2/v3
- Soportar los siguientes Estándares:

o 802.3u Fast Ethernet
o 802.3ab Gigabit Ethernet
o 802.3z Gigabit Ethernet
o 802.3ae 10 Gigabit Ethernet
o 802.3an 10Gase-T

- Soportar los siguientes Estándares:

o 802.1Q VLANs
o 802.1D MAC Bridges
o 802.1w RSTP
o 802.1s MST
o 802.1t Path Cost
o 802.3ad Link Aggregation
o 802.3ae Gigabit Ethernet
o 802.3x Flow Control
o 802 1ab LLDP-MED

- Soportar el protocolo 802.3ad permitiendo la agrupación de hasta 190 LAG por chasis, y hasta 64 puertos por cada LAG.
- Soportar los siguientes Estándares:

o 802.1Qaz ETS y DCBx
o 802.1Qbb PFC
o 802.1Qau Congestion Notification
o Soportar Ruteo Estático
o Soportar ACLs Estándar y Extendidas
o Incluir Policy-Based Routing (PBR)
o Soportar VRF en IPv4/IPv6
o Soportar OSPF
o Soportar OSPF ECMP

- Soportar RIP v2
- Soportar BGPv4
- Soportar L2VPN
- Soportar L3VPN over native MPLS
- Soportar PIM-DM
- Soportar al menos 1,000,000 de entradas en la tabla de ruteo IPv4
- Soportar al menos 50,000 de entradas en la tabla de ruteo IPv6

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 5553 52 65 74 00 www.fonacot.gob.mx

- Soportar al menos 100 interfaces IPv6
- Soportar al menos 10 IP helper address por interface
- Incluir las siguientes funcionalidades para IPv6:

o Ruteo estático
o DVMRPv3
o OSPFv3
o Ruteo basado en políticas IPv6 (PBR)
o PIM-SM v6
o PIM-SSM v6
o MLD v1/v2
o RIPng
o IPv6 ACLs
o DHCP relay
o Neighbor Discovery
o IPSec para OSPFv3

- Soportar los siguientes estandares:

o RFC 1195 Use of OSI IS-IS for Routing in TCP/IP
o RFC 1265 BGP Protocol Analysis
o RFC 1266 Experience with the BGP Protocol
o RFC 1519 CIDR
o RFC 3101 OSPFv2 NSSA
o RFC 1657 Managed Objects for BGP-4 using SMIv2
o RFC 1771 A Border Gateway Protocol 4 (BGP-4)
o RFC 1772 Application of BGP in the Internet
o RFC 1773 Experience with the BGP-4 protocol
o RFC 1774 BGP-4 Protocol Analysis
o RFC 1812 General Routing/RIP Requirements
o RFC 1853 IP in IP Tunneling
o RFC 1886 DNS Extensions to support IP version 6
o RFC 1930 Guidelines for creation, selection, and registration of an Autonomous System (AS)
o RFC 1966 BGP Route Reflection
o RFC 1981 Path MTU Discovery for IPv6
o RFC 1998 BGP Community Attribute in Multi-home Routing
o RFC 2003 IP Encapsulation within IP
o RFC 2082 RIP-II MD5 Authentication
o RFC 2260 Support for Multi-homed Multi-prov
o RFC 2270 Dedicated AS for Sites Homed to one Provider
o RFC 2373 Address notation compression
o RFC2374 IPv6 Aggregatable Global Unicast Address Format
o RFC2375 IPv6 Multicast Address Assignments
o RFC 2391 Load Sharing Using Network Address Translation(LSNAT)
o RFC2401 Security Architecture for the Internet Protocol
o RFC2404 The Use of HMAC-SHA-1-96 within ESP and AH
o RFC2406 IP Encapsulating Security Payload (ESP)

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- RFC2407 Internet IP Security Domain of Interpretation for ISAKMP
- RFC2408 Internet Security Association and Key Management Proto-col (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2450 Proposed TLA and NLA Assignment Rule
- RFC 2460 IPv6 Specification
- RFC 2462 IPv6 Stateless Address Auto-configuration
- RFC 2464 Transmission of IPv6 over Ethernet
- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2474 Definition of DS Field in the IPv4/v6 Headers
- RFC 2519 A Framework for Inter-Domain Route Aggregation
- RFC 2547 BGP/MPLS VPNs
- RFC 2553 BasiCSocket Interface Extensions for IPv6
- RFC 2577 FTP Security Considerations
- RFC 2597 Assured Forwarding PHB Group
- RFC 2685 Virtual Private Networks Identifier
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2715 Interoperability Rules for Multicast Routing Protocols
- RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2784 Generic Routing Encapsulation
- RFC 2890 Key and Sequence Number Extensions to GRE
- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
- RFC 2894 Router Renumbering
- RFC 2918 Route Refresh Capability for BGP
- RFC 2966 Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3065 Autonomous System Confederations for BGP
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3162 RADIUS and IPv6
- RFC 3345 BGP Persistent Route Oscillation
- RFC 3359 TLV Codepoints in IS-IS
- RFC 3373 Three-Way Handshake for IS-IS
- RFC 3567 IS-IS Cryptographic Authentication
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC3596 DNS Extensions to Support IP Version 6
- RFC 3768 VRRP
- RFC 3769 Requirements for IPv6 Prefix Delegation
- RFC 3810 MLDv2 for IPv6
- RFC 3879 Deprecating Site Local Addresses
- RFC 3956 Embedding the RP Address in IPv6 MCAST Address
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4023 Encapsulating MPLS in IP
- RFC 4109 Algorithms for IKEv1
- RFC 4191 Default Router Preferences and More-Specific Routes

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 05 74 00 www.fonacot.gob.mx

- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4213 Basic Transition Mechanisms for IPv6
- RFC 4222 Prioritized Treatment of OSPFv2 Packets
- RFC 4264 BGP Wedgies
- RFC 4265 Definition of Textual Conventions for (VPN) Management
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4272 BGP Security Vulnerabilities Analysis
- RFC 4273 Managed Objects for BGP-4 using SMIv2
- RFC 4274 BGP-4 Protocol Analysis
- RFC 4276 BGP-4 Implementation Report
- RFC 4277 Experience with the BGP-4 protocol
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4301 Security Architecture for IP
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4305 Crypto Algorithm Requirements for ESP and AH
- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in IKEv2
- RFC 4308 Cryptographic Suites for IPSec
- RFC 4360 BGP Extended Communities Attribute
- RFC 4364 BGP/MPLS IP VPNs
- RFC 4365 Applicability Statement for BGP/MPLS IP VPNs
- RFC 4384 BGP Communities for Data Collection
- RFC 4443 ICMPv6 for IPv6
- RFC 4456 BGP Route Reflection
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4451 BGP MULTI_EXIT_DISC (MED) Considerations
- RFC 4541 MLD Snooping
- RFC 4552 Authentication/Confidentiality for OSPFv3
- RFC 4601 PIM-SM
- RFC 4604 IGMPv3 & MLDv2 & Source-Specific Multicast
- RFC 4607 Source-Specific Multicast for IP
- RFC 4608 PIM--SSM in 232/8
- RFC 4610 Anycast-RP Using PIM
- RFC 4611 MSDP Deployment Scenarios
- RFC 4632 Classless Inter-Domain Routing (CIDR)
- RFC 4659 BGP-MPLS (VPN) Extension for IPv6 VPN
- RFC 4724 Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4835 CryptoAlgorithm Requirements for ESP and AH
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 4884 Extended ICMP Multi-Part Messages
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 5059 Bootstrap Router (BSR) Mechanism for (PIM)
- RFC 5065 Autonomous System Confederations for BGP

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 5186 IGMPv3/MLDv2/MCAST Routing Protocol Interaction
- RFC 5187 OSPFv3 Graceful Restart
- RFC 5240 PIM Bootstrap Router MIB
- RFC 5250 The OSPF Opaque LSA Option
- RFC 5291 Outbound Route Filtering Capability for BGP-4
- RFC 5292 Address-Prefix-Outbound Route Filter for BGP-4
- RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 5302 Domain-wide Prefix Distribution with IS-IS
- RFC 5303 3Way Handshake for IS-IS P2P Adjacencies
- RFC 5304 IS-IS Cryptographic Authentication
- RFC 5306 Restart Signaling for IS-IScol for BGP L3 VPNs
- Soportar las siguientes MIB:
- RFC 2578 SNMPv2 SMI
- RFC 3418 SNMPv2 MIB
- RFC 2576 SNMP-Community MIB
- RFC 2863 IF MIB
- RFC 3621 Power Ethernet MIB
- RFC 4750 OSPFv2 MIB
  - CISCO CDP MIB
  - CISCO NETFLOW MIB
  - Incluir la funcionalidad de Redirección de peticiones Web

Funcionalidades de Administración y Monitoreo

- El equipo podrá ser Administrado por:
- Puerto de Consola
- SNMP
- Remotamente por Sesión VTY
  - Soportar SSHv2
  - Soportar Telnet como Servidor y Cliente
  - Soportar SNTP o NTP
  - Soportar Interface Web de Gestión
  - Poseer una función de actualización de firmware y almacenamiento de imágenes de respaldo en caso de que el proceso falle o bien la imagen se encuentre dañada o corrupta.
  - Soportar Múltiples archivos de configuración
  - Soportar download de imágenes de Sistema Operativo o Firmware y archivos de configuración desde servidores:
- FTP
- TFTP
- SCP
  - Incluir una funcionalidad para realizar upgrades de Sistema Operativo o Firmware de forma gradual por tarjeta y por Grupo de Tarjetas, de forma que no se reinicie el equipo completo para aplicar actualizaciones de Sistema Operativo.
  - Incluir funcionalidad de IP SLA para la medición de jitter y delay
  - Soportar VLAN de Administración

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 55 52 65 74 00 www.fonacot.gob.mx

- Capacidad de envío de logs de acuerdo a su grado de severidad al menos hacia 8 servidores Syslog, de ser requerido.
- Soportar la Autenticación y Encripción por algoritmos aprobados FIPS
- Soportar la funcionalidad de especificar por usuario administrador la hora de inicio y termino de acceso al equipo.
- Soportar la funcionalidad de especificar la cantidad máxima de sesiones simultáneas por usuario administrador en el switch.
- Soportar la funcionalidad de especificar la cantidad máxima de días de inactividad por usuario administrador, antes de que la cuenta sea deshabilitada en el switch
- Soportar la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:

o Letra mayúscula
o Letra minúscula
o Numero
o Caracteres especiales

- Soportar 802.3 2008 Clause 57 Ethernet OAM – Link Layer OAM

Funciones de Control y Seguridad

- Soportar rate-limiting desde 8 Kbps
- Soportar rate-limiting de entrada y salida
- Soportar IP ToS/DSCP Marking/Remarking
- Soportar los siguientes Controles de Flood-Limiting por Puerto:

o Broadcast
o Multicast
o Unknown Unicast

- Debe detectar dispositivos de telefonía IP o video de al menos 2 distintos fabricantes, una vez detectados aplicara configuración de forma dinámica en el puerto.
- Debe detectar dispositivos de telefonía IP de terceros para aplicar configuración de forma dinámica en el puerto, los dispositivos de teléfonia podrán emplear los protocolos:

o H.323
o SIP

- Debe realizar Clasificacion y QoS de paquetes multicapa basado en usuario y así dar un tratamiento específico por Grupos de Usuario y Usuario
- Soportar al menos tres distintos mecanismos de gestión de colas (queuing)
- Soporte de múltiples usuarios/dispositivos (como teléfonos IP, computadoras, impresoras, fotocopiadoras, cámaras de seguridad, lectores de tarjeta, servidores virtuales, etc.) y múltiples métodos de autenticación (por 802.1x, WEP y MAC o la combinación de estos) en un puerto o en todos los puertos, soportando por lo menos 1000 usuarios/dispositivos autenticados por módulo.
- Soportar 802.1D
- Soportar 802.1p

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Poseer la funcionalidad de poder detectar eventos de intermitencias o flaps en los puertos y llevar a cabo acciones como inhabilitar el(los) puerto(s) involucrados y generar una entrada de log y/o envío de traps.
- Protección automática para conexión de dispositivos de comunicación no permitidos, los cuales activen el protocolo de STP y generen alguna reconvergencia en la red.
- Soportar autentificación de usuarios administradores de equipos mediante TACACS+.
- Soportar al menos 9 grupos de RMON
- Debe ser capaz de clasificar tráfico en base a los siguientes criterios:

o MAC source address
o MAC destination addres
o Source IPX address
o Destination IPX address
o Source IPX socket
o Destination IPX socket
o Transmission control IPX
o IPX packet type
o IPv6 source address
o IPv6 destination address
o IPv6 flow label
o Source IP address.
o Destination IP address.
o IP fragmentation value.
o UDP source port
o UDP destination port
o TCP source port
o TCP destination port
o ICMP packet type
o Time-To-Live (TTL)
o Type of Service
o ICMPv6 packet type
o VLAN tag
o Port-string
o Incluir la funcionalidad de limitar el acceso de una MAC Address dada a un puerto especifico, la cual puede aprender el equipo de forma estática o dinámica

- Incluir mecanismos de mitigación ante los siguientes ataques DoS:

o Bad SIP
o Christmas Tree
o Fragmented ICMP
o ICMP Flood
o Large ICMP
o LANd
o Smurf
o Fraggle Attack

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- SYN Flood
  - Contar con al menos 3 distintos mecanismos anti-spoofing
  - Soportar RADIUS accounting / snooping
  - Soportar RFC 3580
  - Soportar prevención de ARP storm
  - El equipo debe soportar e incluir una funcionalidad capaz de distinguir la identidad de un usuario/dispositivo que es autenticado en otro switch conectado a este mismo, pudiendo asignar alguna política de L2, L3 y L4, permitiendo, negando, etiquetando, redireccionando, asignando una prioridad y un rate limiting.
  - Soportar funciones de mitigación de ataques de tipo DoS de tal forma que se pueden configurar umbrales permitidos de cantidad de tráfico, los cuales puedan desencadenar acciones como descartar tráfico excedente, envío de SNMP o logs e inclusive hasta desactivar una o más interfaces.

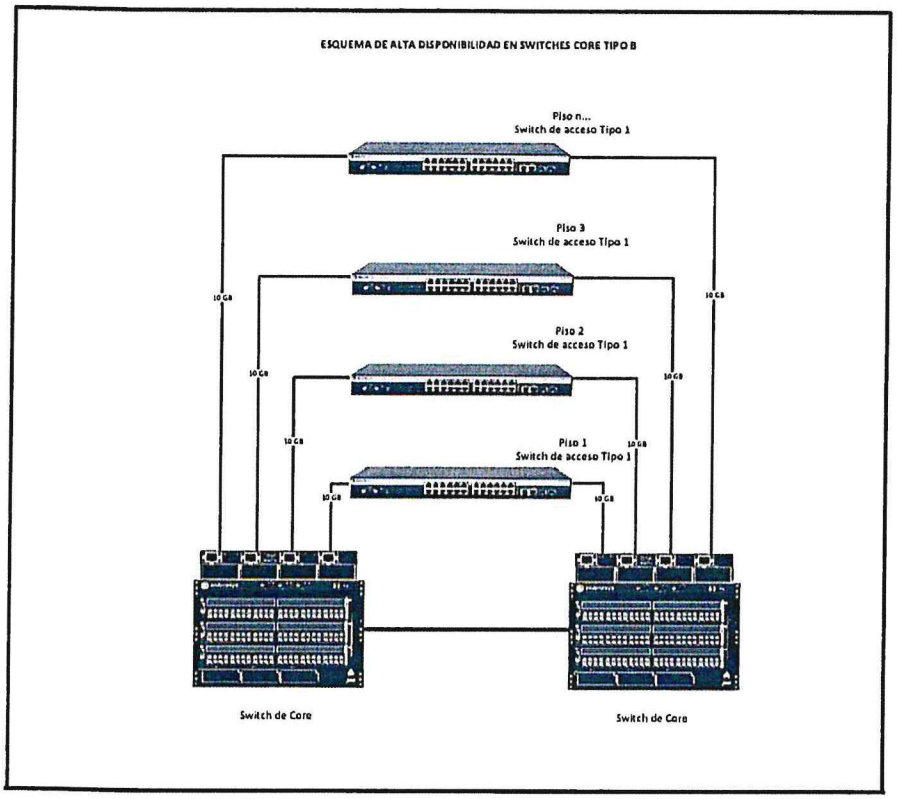
2.3.2.3.Esquema de Alta Disponibilidad en Switches CORE Tipo B

El LICITANTE deberá implementar un esquema de alta disponibilidad en la sede de Plaza de la Republica del Instituto FONACOT, basado en dos Switches CORE de última generación con la finalidad de contar con redundancia a nivel backbone de fibra óptica. Es responsabilidad del LICITANTE considerar el dimensionamiento adecuado en cuanto a hardware, licenciamiento, actualizaciones, componentes y cualquier otro elemento que se requiera para la adecuada operación de los equipos que conformen este esquema.

Es responsabilidad del LICITANTE, garantizar que el esquema de alta disponibilidad implementado mantenga las configuraciones, niveles de seguridad y control de tráfico por servicio y por usuario que actualmente tiene definidas el área técnica Instituto FONACOT. Los equipos CORE propuestos para este esquema, deberán integrarse nativamente con la herramienta de administración de la Red, propiedad del Instituto FONACOT.

A continuación, se muestra el esquema de alta disponibilidad de switches core tipo 2 solicitado en **Plaza de la Republica** para el presente proyecto.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx



Los Switches CORE que conformen el esquema de alta disponibilidad en Plaza de la Republica del Instituto FONACOT, deberán cumplir con al menos las siguientes características tecnicas:

- El equipo deberá proveer al menos 03 ranuras para la inserción de tarjetas y crecimientos en un futuro.
- El equipo debe ser capaz de soportar las siguientes densidades de puertos:
  - 216 puertos 10/100/1000 Base-TX o 1000Base-X SFP
  - 96 puertos 10GBase-X SFP+
- Soportar voltaje de Alimentación 100-240 VCA, a una frecuencia de 50-60 Hz
- Incluirá Ventiladores y Fuentes de alimentación de tipo Hot-swappable
- Proveer la facilidad de insertar, remover o reemplazar módulos, sin interrumpir la operación del sistema.
- El equipo deberá incluir al menos 2 fuentes de poder internas en modo redundante, para garantizar la total operación de la unidad, aun cuando una fuente de poder haya fallado. Las fuentes de poder redundantes deberán de realizar balanceo de carga.
- Debe soportar la funcionalidad de "Virtual Chassis", "Chassis Bonding", "Virtual Switching System" o similar. Con la finalidad de poder realizar configuraciones de alta disponibilidad a nivel de L2, sin que existan los problemas y tiempo de re-convergencia por los protocolos de Spanning Tree, permitiendo la Administración de dos switches como uno sólo.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 55 1552 05 78 00 www.fonacot.gob.mx

- Acorde a la arquitectura del equipo, deberá incluir redundancia en tarjetas supervisoras (controladoras) o en su defecto un esquema de procesamiento distribuido
- Debe incluir al menos para los 2 equipos de Plaza de la Republica:
  - 48 Puertos 10/100/1000Base-TX RJ45 PoE+
  - 12puertos Ethernet 10GBase X
- Soportar auto-mdi/mdix, auto-sensing y auto-negotiation en todos los puertos 10/100/1000 Base-TX
- Contar con puerto serial USB y RJ45 para configuración del equipo y carga de firmware, así como de carga y descarga de archivos.
- Soportar Power over Ethernet con estándares 802.3af/802.3at
- La capacidad de conmutación o switching capacity del chasis deberá ser de al menos 360 Gbps
- Un Throughput IPv4 por chasis de al menos 90 Mpps
- Soportar un desempeño mínimo por cada tarjeta de servicio (tarjeta I/O) de 160 Gbps
- Contar con al menos 10 colas de prioridad (Queues) por puerto
- Soportar al menos 128000 MAC Address
- Soportar al menos 4000 VLANs
- Deberá soportar e incluir Netflow v9, v9 para el monitoreo de al menos 20 interfases del equipo, y soportar al menos configuración de 4 colectores posibles, sin la necesidad de un licenciamiento adicional, cambio o modificación del hardware para el empleo de dicho protocolo, y cuyo empleo no impacte en el desempeño del equipo tanto en funcionalidades de switching como de routing
- Contar con el soporte de Jumbo frames de 9216bytes
- Soportar SNMP v1/v2c/v3
- Soportar al menos 15 mirrors por chasis, los cuales pueden ser de:
  - Uno a uno
  - Uno a muchos
  - Muchos a uno
  - Mirror de Vlans
- Soportar Remote Port Mirror
- Soportar CDP v1/2
- Incluirá la funcionalidad Proxy ARP
- Incluir la funcionalidad Bi-directional Forwarding Detection (BFD)
- Contar con la funcionalidad Q-in-Q
- Ser capaz de implementar NTP (Network Time Protocol) ó SNTP (Simple Network Time Protocol).
- Incluirá la funcionalidad de NAT
- Con el sistema operativo base, deberá proveer la función de balanceo de servicios, de tal forma que se puedan generar gateways virtuales de servicios como WEB, SMTP o algún otro aplicativo, sin la necesidad de agregar módulos especiales y licenciamiento para este propósito.
- Soportar la funcionalidad DHCP Server / Relay
- Soportar la funcionalidad Unidirectional Link Detection

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Incluirá la funcionalidad de Supresión de Broadcast
- Soportar el estándar 802.1ak MVRP
- Incluir la funcionalidad Generic VLAN Registration Protocol (GVRP)
- Soportar IGMP v1/v2/v3
- Soportar los siguientes Estándares:
  - 802.3u Fast Ethernet
  - 802.3ab Gigabit Ethernet
  - 802.3z Gigabit Ethernet
  - 802.3ae 10 Gigabit Ethernet
  - 802.3an 10Gase-T
- Soportar los siguientes Estándares:
  - 802.1Q VLANs
  - 802.1D MAC Bridges
  - 802.1w RSTP
  - 802.1s MST
  - 802.1t Path Cost
  - 802.3ad Link Aggregation
  - 802.3ae Gigabit Ethernet
  - 802.3x Flow Control
  - 802 1ab LLDP-MED
- Soportar el protocolo 802.3ad permitiendo la agrupación de hasta 190 LAG por chasis, y hasta 64 puertos por cada LAG.
- Soportar los siguientes Estándares:
  - 802.1Qaz ETS y DCBx
  - 802.1Qbb PFC
  - 802.1Qau Congestion Notification
  - Soportar Ruteo Estático
  - Soportar ACLs Estándar y Extendidas
  - Incluir Policy-Based Routing (PBR)
  - Soportar VRF en IPv4/IPv6
  - Soportar OSPF
  - Soportar OSPF ECMP
- Soportar RIP v2
- Soportar BGPv4
- Soportar L2VPN
- Soportar L3VPN over native MPLS
- Soportar PIM-DM
- Soportar al menos 1,000,000 de entradas en la tabla de ruteo IPv4
- Soportar al menos 50,000 de entradas en la tabla de ruteo IPv6
- Soportar al menos 100 interfaces IPv6
- Soportar al menos 10 IP helper address por interface
- Incluir las siguientes funcionalidades para IPv6:
  - Ruteo estático
  - DVMRPv3
  - OSPFv3

Av. Insurgentes Sur 452 Col. Roma Sur, D.F. Cuauhtémoc, C.P. 06760, México D.F.
Tel. +55 1520 65 7500 www.fonacot.gob.mx

- Ruteo basado en políticas IPv6 (PBR)
- PIM-SM v6
- PIM-SSM v6
- MLD v1/v2
- RIPng
- IPv6 ACLs
- DHCP relay
- Neighbor Discovery
- IPSec para OSPFv3

- Soportar los siguientes estandares:
  - RFC 1195 Use of OSI IS-IS for Routing in TCP/IP
  - RFC 1265 BGP Protocol Analysis
  - RFC 1266 Experience with the BGP Protocol
  - RFC 1519 CIDR
  - RFC 3101 OSPFv2 NSSA
  - RFC 1657 Managed Objects for BGP-4 using SMIv2
  - RFC 1771 A Border Gateway Protocol 4 (BGP-4)
  - RFC 1772 Application of BGP in the Internet
  - RFC 1773 Experience with the BGP-4 protocol
  - RFC 1774 BGP-4 Protocol Analysis
  - RFC 1812 General Routing/RIP Requirements
  - RFC 1853 IP in IP Tunneling
  - RFC 1886 DNS Extensions to support IP version 6
  - RFC 1930 Guidelines for creation, selection, and registration of an Autonomous System (AS)
  - RFC 1966 BGP Route Reflection
  - RFC 1981 Path MTU Discovery for IPv6
  - RFC 1998 BGP Community Attribute in Multi-home Routing
  - RFC 2003 IP Encapsulation within IP
  - RFC 2082 RIP-II MD5 Authentication
  - RFC 2260 Support for Multi-homed Multi-prov
  - RFC 2270 Dedicated AS for Sites Homed to one Provider
  - RFC 2373 Address notation compression
  - RFC2374 IPv6 Aggregatable Global Unicast Address Format
  - RFC2375 IPv6 Multicast Address Assignments
  - RFC 2391 Load Sharing Using Network Address Translation(LSNAT)
  - RFC2401 Security Architecture for the Internet Protocol
  - RFC2404 The Use of HMAC-SHA-1-96 within ESP and AH
  - RFC2406 IP Encapsulating Security Payload (ESP)
  - RFC2407 Internet IP Security Domain of Interpretation for ISAKMP
  - RFC2408 Internet Security Association and Key Management Proto-col (ISAKMP)
  - RFC 2409 The Internet Key Exchange (IKE)
  - RFC 2450 Proposed TLA and NLA Assignment Rule
  - RFC 2460 IPv6 Specification

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- RFC 2462 IPv6 Stateless Address Auto-configuration
- RFC 2464 Transmission of IPv6 over Ethernet
- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2474 Definition of DS Field in the IPv4/v6 Headers
- RFC 2519 A Framework for Inter-Domain Route Aggregation
- RFC 2547 BGP/MPLS VPNs
- RFC 2553 BasiCSocket Interface Extensions for IPv6
- RFC 2577 FTP Security Considerations
- RFC 2597 Assured Forwarding PHB Group
- RFC 2685 Virtual Private Networks Identifier
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2715 Interoperability Rules for Multicast Routing Protocols
- RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2784 Generic Routing Encapsulation
- RFC 2890 Key and Sequence Number Extensions to GRE
- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
- RFC 2894 Router Renumbering
- RFC 2918 Route Refresh Capability for BGP
- RFC 2966 Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3065 Autonomous System Confederations for BGP
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3162 RADIUS and IPv6
- RFC 3345 BGP Persistent Route Oscillation
- RFC 3359 TLV Codepoints in IS-IS
- RFC 3373 Three-Way Handshake for IS-IS
- RFC 3567 IS-IS Cryptographic Authentication
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC3596 DNS Extensions to Support IP Version 6
- RFC 3768 VRRP
- RFC 3769 Requirements for IPv6 Prefix Delegation
- RFC 3810 MLDv2 for IPv6
- RFC 3879 Deprecating Site Local Addresses
- RFC 3956 Embedding the RP Address in IPv6 MCAST Address
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4023 Encapsulating MPLS in IP
- RFC 4109 Algorithms for IKEv1
- RFC 4191 Default Router Preferences and More-Specific Routes
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4213 Basic Transition Mechanisms for IPv6
- RFC 4222 Prioritized Treatment of OSPFv2 Packets
- RFC 4264 BGP Wedgies
- RFC 4265 Definition of Textual Conventions for (VPN) Management

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4272 BGP Security Vulnerabilities Analysis
- RFC 4273 Managed Objects for BGP-4 using SMIv2
- RFC 4274 BGP-4 Protocol Analysis
- RFC 4276 BGP-4 Implementation Report
- RFC 4277 Experience with the BGP-4 protocol
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4301 Security Architecture for IP
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4305 Crypto Algorithm Requirements for ESP and AH
- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in IKEv2
- RFC 4308 Cryptographic Suites for IPSec
- RFC 4360 BGP Extended Communities Attribute
- RFC 4364 BGP/MPLS IP VPNs
- RFC 4365 Applicability Statement for BGP/MPLS IP VPNs
- RFC 4384 BGP Communities for Data Collection
- RFC 4443 ICMPv6 for IPv6
- RFC 4456 BGP Route Reflection
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4451 BGP MULTI_EXIT_DISC (MED) Considerations
- RFC 4541 MLD Snooping
- RFC 4552 Authentication/Confidentiality for OSPFv3
- RFC 4601 PIM-SM
- RFC 4604 IGMPv3 & MLDv2 & Source-Specific Multicast
- RFC 4607 Source-Specific Multicast for IP
- RFC 4608 PIM--SSM in 232/8
- RFC 4610 Anycast-RP Using PIM
- RFC 4611 MSDP Deployment Scenarios
- RFC 4632 Classless Inter-Domain Routing (CIDR)
- RFC 4659 BGP-MPLS (VPN) Extension for IPv6 VPN
- RFC 4724 Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4835 CryptoAlgorithm Requirements for ESP and AH
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 4884 Extended ICMP Multi-Part Messages
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 5059 Bootstrap Router (BSR) Mechanism for (PIM)
- RFC 5065 Autonomous System Confederations for BGP
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 5186 IGMPv3/MLDv2/MCAST Routing Protocol Interaction
- RFC 5187 OSPFv3 Graceful Restart
- RFC 5240 PIM Bootstrap Router MIB
- RFC 5250 The OSPF Opaque LSA Option

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

  - RFC 5291 Outbound Route Filtering Capability for BGP-4
  - RFC 5292 Address-Prefix-Outbound Route Filter for BGP-4
  - RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
  - RFC 5302 Domain-wide Prefix Distribution with IS-IS
  - RFC 5303 3Way Handshake for IS-IS P2P Adjacencies
  - RFC 5304 IS-IS Cryptographic Authentication
  - RFC 5306 Restart Signaling for IS-IScol for BGP L3 VPNs
- Soportar las siguientes MIB:
  - RFC 2578 SNMPv2 SMI
  - RFC 3418 SNMPv2 MIB
  - RFC 2576 SNMP-Community MIB
  - RFC 2863 IF MIB
  - RFC 3621 Power Ethernet MIB
  - RFC 4750 OSPFv2 MIB
- CISCO CDP MIB
- CISCO NETFLOW MIB
- Incluir la funcionalidad de Redirección de peticiones Web

Funcionalidades de Administración y Monitoreo

- El equipo podrá ser Administrado por:
  - Puerto de Consola
  - SNMP
  - Remotamente por Sesión VTY
- Soportar SSHv2
- Soportar Telnet como Servidor y Cliente
- Soportar SNTP o NTP
- Soportar Interface Web de Gestión
- Poseer una función de actualización de firmware y almacenamiento de imágenes de respaldo en caso de que el proceso falle o bien la imagen se encuentre dañada o corrupta.
- Soportar Múltiples archivos de configuración
- Soportar download de imágenes de Sistema Operativo o Firmware y archivos de configuración desde servidores:
  - FTP
  - TFTP
  - SCP
- Incluir una funcionalidad para realizar upgrades de Sistema Operativo o Firmware de forma gradual por tarjeta y por Grupo de Tarjetas, de forma que no se reinicie el equipo completo para aplicar actualizaciones de Sistema Operativo.
- Incluir funcionalidad de IP SLA para la medición de jitter y delay
- Soportar VLAN de Administración
- Capacidad de envío de logs de acuerdo a su grado de severidad al menos hacia 8 servidores Syslog, de ser requerido.
- Soportar la Autenticación y Encripción por algoritmos aprobados FIPS
- Soportar la funcionalidad de especificar por usuario administrador la hora de inicio y termino de acceso al equipo.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 5551 52 05 74 00 www.fonacot.gob.mx

- Soportar la funcionalidad de especificar la cantidad máxima de sesiones simultáneas por usuario administrador en el switch.
- Soportar la funcionalidad de especificar la cantidad máxima de días de inactividad por usuario administrador, antes de que la cuenta sea deshabilitada en el switch
- Soportar la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula
  - Letra minúscula
  - Numero
  - Caracteres especiales
- Contar con un packet buffering de 6 GB
- Soportar 802.3 2008 Clause 57 Ethernet OAM – Link Layer OAM

Funciones de Control y Seguridad

- Soportar rate-limiting desde 8 Kbps
- Soportar rate-limiting de entrada y salida
- Soportar IP ToS/DSCP Marking/Remarking
- Soportar los siguientes Controles de Flood-Limiting por Puerto:
  - Broadcast
  - Multicast
  - Unknown Unicast
- Debe detectar dispositivos de telefonía IP o video de al menos 2 distintos fabricantes, una vez detectados aplicara configuración de forma dinámica en el puerto.
- Debe detectar dispositivos de telefonía IP de terceros para aplicar configuración de forma dinámica en el puerto, los dispositivos de teléfonia podrán emplear los protocolos:
  - H.323
  - SIP
  - Debe realizar Clasificacion y QoS de paquetes multicapa basado en usuario y así dar un tratamiento específico por Grupos de Usuario y Usuario
- Soportar al menos tres distintos mecanismos de gestión de colas (queuing)
- Soporte de múltiples usuarios/dispositivos (como teléfonos IP, computadoras, impresoras, fotocopiadoras, cámaras de seguridad, lectores de tarjeta, servidores virtuales, etc.) y múltiples métodos de autenticación (por 802.1x, WEP y MAC o la combinación de estos) en un puerto o en todos los puertos, soportando por lo menos 1000 usuarios/dispositivos autenticados por módulo.
- Soportar 802.1D
- Soportar 802.1p
- Poseer la funcionalidad de poder detectar eventos de intermitencias o flaps en los puertos y llevar a cabo acciones como inhabilitar el(los) puerto(s) involucrados y generar una entrada de log y/o envío de traps.
- Protección automática para conexión de dispositivos de comunicación no permitidos, los cuales activen el protocolo de STP y generen alguna reconvergencia en la red.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

- Soportar autentificación de usuarios administradores de equipos mediante TACACS+.
- Soportar al menos 9 grupos de RMON
- Debe ser capaz de clasificar tráfico en base a los siguientes criterios:
  - MAC source address
  - MAC destination addres
  - Source IPX address
  - Destination IPX address
  - Source IPX socket
  - Destination IPX socket
  - Transmission control IPX
  - IPX packet type
  - IPv6 source address
  - IPv6 destination address
  - IPv6 flow label
  - Source IP address.
  - Destination IP address.
  - IP fragmentation value.
  - UDP source port
  - UDP destination port
  - TCP source port
  - TCP destination port
  - ICMP packet type
  - Time-To-Live (TTL)
  - Type of Service
  - ICMPv6 packet type
  - VLAN tag
  - Port-string
  - Incluir la funcionalidad de limitar el acceso de una MAC Address dada a un puerto especifico, la cual puede aprender el equipo de forma estática o dinámica
- Incluir mecanismos de mitigación ante los siguientes ataques DoS:
  - Bad SIP
  - Christmas Tree
  - Fragmented ICMP
  - ICMP Flood
  - Large ICMP
  - LANd
  - Smurf
  - Fraggle Attack
  - SYN Flood
- Soportar RADIUS accounting / snooping
- Contar con al menos 3 mecanismos anti spoofing
- Soportar RFC 3580
- Soportar prevención de ARP storm

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- El equipo debe soportar e incluir una funcionalidad capaz de distinguir la identidad de un usuario/dispositivo que es autenticado en otro switch conectado a este mismo, pudiendo asignar alguna política de L2, L3 y L4, permitiendo, negando, etiquetando, redireccionando, asignando una prioridad y un rate limiting.
- Soportar funciones de mitigación de ataques de tipo DoS de tal forma que se pueden configurar umbrales permitidos de cantidad de tráfico, los cuales puedan desencadenar acciones como descartar tráfico excedente, envío de SNMP o logs e inclusive hasta desactivar una o más interfaces.

2.3.3.Switches de acceso

El LICITANTE ganador deberá mantener la operación en todas las sucursales del Instituto FONACOT, incluyendo Oficinas Centrales y Plaza de la Republica. Para el caso particular de estos dos últimos sitios, el LICITANTE debera implementar un esquema de alta disponibilidad en conjunto con los switches de CORE propuestos, para lo cual el LICITANTE deberá considerar el dimensionamiento adecuado en cuanto a hardware, licenciamiento, actualizaciones, componentes y cualquier otro elemento que se requiera para la adecuada operación de este esquema.

Los switches de acceso propuestos por el LICITANTE para este servicio, deberán cumplir con al menos las siguientes características técnicas:

2.3.3.1.Switch de acceso Tipo1

- El equipo deberá proveer al menos 03 ranuras para la inserción de tarjetas y crecimientos en un futuro.
- El equipo debe ser capaz de soportar las siguientes densidades de puertos:
  - 216 puertos 10/100/1000 Base-TX o 1000Base-X SFP
  - 96 puertos 10GBase-X SFP

  Soportar voltaje de Alimentación 100-240 VCA, a una frecuencia de 50-60 Hz
- Incluirá Ventiladores y Fuentes de alimentación de tipo Hot-swappable
- Proveer la facilidad de insertar, remover o reemplazar módulos, sin interrumpir la operación del sistema.
- El equipo deberá incluir al menos 2 fuentes de poder internas en modo redundante, para garantizar la total operación de la unidad, aun cuando una fuente de poder haya fallado. Las fuentes de poder redundantes deberán de realizar balanceo de carga.
- Debe soportar la funcionalidad de "Virtual Chassis", "Chassis Bonding", "Virtual Switching System" o similar. Con la finalidad de poder realizar configuraciones de alta disponibilidad a nivel de L2, sin que existan los

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

problemas y tiempo de re-convergencia por los protocolos de Spanning Tree, permitiendo la Administración de dos switches como uno sólo.

- Acorde a la arquitectura del equipo, deberá incluir redundancia en tarjetas supervisoras (controladoras) o en su defecto un esquema de procesamiento distribuido
- Debe incluir al menos:
  - 144 Puertos 10/100/1000Base-TX RJ45 PoE+
  - Se deberán incluir al menos 2 conectores opticos 10G SR SFP+
- Soportar auto-mdi/mdix, auto-sensing y auto-negotiation en todos los puertos 10/100/1000 Base-TX
- Contar con puerto serial USB y RJ45 para configuración del equipo y carga de firmware, así como de carga y descarga de archivos.
- Soportar Power over Ethernet con estándares 802.3af/802.3at
- La capacidad de conmutación o switching capacity del chasis deberá ser de al menos 360 Gbps
- Un Throughput IPv4 por chasis de al menos 360 Mpps
- Soportar un desempeño mínimo por cada tarjeta de servicio (tarjeta I/O) de 120 Gbps
- Contar con al menos 10 colas de prioridad (Queues) por puerto
- Soportar al menos 65,000 MAC Address
- Soportar al menos 4000 VLANs
- Deberá soportar e incluir Netflow
- Contar con el soporte de Jumbo frames.
- Soportar SNMP v1/v2c/v3
- Soportar al menos 15 mirrors por chasis, los cuales pueden ser de:
  - Uno a uno
  - Uno a muchos
  - Muchos a uno
  - Mirror de VLANs.
- Soportar Remote Port Mirror
- Soportar CDP v1/2
- Incluirá la funcionalidad Proxy ARP
- Incluir la funcionalidad Bi-directional Forwarding Detection (BFD)
- Contar con la funcionalidad Q-in-Q
- Ser capaz de implementar NTP (Network Time Protocol) ó SNTP (Simple Network Time Protocol).
- Incluirá la funcionalidad de NAT
- Con el sistema operativo base, deberá proveer la función de balanceo de servicios, de tal forma que se puedan generar gateways virtuales de servicios como WEB, SMTP o algún otro aplicativo, sin la necesidad de agregar módulos especiales y licenciamiento para este propósito.
- Soportar la funcionalidad DHCP Server / Relay
- Soportar la funcionalidad Unidirectional Link Detection
- Incluirá la funcionalidad de Supresión de Broadcast
- Soportar el estándar 802.1ak MVRP

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 65 74 00 www.fonacot.gob.mx

- Incluir la funcionalidad Generic VLAN Registration Protocol (GVRP)
- Soportar IGMP v1/v2/v3
- Soportar los siguientes Estándares:
  - 802.3u Fast Ethernet
  - 802.3ab Gigabit Ethernet
  - 802.3z Gigabit Ethernet
  - 802.3ae 10 Gigabit Ethernet
  - 802.3an 10Gase-T
- Soportar los siguientes Estándares:
  - 802.1Q VLANs
  - 802.1D MAC Bridges
  - 802.1w RSTP
  - 802.1s MST
  - 802.1t Path Cost
  - 802.3ad Link Aggregation
  - 802.3ae Gigabit Ethernet
  - 802.3x Flow Control
  - 802 1ab LLDP-MED
- Soportar el protocolo 802.3ad permitiendo la agrupación de hasta 190 LAG por chasis, y hasta 64 puertos por cada LAG.
- Soportar los siguientes Estándares:
  - 802.1Qaz ETS y DCBx
  - 802.1Qbb PFC
  - 802.1Qau Congestion Notification
  - Soportar Ruteo Estático
  - Soportar ACLs Estándar y Extendidas
  - Incluir Policy-Based Routing (PBR)
  - Soportar VRF en IPv4/IPv6
  - Soportar OSPF
  - Soportar OSPF ECMP
- Soportar RIP v2
- Soportar BGPv4
- Soportar L2VPN
- Soportar L3VPN over native MPLS
- Soportar PIM-DM
- Soportar al menos 1,000,000 de entradas en la tabla de ruteo IPv4
- Soportar al menos 50,000 de entradas en la tabla de ruteo IPv6
- Soportar al menos 100 interfaces IPv6
- Soportar al menos 10 IP helper address por interface
- Incluir las siguientes funcionalidades para IPv6:
  - Ruteo estático
  - DVMRPv3
  - OSPFv3
  - Ruteo basado en políticas IPv6 (PBR)
  - PIM-SM v6

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- PIM-SSM v6
- MLD v1/v2
- RIPng
- IPv6 ACLs
- DHCP relay
- Neighbor Discovery
- IPSec para OSPFv3

- Soportar los siguientes estandares:
  - RFC 1195 Use of OSI IS-IS for Routing in TCP/IP
  - RFC 1265 BGP Protocol Analysis
  - RFC 1266 Experience with the BGP Protocol
  - RFC 1519 CIDR
  - RFC 3101 OSPFv2 NSSA
  - RFC 1657 Managed Objects for BGP-4 using SMIv2
  - RFC 1771 A Border Gateway Protocol 4 (BGP-4)
  - RFC 1772 Application of BGP in the Internet
  - RFC 1773 Experience with the BGP-4 protocol
  - RFC 1774 BGP-4 Protocol Analysis
  - RFC 1812 General Routing/RIP Requirements
  - RFC 1853 IP in IP Tunneling
  - RFC 1886 DNS Extensions to support IP version 6
  - RFC 1930 Guidelines for creation, selection, and registration of an Autonomous System (AS)
  - RFC 1966 BGP Route Reflection
  - RFC 1981 Path MTU Discovery for IPv6
  - RFC 1998 BGP Community Attribute in Multi-home Routing
  - RFC 2003 IP Encapsulation within IP
  - RFC 2082 RIP-II MD5 Authentication
  - RFC 2260 Support for Multi-homed Multi-prov
  - RFC 2270 Dedicated AS for Sites Homed to one Provider
  - RFC 2373 Address notation compression
  - RFC2374 IPv6 Aggregatable Global Unicast Address Format
  - RFC2375 IPv6 Multicast Address Assignments
  - RFC 2391 Load Sharing Using Network Address Translation(LSNAT)
  - RFC2401 Security Architecture for the Internet Protocol
  - RFC2404 The Use of HMAC-SHA-1-96 within ESP and AH
  - RFC2406 IP Encapsulating Security Payload (ESP)
  - RFC2407 Internet IP Security Domain of Interpretation for ISAKMP
  - RFC2408 Internet Security Association and Key Management Proto-col (ISAKMP)
  - RFC 2409 The Internet Key Exchange (IKE)
  - RFC 2450 Proposed TLA and NLA Assignment Rule
  - RFC 2460 IPv6 Specification
  - RFC 2462 IPv6 Stateless Address Auto-configuration
  - RFC 2464 Transmission of IPv6 over Ethernet

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 06 74 00 www.fonacot.gob.mx

- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2474 Definition of DS Field in the IPv4/v6 Headers
- RFC 2519 A Framework for Inter-Domain Route Aggregation
- RFC 2547 BGP/MPLS VPNs
- RFC 2553 BasiCSocket Interface Extensions for IPv6
- RFC 2577 FTP Security Considerations
- RFC 2597 Assured Forwarding PHB Group
- RFC 2685 Virtual Private Networks Identifier
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2715 Interoperability Rules for Multicast Routing Protocols
- RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2784 Generic Routing Encapsulation
- RFC 2890 Key and Sequence Number Extensions to GRE
- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
- RFC 2894 Router Renumbering
- RFC 2918 Route Refresh Capability for BGP
- RFC 2966 Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3065 Autonomous System Confederations for BGP
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3162 RADIUS and IPv6
- RFC 3345 BGP Persistent Route Oscillation
- RFC 3359 TLV Codepoints in IS-IS
- RFC 3373 Three-Way Handshake for IS-IS
- RFC 3567 IS-IS Cryptographic Authentication
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC3596 DNS Extensions to Support IP Version 6
- RFC 3768 VRRP
- RFC 3769 Requirements for IPv6 Prefix Delegation
- RFC 3810 MLDv2 for IPv6
- RFC 3879 Deprecating Site Local Addresses
- RFC 3956 Embedding the RP Address in IPv6 MCAST Address
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4023 Encapsulating MPLS in IP
- RFC 4109 Algorithms for IKEv1
- RFC 4191 Default Router Preferences and More-Specific Routes
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4213 Basic Transition Mechanisms for IPv6
- RFC 4222 Prioritized Treatment of OSPFv2 Packets
- RFC 4264 BGP Wedgies
- RFC 4265 Definition of Textual Conventions for (VPN) Management
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4272 BGP Security Vulnerabilities Analysis

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

EdP

- RFC 4273 Managed Objects for BGP-4 using SMIv2
- RFC 4274 BGP-4 Protocol Analysis
- RFC 4276 BGP-4 Implementation Report
- RFC 4277 Experience with the BGP-4 protocol
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4301 Security Architecture for IP
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4305 Crypto Algorithm Requirements for ESP and AH
- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in IKEv2
- RFC 4308 Cryptographic Suites for IPSec
- RFC 4360 BGP Extended Communities Attribute
- RFC 4364 BGP/MPLS IP VPNs
- RFC 4365 Applicability Statement for BGP/MPLS IP VPNs
- RFC 4384 BGP Communities for Data Collection
- RFC 4443 ICMPv6 for IPv6
- RFC 4456 BGP Route Reflection
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4451 BGP MULTI_EXIT_DISC (MED) Considerations
- RFC 4541 MLD Snooping
- RFC 4552 Authentication/Confidentiality for OSPFv3
- RFC 4601 PIM-SM
- RFC 4604 IGMPv3 & MLDv2 & Source-Specific Multicast
- RFC 4607 Source-Specific Multicast for IP
- RFC 4608 PIM--SSM in 232/8
- RFC 4610 Anycast-RP Using PIM
- RFC 4611 MSDP Deployment Scenarios
- RFC 4632 Classless Inter-Domain Routing (CIDR)
- RFC 4659 BGP-MPLS (VPN) Extension for IPv6 VPN
- RFC 4724 Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4835 CryptoAlgorithm Requirements for ESP and AH
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 4884 Extended ICMP Multi-Part Messages
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 5059 Bootstrap Router (BSR) Mechanism for (PIM)
- RFC 5065 Autonomous System Confederations for BGP
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 5186 IGMPv3/MLDv2/MCAST Routing Protocol Interaction
- RFC 5187 OSPFv3 Graceful Restart
- RFC 5240 PIM Bootstrap Router MIB
- RFC 5250 The OSPF Opaque LSA Option
- RFC 5291 Outbound Route Filtering Capability for BGP-4
- RFC 5292 Address-Prefix-Outbound Route Filter for BGP-4

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 03 74 00 www.fonacot.gob.mx

- RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 5302 Domain-wide Prefix Distribution with IS-IS
- RFC 5303 3Way Handshake for IS-IS P2P Adjacencies
- RFC 5304 IS-IS Cryptographic Authentication
- RFC 5306 Restart Signaling for IS-IScol for BGP L3 VPNs
- Soportar las siguientes MIB:
- RFC 2578 SNMPv2 SMI
- RFC 3418 SNMPv2 MIB
- RFC 2576 SNMP-Community MIB
- RFC 2863 IF MIB
- RFC 3621 Power Ethernet MIB
- RFC 4750 OSPFv2 MIB

- CISCO CDP MIB
- CISCO NETFLOW MIB
- Incluir la funcionalidad de Redirección de peticiones Web

Funcionalidades de Administración y Monitoreo

- El equipo podrá ser Administrado por:
  - Puerto de Consola
  - SNMP
  - Remotamente por Sesión VTY
- Soportar SSHv2
- Soportar Telnet como Servidor y Cliente
- Soportar SNTP o NTP
- Soportar Interface Web de Gestión
- Poseer una función de actualización de firmware y almacenamiento de imágenes de respaldo en caso de que el proceso falle o bien la imagen se encuentre dañada o corrupta.
- Soportar Múltiples archivos de configuración
- Soportar download de imágenes de Sistema Operativo o Firmware y archivos de configuración desde servidores:
  - FTP
  - TFTP
  - SCP
- Incluir una funcionalidad para realizar upgrades de Sistema Operativo o Firmware de forma gradual por tarjeta y por Grupo de Tarjetas, de forma que no se reinicie el equipo completo para aplicar actualizaciones de Sistema Operativo.
- Incluir funcionalidad de IP SLA para la medición de jitter y delay
- Soportar VLAN de Administración
- Capacidad de envío de logs de acuerdo a su grado de severidad al menos hacia 8 servidores Syslog, de ser requerido.
- Soportar la Autenticación y Encripción por algoritmos aprobados FIPS
- Soportar la funcionalidad de especificar por usuario administrador la hora de inicio y termino de acceso al equipo.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

- Soportar la funcionalidad de especificar la cantidad máxima de sesiones simultáneas por usuario administrador en el switch.
- Soportar la funcionalidad de especificar la cantidad máxima de días de inactividad por usuario administrador, antes de que la cuenta sea deshabilitada en el switch
- Soportar la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula
  - Letra minúscula
  - Numero
  - Caracteres especiales
  - Contar con un packet buffering.
- Soportar 802.3 2008 Clause 57 Ethernet OAM – Link Layer OAM

Funciones de Control y Seguridad

- Soportar rate-limiting desde 8 Kbps
- Soportar rate-limiting de entrada y salida
- Soportar IP ToS/DSCP Marking/Remarking
- Soportar los siguientes Controles de Flood-Limiting por Puerto:
  - Broadcast
  - Multicast
  - Unknown Unicast
- Debe detectar dispositivos de telefonía IP o video de al menos 2 distintos fabricantes, una vez detectados aplicara configuración de forma dinámica en el puerto.
- Debe detectar dispositivos de telefonía IP de terceros para aplicar configuración de forma dinámica en el puerto, los dispositivos de teléfonia podrán emplear los protocolos:
  - H.323
  - SIP
- Debe realizar Clasificacion y QoS de paquetes multicapa basado en usuario y así dar un tratamiento específico por Grupos de Usuario y Usuario
- Soporte de múltiples usuarios/dispositivos (como teléfonos IP, computadoras, impresoras, fotocopiadoras, cámaras de seguridad, lectores de tarjeta, servidores virtuales, etc.) y múltiples métodos de autenticación (por 802.1x, WEP y MAC o la combinación de estos) en un puerto o en todos los puertos, soportando por lo menos 1000 usuarios/dispositivos autenticados por módulo.
- Soportar 802.1D
- Soportar 802.1p
- Poseer la funcionalidad de poder detectar eventos de intermitencias o flaps en los puertos y llevar a cabo acciones como inhabilitar el(los) puerto(s) involucrados y generar una entrada de log y/o envío de traps.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Protección automática para conexión de dispositivos de comunicación no permitidos, los cuales activen el protocolo de STP y generen alguna reconvergencia en la red.
- Soportar autentificación de usuarios administradores de equipos mediante TACACS+.
- Soportar al menos 9 grupos de RMON
- Debe ser capaz de clasificar tráfico en base a los siguientes criterios:
  - MAC source address
  - MAC destination addres
  - Source IPX address
  - Destination IPX address
  - Source IPX socket
  - Destination IPX socket
  - Transmission control IPX
  - IPX packet type
  - IPv6 source address
  - IPv6 destination address
  - IPv6 flow label
  - Source IP address.
  - Destination IP address.
  - IP fragmentation value.
  - UDP source port
  - UDP destination port
  - TCP source port
  - TCP destination port
  - ICMP packet type
  - Time-To-Live (TTL)
  - Type of Service
  - ICMPv6 packet type
  - VLAN tag
  - Port-string
- Incluir la funcionalidad de limitar el acceso de una MAC Address dada a un puerto especifico, la cual puede aprender el equipo de forma estática o dinámica
- Incluir mecanismos de mitigación ante los siguientes ataques DoS:
  - Bad SIP
  - Fragmented ICMP
  - ICMP Flood
  - Large ICMP
  - LANd
  - Smurf
  - Fraggle Attack
  - SYN Flood
- Contar con al menos 3 distintos mecanismos anti-spoofing
- Soportar RADIUS accounting / snooping

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Soportar RFC 3580
- Soportar prevención de ARP storm
- El equipo debe soportar e incluir una funcionalidad capaz de distinguir la identidad de un usuario/dispositivo que es autenticado en otro switch conectado a este mismo, pudiendo asignar alguna política de L2, L3 y L4, permitiendo, negando, etiquetando, redireccionando, asignando una prioridad y un rate limiting.
- Soportar funciones de mitigación de ataques de tipo DoS de tal forma que se pueden configurar umbrales permitidos de cantidad de tráfico, los cuales puedan desencadenar acciones como descartar tráfico excedente, envío de SNMP o logs e inclusive hasta desactivar una o más interfases

2.3.3.2. Switch de acceso Tipo2

- Switch apilable con desempeño mínimo de 260 Gbps y 193 Mpps con arquitectura no bloqueable, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad.
- El equipo debe contar con al menos la siguiente densidad de puertos:
  - 48 puertos 10/100/1000 BASE-T
  - 4 puertos 10GBase-X (SFP+) se deberán incluir al menos 2 conectores opticos 10G SR SFP+
  - 2 Puertos de apilamiento dedicado
  - 1 puerto serial
  - 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda
  - 1 puerto USB para almacenamiento externo
- El equipo deberá soportar el siguiente tipo de interfaces:
  - Gigabit Ethernet: SX, LX, ZX, BX-D, BX-U, 100FX/1000LX, 10/100/1000BASE-T en formato SFP
  - 10 Gigabit Ethernet: SR, LR, ER, LRM y CR en formato SFP+
- Deberá contar con un procesador de 64-bits a 1GHz y al menos 1GB en RAM
- Soporte de los siguientes estándares:
  - IEEE 802.3af / at
  - IEEE 802.3az
- El equipo debe contar con un sistema de ventilación Front-to-Back.
- El equipo debe soportar fuentes redundantes internas.
- El equipo deberá estar diseñado para una altura no mayor a una unidad de rack (1 RU)
- El equipo debe tener una latencia menor a 5 micro segundos
- Soportar al menos 50,000 MAC Address
- Soportar al menos 4094 VLANs
- Soporte de Jumbo Frames 9216 Bytes

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 5531 52 65 74 00 www.fonacot.gob.mx

- El equipo debe ser capaz de soportar apilamiento con un ancho de banda de al menos 80 Gbps
- Soporte de apilamiento de hasta 8 unidades
- Deberá tener la capacidad de apilarse con switches de la misma familia de productos, aunque sea otro modelo de menor o mayor capacidad.
- Funcionalidades de Capa 2, Switching
- El equipo deberá soportar al menos las siguientes funcionalidades y especificaciones:
- Soporte de IEEE 802.1D STP
- Soporte de IEEE 802.1w RSTP
- Soporte de IEEE 802.1s MSTP
- Soporte de PVST+, Per VLAN STP
- Soporte de IEEE 802.3ad LACP, con la capacidad de al menos 120 grupos de agregación cuyo máximo sea de al menos 30 puertos por cada cada grupo.
- Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
- Soporte de LLDP-MED
- Soporte de Cisco Discovery Protocol (CDP) v1 y v2
- Soporte de IEEE 802.1ag Connectivity Fault Management
- Soporte del estándar Y.1731 Frame Delay
- Soporte de ITU G.8032 Ethernet Ring Protection Switching
- Soporte de PIM Snooping
- Soporte de Multicast VLAN Registration (MVR)
- Soporte de IEEE 802.1Q VLAN Tagging
- Soporte de IEEE 802.1v
- Soporte de VLANs basadas por Puerto, MAC y Protocolo
- Contar con la capacidad de trasladar los tags 802.1Q de varias VLANs al tag de una sola VLAN.
- Soporte de IEEE 802.1AK MVRP
- IEEE 802.1 Audio Video Bridging (AVB), este protocolo no es imprescindible incluirlo en la propuesta, sin embargo, el equipo ofertado deberá estar capacitado para soportarlo sin la necesidad de hardware adicional.
- Deberá de soportar un mecanismo de redundancia a nivel de capa 2, que permita un tiempo de recuperación en caso de caída o restauración de la red en menos de 1 segundo, garantizando disponibilidad y confiabilidad a la red para aplicaciones como voz y video. Este mecanismo deberá de trabajar al menos en topologías de anillo.
- Deberá de contar con un mecanismo correctivo de detección de Loops que permita tomar medidas de manera inmediata ante una falla en la red, diferente a Spanning Tree Protocol.
- Deberá contar con una funcionalidad que permita conjuntar o agregar puertos en al menos 2 switches de tal forma que dicho arreglo proporcione una sóla conexión lógica hacia otro dispositivo, en donde

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

dicho dispositivo puede ser un servidor o algún otro dispositivo de red que puede ser configurado por medio de algún protocolo como LAG o similar.

- Soporte de Port Mirroring tanto local como remoto
- Soportar al menos 120 filtros por puerto espejo, permitiendo una mayor granularidad en el tipo de información que se necesita monitorear
- Funcionalidades de Clasificación de Tráfico y Calidad de Servicio
- Contar con al menos 8 colas (queues) por puerto y soportar los siguientes algoritmos de encolamiento: Weigthed Fair Queuing, Round Robin Priority y Strict Priority Queuing
- Calidad de servicio aplicable a tráfico por clasificación de acuerdo a los siguientes criterios: VLAN ID, dirección MAC, dirección IP, puerto TCP/UDP, 802.1p, DiffServ
- Soportar un rate-limiting con una granularidad de 8 kbps tanto de ingreso como de egreso
- Soporte de rate shaping
- Funcionalidades de Capa 3
- Soporte IGMP v1/v2/v3
- Ruteo estático unicast y multicast para IPv4
- Deberá soportar al menos 15,000 entradas de IPv4
- Soporte de IP Route Compression
- Soporte de CIDR
- Soporte de ECMP
- Soporte de VRRPv2
- Soporte de BOOTP/DHCP relay agent y DHCP server
- Soporte de RIPv1 y RIPV2
- Soporte de OSPFv2
- Soporte de Autenticación MD5 para OSPF
- Soporte de PIM-SM, PIM-SSM
- Soporte de Policy Based Routing para IPv4 e IPv6
- Soportar al menos 8,000 entradas en IPv6
- Soporte de Virtual Routers, al menos 48
- Soporte de VRFs
- Soporte de ruteo estático unicast para IPv6
- Soporte de RIPng
- Soporte de MLDv1/v2
- Soporte de ICMP sobre IPv6
- Soporte de Traceroute sobre IPv6
- Soporte de Telnet sobre IPv6
- Soporte de SSHv2 sobre IPv6
- Soporte de las siguientes especificaciones para IPv6:
  - RFC 2460 - Internet Protocol,Version 6 (IPv6) Specification
  - RFC 4861 - Neighbor Discovery for IP Version 6
  - RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks
  - RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. 1551 52 65 74 60 www.fonacot.gob.mx

- RFC 5722 - Handling of Overlapping IPv6
- RFC 2462 - IPv6 Stateless Address Auto Configuration – Router Requirements
- RFC 2740 OSPF v3 for IPv6 Seguridad

- El equipo debe contar con protección para contra ataques DoS y man-in-the-middle
- El sistema operativo del equipo debe soportar CLI Scripting, que permita automatizar configuraciones, tales como QoS, ACLs, etc.
- El equipo debe soportar múltiples suplicantes por puerto, y múltiples métodos de autenticación: 802.1x, MAC y Web
- El equipo debe ser capaz de permitir el acceso a la red de los usuarios, a través de autenticación y Kerberos snooping.
- Debe contar con la funcionalidad de aplicar políticas de seguridad (perfiles), con base al rol que tenga el usuario de la red en la organización, y debe contar con las siguientes características:
- La creación de roles o perfiles deberá ajustarse a las necesidades del negocio, de tal modo que cada uno cuente con los privilegios específicos para el acceso de los recursos de red y de aplicativos.
- El rol o perfil debe ser asignado por usuario y este debe prevalecer incluso si se mueve de puerto.
- El rol o perfil puede ser asignado de forma dinámica por medio de mecanismos de autenticación RADIUS con base en lo siguiente:
  - Por atributos que la propia arquitectura defina tales como campos Filter-ID o VSA.
  - Soporte del estándar RFC 3580 por medio de atributos VLAN Tunnels,
  - Soportar un modo mixto o híbrido, de acuerdo a los dos esquemas antes solicitados.
- La funcionalidad de políticas o perfiles de seguridad debe contar con al menos las siguientes capacidades:
  - 60 Periles o Roles por Switch
  - 800 Reglas por cada perfil o rol por Switch
  - 128 usuarios autenticados por Puerto
  - 512 usuarios por Switch
- La funcionalidad de políticas o perfiles de seguridad debe ser capaz de clasificar o identificar el tráfico por los siguientes criterios de capa 2/3/4:
  - Por identificación del campo Type de tramas Ethernet II
  - Dirección MAC origen/destino
  - Dirección IP origen/destino
  - Dirección IPX origen/destino
  - Socket IPX origen/destino
  - Por el campo de tipo de servicio (Type of Service) en los paquetes IP
  - Puerto UDP y TCP origen/destino
  - Puerto UDP y TCP origen/destino
  - Por tipo de ICMP

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

  - Por tipo de Protocolo IP
  - Por identificador del puerto físico del equipo
  - Por el TAG de la VLAN
- La funcionalidad de políticas o perfiles de seguridad debe de contar con al menos las siguientes acciones a ejecutar:
  - Asignación de VLAN
  - Filtrado de tráfico (Permitir/Negar)
  - Asignación de Rate-Limiting
  - Rate Shaping
  - Priorización del tráfico
  - Manipulación y reescritura del campo TCI
- Deberá contar con un mecanismo de seguridad que permita detectar amenazas y reaccionar ante la intrusión de la red. Esto basado en modelo de alertas basadas en el traspaso de umbrales definidos por el administrador de la red.
- Deberá contar con herramientas que permitan rastrear a los usuarios de la red y proporcionar información tal como: el switch al que se conecta el usuario, el puerto físico de conexión, la MAC address, la VLAN de trabajo e identidad del usuario.
- El equipo deberá de soportar aprovisionamiento automático a través de perfiles, basados en eventos como el logging o logoff de un usuario, hora del día por medio del uso de scripts o LLDP, permitiendo configurar los parámetros necesarios de manera automática en el puerto para soluciones de telefonía IP, videoconferencia, video vigilancia, autenticación de usuarios.
- Deberá de contar con un mecanismo que permita soportar la migración de máquinas virtuales, configuración de su puerto e inventario de manera automática, el equipo deberá de ser capaz de identificar la máquina virtual a través de su dirección MAC y autenticar la conexión a la red, aplicar la configuración al puerto autenticado y remover la configuración del puerto en donde la máquina virtual ha sido removida, así como de las políticas que se le hayan aplicado a la misma, sin necesidad de reconfigurar los equipos de la red.
- Deberá de contar con un mecanismo de notificaciones de eventos a través de XML, como un cambio en la configuración, cambio de estado, o cualquier evento deseado que quiera ser reportado, a través de un servidor Web externo, esto con la finalidad de alinear la estrategia de las mejores prácticas de TI y contar con una bitácora precisa de los cambios y eventos ocurridos en la red.
- Soporte de las siguientes especificaciones:
  - RFC 1492 TACACS+
  - RFC 1866 HTML
  - RFC 3580 IEEE 802.1x RADIUS
  - RFC 3579 RADIUS EAP
  - RFC 2866 RADIUS Accounting

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. +55 5241 6573 00 www.fonacot.gob.mx

- RFC 2865 RADIUS Authentication
- RFC 4668 RADIUS Authentication Client MIB for IPv6
- RFC 4670 RADIUS Accounting Client MIB for Ipv6
- Soporte de Listas de Control de Acceso (ACLs) en capas 2/3/4 y Wire-Speed

- Deberá de soportar al menos 4,000 listas de control de acceso para garantizar la seguridad de la red.
- Manejo de Guest VLAN para 802.1x
- Soporte de SSL/TLS
- Soporte de mecanismos para la limitar el número de direcciones MAC determinadas por puerto.
- Soporte de mecanismo para prevenir que dispositivos no autorizados tengan acceso a la red basados en su dirección MAC, garantizando sólo aquellos que estén debidamente registrados o asociados a los puertos.
- Soporte de DHCP Snooping o Trusted DHCP Server
- Soporte de Dynamic ARP Inspection o ARP Validation
- Soporte de MD5 para protocolos de enrutamientoistración
- Debe contar un esquema de protección de memoria para cada aplicación, para que se manejen como procesos separados; el sistema operativo deberá ser modular y contar con funciones de monitoreo y reinicio de procesos sin la necesidad de reiniciar el equipo completamente.
- Contar con APIs XML para integración con terceros.
- Contar con la capacidad de soportar scripts CLI a través de lenguajes de programación como Python.
- Soporte de Telnet en modalidad cliente y servidor
- Soporte de SSH2 en modalidad cliente y servidor
- Soporte de SCP en modalidad cliente y servidor
- Soporte de SFTP en modalidad servidor
- Soporte de TFTP
- Soporte de Syslog para envío de al menos para 4 servidores
- Soporte de las siguientes especificaciones:
  - RFC 1650 Ethernet-Like MIB
  - RFC 1901 – 1908 SNMPv2c, SMIv2 and Revised MIB-II
  - RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management Framework
  - RFC 1155 Structure of Management Information (SMIv1)
  - RFC 5905 1 – Network Time Protocol v4
  - RFC 2030 – SNTP, Simple Network Time Protocol v4
  - RFC 2613 SMON MIB
  - RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- Soporte de SNMPv1/v2/v3
- Soporte de gestión vía HTTP y HTTPS
- 4 Grupos de RMON

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

- Soportar la funcionalidad de muestreo mediante el protocolo sFlow v5 o IPFIX
- Soporte de DDMI
- Manejo de múltiples archivos de configuración
- Manejo de múltiples imágenes de firmware o Sistema operativo
- Soportar la funcionalidad de especificar un periodo de inactividad en las cuentas de administrador local después de haber sido bloqueada por intentos fallidos de la misma y tener la capacidad de habilitarse automáticamente al haber transcurrido el periodo especificado.
- Soportar la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula
  - Letra minúscula
  - Numero
  - Caracteres especiales
- Soportar la funcionalidad de prevenir que un usuario administrador local pueda emplear un password que anteriormente empleó y ya ha caducado.
- Soportar SDN OpenStack, con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Funcionalidad para configurar un modelo de Redes Definidas por Software (SDN) mediante la especificación de estándar abierto OpenFlow 1.0, con el cual desde un Sistema Controlador se manipulen los flujos de datos usando protocolos estándares para que de forma dinámica se configuren las tablas de flujos, esto con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Deberá de contar con la capacidad de manejar comunicación FCoE, iSCI via Data Center Bridging IEEE P802.1Qaz
- Deberá soportar la especificación IEEE VEPA – Direct Attach
- Especificaciones a cumplir y Condiciones de Operación
- Rango de Temperatura de Operación: 0°C - 48°C
- Humedad en condiciones operativas: 10 – 95 % Humedad relativa no condensada
- Altura en condiciones operativas: 0 – 4500 m
- UL 60950-1
- FCC 21CFR 1040.10 (U.S. Laser Safety)
- EN 60825-1+A2:2001 (Lasers Safety)
- FCC CFR 47 part 15 Class A (USA)
- EN 55022:2006+A1:2007 Class A
- EN 61000-3-2 (Harmonics)
- EN 61000-3-3 2008 (Flicker)
- CISPR 22: 2006 (International Emissions)
- CISPR 24:A2:2003 Class A (International Immunity)
- IEC 61000-4-5:2005

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 4551 52 05 74 00 www.fonacot.gob.mx

- EN 61000-4-5:2006
- IEC/EN 61000-4-11:2004
- ETSI EN 300 386:2001
- VCCI Class A
- ETSI EN 300 019

2.3.3.3. Switch de acceso Tipo 3

Características Generales

- Switch apilable con desempeño mínimo de 212 Gbps y 157 Mpps con arquitectura no bloqueable, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad.
- El equipo debe contar con al menos la siguiente densidad de puertos:
  - 24 puertos 10/100/1000 BASE-T
  - 4 puertos 10GBase-X (SFP+) se deberán incluir al menos 2 conectores ópticos 10G SR SFP+
  - 2 Puertos de apilamiento dedicado.
  - 1 puerto serial
  - 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda
  - 1 puerto USB para almacenamiento externo
- El equipo deberá soportar el siguiente tipo de interfaces:
  - Gigabit Ethernet: SX, LX, ZX, BX-D, BX-U, 100FX/1000LX, 10/100/1000BASE-T en formato SFP
  - 10 Gigabit Ethernet: SR, LR, ER, LRM y CR en formato SFP+
- Deberá contar con un procesador de 64-bits a 1GHz y al menos 1GB en RAM
- Soporte de los siguientes estándares:
  - IEEE 802.3af / at
  - IEEE 802.3az
- El equipo debe contar con un sistema de ventilación Front-to-Back.
- El equipo debe soportar fuentes redundantes internas.
- El equipo deberá estar diseñado para una altura no mayor a una unidad de rack (1 RU)
- El equipo debe tener una latencia menor a 5 micro segundos
- Soportar al menos 50,000 MAC Address
- Soportar al menos 4094 VLANs
- Soporte de Jumbo Frames 9216 Bytes
- El equipo debe ser capaz de soportar apilamiento con un ancho de banda de al menos 80 Gbps
- Soporte de apilamiento de hasta 8 unidades
- Deberá tener la capacidad de apilarse con switches de la misma familia de productos aunque sea otro modelo de menor o mayor capacidadades de Capa 2, Switching

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- El equipo deberá soportar al menos las siguientes funcionalidades y especificaciones:
  - Soporte de IEEE 802.1D STP
  - Soporte de IEEE 802.1w RSTP
  - Soporte de IEEE 802.1s MSTP
  - Soporte de PVST+, Per VLAN STP
  - Soporte de IEEE 802.3ad LACP, con la capacidad de al menos 120 grupos de agregación cuyo máximo sea de al menos 30 puertos por cada cada grupo.
  - Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
  - Soporte de LLDP-MED
  - Soporte de Cisco Discovery Protocol (CDP) v1 y v2
  - Soporte de IEEE 802.1ag Connectivity Fault Management
  - Soporte del estándar Y.1731 Frame Delay
  - Soporte de ITU G.8032 Ethernet Ring Protection Switching
  - Soporte de PIM Snooping
  - Soporte de Multicast VLAN Registration (MVR)
  - Soporte de IEEE 802.1Q VLAN Tagging
  - Soporte de IEEE 802.1v
  - Soporte de VLANs basadas por Puerto, MAC y Protocolo
  - Contar con la capacidad de trasladar los tags 802.1Q de varias VLANs al tag de una sola VLAN.
- Deberá de soportar un mecanismo de redundancia a nivel de capa 2, que permita un tiempo de recuperación en caso de caída o restauración de la red en menos de 1 segundo, garantizando disponibilidad y confiabilidad a la red para aplicaciones como voz y video. Este mecanismo deberá de trabajar al menos en topologías de anillo.
- Deberá de contar con un mecanismo correctivo de detección de Loops que permita tomar medidas de manera inmediata ante una falla en la red, diferente a Spanning Tree Protocol.
- Deberá contar con una funcionalidad que permita conjuntar o agregar puertos en al menos 2 switches de tal forma que dicho arreglo proporcione una sóla conexión lógica hacia otro dispositivo, en donde dicho dispositivo puede ser un servidor o algún otro dispositivo de red que puede ser configurado por medio de algún protocolo como LAG o similar.
- Soporte de Port Mirroring tanto local como remoto
- Soportar al menos 120 filtros por puerto espejo, permitiendo una mayor granularidad en el tipo de información que se necesita monitoreardad de Servicio
- Contar con al menos 8 colas (queues) por puerto y soportar los siguientes algoritmos de encolamiento: Weigthed Fair Queuing, Round Robin Priority y Strict Priority Queuing
- Calidad de servicio aplicable a tráfico por clasificación de acuerdo a los siguientes criterios: VLAN ID, dirección MAC, dirección IP, puerto TCP/UDP, 802.1p, DiffServ

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 65 73 00 www.fonacot.gob.mx

- Soportar un rate-limiting con una granularidad de 8 kbps tanto de ingreso como de egreso
- Soporte de rate shapingnalidades de Capa 3
- Soporte IGMP v1/v2/v3
- Ruteo estático unicast y multicast para IPv4
- Deberá soportar al menos 15,000 entradas de IPv4
- Soporte de IP Route Compression
- Soporte de CIDR
- Soporte de ECMP
- Soporte de VRRPv2
- Soporte de BOOTP/DHCP relay agent y DHCP server
- Soporte de RIPv1 y RIPV2
- Soporte de OSPFv2
- Soporte de Autenticación MD5 para OSPF
- Soporte de PIM-SM, PIM-SSM
- Soporte de Policy Based Routing para IPv4 e IPv6
- Soportar al menos 8,000 entradas en IPv6
- Soporte de Virtual Routers, al menos 48
- Soporte de VRFs
- Soporte de ruteo estático unicast para IPv6
- Soporte de RIPng
- Soporte de MLDv1/v2
- Soporte de ICMP sobre IPv6
- Soporte de Traceroute sobre IPv6
- Soporte de Telnet sobre IPv6
- Soporte de SSHv2 sobre IPv6
- Soporte de las siguientes especificaciones para IPv6:
  - RFC 2460 - Internet Protocol,Version 6 (IPv6) Specification
  - RFC 4861 - Neighbor Discovery for IP Version 6
  - RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks
  - RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture
  - RFC 5722 - Handling of Overlapping IPv6
  - RFC 2462 - IPv6 Stateless Address Auto Configuration – Router Requirements
  - RFC 2740 OSPF v3 for IPv6
- El equipo debe contar con protección para contra ataques DoS y man-in-the-middle
- El sistema operativo del equipo debe soportar CLI Scripting, que permita automatizar configuraciones, tales como QoS, ACLs, etc.
- El equipo debe soportar múltiples suplicantes por puerto, y múltiples métodos de autenticación: 802.1x, MAC y Web
- El equipo debe ser capaz de permitir el acceso a la red de los usuarios, a través de autenticación y Kerberos snooping.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Debe contar con la funcionalidad de aplicar políticas de seguridad (perfiles), con base al rol que tenga el usuario de la red en la organización, y debe contar con las siguientes características:
- La creación de roles o perfiles deberá ajustarse a las necesidades del negocio, de tal modo que cada uno cuente con los privilegios específicos para el acceso de los recursos de red y de aplicativos.
- El rol o perfil debe ser asignado por usuario y este debe prevalecer incluso si se mueve de puerto.
- El rol o perfil puede ser asignado de forma dinámica por medio de mecanismos de autenticación RADIUS con base en lo siguiente:
- Por atributos que la propia arquitectura defina tales como campos Filter-ID o VSA.
- Soporte del estándar RFC 3580 por medio de atributos VLAN Tunnels,
- Soportar un modo mixto o híbrido, de acuerdo a los dos esquemas antes solicitados.
- La funcionalidad de políticas o perfiles de seguridad debe contar con al menos las siguientes capacidades:
  - 60 Periles o Roles por Switch
  - 800 Reglas por cada perfil o rol por Switch
  - 128 usuarios autenticados por Puerto
  - 512 usuarios por Switch
- La funcionalidad de políticas o perfiles de seguridad debe ser capaz de clasificar o identificar el tráfico por los siguientes criterios de capa 2/3/4:
  - Por identificación del campo Type de tramas Ethernet II
  - Dirección MAC origen/destino
  - Dirección IP origen/destino
  - Dirección IPX origen/destino
  - Socket IPX origen/destino
  - Por el campo de tipo de servicio (Type of Service) en los paquetes IP
  - Puerto UDP y TCP origen/destino
  - Puerto UDP y TCP origen/destino
  - Por tipo de ICMP
  - Por tipo de Protocolo IP
  - Por identificador del puerto físico del equipo
  - Por el TAG de la VLAN
- La funcionalidad de políticas o perfiles de seguridad debe de contar con al menos las siguientes acciones a ejecutar:
  - Asignación de VLAN
  - Filtrado de tráfico (Permitir/Negar)
  - Asignación de Rate-Limiting
  - Rate Shaping
  - Priorización del tráfico
  - Manipulación y reescritura del campo TCI
- Deberá contar con un mecanismo de seguridad que permita detectar amenazas y reaccionar ante la intrusión de la red. Esto basado en modelo

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 65 74 00 www.fonacot.gob.mx

de alertas basadas en el traspaso de umbrales definidos por el administrador de la red.

- Deberá contar con herramientas que permitan rastrear a los usuarios de la red y proporcionar información tal como: el switch al que se conecta el usuario, el puerto físico de conexión, la MAC address, la VLAN de trabajo e identidad del usuario.
- El equipo deberá de soportar aprovisionamiento automático a través de perfiles, basados en eventos como el logging o logoff de un usuario, hora del día por medio del uso de scripts o LLDP, permitiendo configurar los parámetros necesarios de manera automática en el puerto para soluciones de telefonía IP, videoconferencia, video vigilancia, autenticación de usuarios.
- Deberá de contar con un mecanismo que permita soportar la migración de máquinas virtuales, configuración de su puerto e inventario de manera automática, el equipo deberá de ser capaz de identificar la máquina virtual a través de su dirección MAC y autenticar la conexión a la red, aplicar la configuración al puerto autenticado y remover la configuración del puerto en donde la máquina virtual ha sido removida, así como de las políticas que se le hayan aplicado a la misma, sin necesidad de reconfigurar los equipos de la red.
- Deberá de contar con un mecanismo de notificaciones de eventos a través de XML, como un cambio en la configuración, cambio de estado, o cualquier evento deseado que quiera ser reportado, a través de un servidor Web externo, esto con la finalidad de alinear la estrategia de las mejores prácticas de TI y contar con una bitácora precisa de los cambios y eventos ocurridos en la red.
- Soporte de las siguientes especificaciones:
  - RFC 1492 TACACS+
  - RFC 1866 HTML
  - RFC 3580 IEEE 802.1x RADIUS
  - RFC 3579 RADIUS EAP
  - RFC 2866 RADIUS Accounting
  - RFC 2865 RADIUS Authentication
  - RFC 4668 RADIUS Authentication Client MIB for IPv6
  - RFC 4670 RADIUS Accounting Client MIB for Ipv6
- Soporte de Listas de Control de Acceso (ACLs) en capas 2/3/4 y Wire-Speed
- Deberá de soportar al menos 4,000 listas de control de acceso para garantizar la seguridad de la red.
- Manejo de Guest VLAN para 802.1x
- Soporte de SSL/TLS
- Soporte de mecanismos para la limitar el número de direcciones MAC determinadas por puerto.
- Soporte de mecanismo para prevenir que dispositivos no autorizados tengan acceso a la red basados en su dirección MAC, garantizando sólo aquellos que estén debidamente registrados o asociados a los puertos.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Soporte de DHCP Snooping o Trusted DHCP Server
- Soporte de Dynamic ARP Inspection o ARP Validation
- Soporte de MD5 para protocolos de enrutamiento
- Funcionalidades de Administración
- Debe contar un esquema de protección de memoria para cada aplicación, para que se manejen como procesos separados; el sistema operativo deberá ser modular y contar con funciones de monitoreo y reinicio de procesos sin la necesidad de reiniciar el equipo completamente.
- Contar con APIs XML para integración con terceros.
- Contar con la capacidad de soportar scripts CLI a través de lenguajes de programación como Python.
- Soporte de Telnet en modalidad cliente y servidor
- Soporte de SSH2 en modalidad cliente y servidor
- Soporte de SCP en modalidad cliente y servidor
- Soporte de SFTP en modalidad servidor
- Soporte de TFTP
- Soporte de Syslog para envío de al menos para 4 servidores
- Soporte de las siguientes especificaciones:
  - RFC 1650 Ethernet-Like MIB
  - RFC 1901 – 1908 SNMPv2c, SMIv2 and Revised MIB-II
  - RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management Framework
  - RFC 1155 Structure of Management Information (SMIv1)
  - RFC 5905 1 – Network Time Protocol v4
  - RFC 2030 – SNTP, Simple Network Time Protocol v4
  - RFC 2613 SMON MIB
  - RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- Soporte de SNMPv1/v2/v3
- Soporte de gestión vía HTTP y HTTPS
- 4 Grupos de RMON
- Soportar la funcionalidad de muestreo mediante el protocolo sFlow v5 o IPFIX
- Soporte de DDMI
- Manejo de múltiples archivos de configuración
- Manejo de múltiples imágenes de firmware o Sistema operativo
- Soportar la funcionalidad de especificar un periodo de inactividad en las cuentas de administrador local después de haber sido bloqueada por intentos fallidos de la misma y tener la capacidad de habilitarse automáticamente al haber transcurrido el periodo especificado.
- Soportar la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, CP 06760, México D.F.
Tel. (55) 52 -- 67 74 00 www.fonacot.gob.mx

- Letra minúscula
- Numero
- Caracteres especiales
- Soportar la funcionalidad de prevenir que un usuario administrador local pueda emplear un password que anteriormente empleó y ya ha caducado.
- Funcionalidades Especiales

- Soportar SDN OpenStack, con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Funcionalidad para configurar un modelo de Redes Definidas por Software (SDN) mediante la especificación de estándar abierto OpenFlow, con el cual desde un Sistema Controlador se manipulen los flujos de datos usando protocolos estándares para que de forma dinámica se configuren las tablas de flujos, esto con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Deberá de contar con la capacidad de manejar comunicación FCoE, iSCI via Data Center Bridging IEEE P802.1Qaz
- Deberá soportar la especificación IEEE VEPA – Direct Attach
- Especificaciones a cumplir y Condiciones de Operación
- Rango de Temperatura de Operación: 0°C - 48°C
- Humedad en condiciones operativas: 10 – 95 % Humedad relativa no condensada
- Altura en condiciones operativas: 0 – 4500 m
- UL 60950-1
- FCC 21CFR 1040.10 (U.S. Laser Safety)
- EN 60825-1+A2:2001 (Lasers Safety)
- FCC CFR 47 part 15 Class A (USA)
- EN 55022:2006+A1:2007 Class A
- EN 61000-3-2 (Harmonics)
- EN 61000-3-3 2008 (Flicker)
- CISPR 22: 2006 (International Emissions)
- CISPR 24:A2:2003 Class A (International Immunity)
- IEC 61000-4-5:2005
- EN 61000-4-5:2006
- IEC/EN 61000-4-11:2004
- ETSI EN 300 386:2001
- VCCI Class A
- ETSI EN 300 019

2.3.3.4. Switch de acceso Tipo4

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 63 74 00 www.fonacot.gob.mx

- Switch apilable con desempeño mínimo de 260 Gbps y 193 Mpps con arquitectura no bloqueable, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad.
- El equipo debe contar con al menos la siguiente densidad de puertos:
  - 48 puertos 10/100/1000 BASE-T
  - 1 puerto serial
  - 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda
  - 1 puerto USB para almacenamiento externo
- El equipo deberá soportar el siguiente tipo de interfaces:
  - Gigabit Ethernet: SX, LX, ZX, BX-D, BX-U, 100FX/1000LX, 10/100/1000BASE-T en formato SFP
  - 10 Gigabit Ethernet: SR, LR, ER, LRM y CR en formato SFP+
- Soporte de los siguientes estándares:
  - IEEE 802.3af / at
  - IEEE 802.3az
- El equipo debe soportar fuentes redundantes.
- El equipo debe tener una latencia menor a 5 micro segundos
- Soportar al menos 32,000 MAC Address
- Soportar al menos 4094 VLANs
- Soporte de Jumbo Frames.
- Funcionalidades de Capa 2, Switching
- El equipo deberá soportar al menos las siguientes funcionalidades y especificaciones:
- Soporte de IEEE 802.1D STP
- Soporte de IEEE 802.1w RSTP
- Soporte de IEEE 802.1s MSTP
- Soporte de PVST+, Per VLAN STP
- Soporte de IEEE 802.3ad LACP.
- Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
- Soporte de LLDP-MED
- Soporte de Cisco Discovery Protocol (CDP) v1 y v2
- Soporte de IEEE 802.1ag Connectivity Fault Management
- Soporte del estándar Y.1731 Frame Delay
- Soporte de ITU G.8032 Ethernet Ring Protection Switching
- Soporte de PIM Snooping
- Soporte de Multicast VLAN Registration (MVR)
- Soporte de IEEE 802.1Q VLAN Tagging
- Soporte de IEEE 802.1v
- Soporte de VLANs basadas por Puerto, MAC y Protocolo
- Contar con la capacidad de trasladar los tags 802.1Q de varias VLANs al tag de una sola VLAN.
- Soporte de IEEE 802.1AK MVRP
- IEEE 802.1 Audio Video Bridging (AVB), este protocolo no es imprescindible incluirlo en la propuesta, sin embargo, el equipo ofertado

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 05 74 00 www.fonacot.gob.mx

deberá estar capacitado para soportarlo sin la necesidad de hardware adicional.

- Deberá de soportar un mecanismo de redundancia a nivel de capa 2, que permita un tiempo de recuperación en caso de caída o restauración de la red en menos de 1 segundo, garantizando disponibilidad y confiabilidad a la red para aplicaciones como voz y video. Este mecanismo deberá de trabajar al menos en topologías de anillo.
- Deberá de contar con un mecanismo correctivo de detección de Loops que permita tomar medidas de manera inmediata ante una falla en la red, diferente a Spanning Tree Protocol.
- Deberá contar con una funcionalidad que permita conjuntar o agregar puertos en al menos 2 switches de tal forma que dicho arreglo proporcione una sóla conexión lógica hacia otro dispositivo, en donde dicho dispositivo puede ser un servidor o algún otro dispositivo de red que puede ser configurado por medio de algún protocolo como LAG o similar.
- Soporte de Port Mirroring tanto local como remoto
- Funcionalidades de Clasificación de Tráfico y Calidad de Servicio
- Contar con al menos 8 colas (queues) por puerto y soportar los siguientes algoritmos de encolamiento: Weigthed Fair Queuing, Round Robin Priority y Strict Priority Queuing
- Calidad de servicio aplicable a tráfico por clasificación de acuerdo a los siguientes criterios: VLAN ID, dirección MAC, dirección IP, puerto TCP/UDP, 802.1p, DiffServ
- Soportar un rate-limiting con una granularidad de 8 kbps tanto de ingreso como de egreso
- Soporte de rate shaping
- Funcionalidades de Capa 3
- Soporte IGMP v1/v2/v3
- Ruteo estático unicast y multicast para IPv4
- Deberá soportar al menos 15,000 entradas de IPv4
- Soporte de CIDR
- Soporte de ECMP
- Soporte de VRRPv2
- Soporte de BOOTP/DHCP relay agent y DHCP server
- Soporte de RIPv1 y RIPV2
- Soporte de OSPFv2
- Soporte de Autenticación MD5 para OSPF
- Soporte de PIM-SM, PIM-SSM
- Soporte de Policy Based Routing para IPv4 e IPv6
- Soporte de Virtual Routers, al menos 48
- Soporte de VRFs
- Soporte de ruteo estático unicast para IPv6
- Soporte de RIPng
- Soporte de MLDv1/v2
- Soporte de ICMP sobre IPv6

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

- Soporte de Traceroute sobre IPv6
- Soporte de Telnet sobre IPv6
- Soporte de SSHv2 sobre IPv6
- Soporte de las siguientes especificaciones para IPv6:
  - RFC 2460 - Internet Protocol,Version 6 (IPv6) Specification
  - RFC 4861 - Neighbor Discovery for IP Version 6
  - RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks
  - RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture
  - RFC 5722 - Handling of Overlapping IPv6
  - RFC 2462 - IPv6 Stateless Address Auto Configuration – Router Requirements
  - RFC 2740 OSPF v3 for IPv6 Seguridad
- El equipo debe contar con protección para contra ataques DoS y man-in-the-middle
- El sistema operativo del equipo debe soportar CLI Scripting, que permita automatizar configuraciones, tales como QoS, ACLs, etc.
- El equipo debe soportar múltiples suplicantes por puerto, y múltiples métodos de autenticación: 802.1x, MAC y Web
- El equipo debe ser capaz de permitir el acceso a la red de los usuarios, a través de autenticación y Kerberos snooping.
- Debe contar con la funcionalidad de aplicar políticas de seguridad (perfiles), con base al rol que tenga el usuario de la red en la organización, y debe contar con las siguientes características:
- La creación de roles o perfiles deberá ajustarse a las necesidades del negocio, de tal modo que cada uno cuente con los privilegios específicos para el acceso de los recursos de red y de aplicativos.
- El rol o perfil debe ser asignado por usuario y este debe prevalecer incluso si se mueve de puerto.
- El rol o perfil puede ser asignado de forma dinámica por medio de mecanismos de autenticación RADIUS con base en lo siguiente:
  - Por atributos que la propia arquitectura defina tales como campos Filter-ID o VSA.
  - Soporte del estándar RFC 3580 por medio de atributos VLAN Tunnels,
  - Soportar un modo mixto o híbrido, de acuerdo a los dos esquemas antes solicitados.
- La funcionalidad de políticas o perfiles de seguridad debe contar con al menos las siguientes capacidades:
  - 60 Periles o Roles por Switch
  - 800 Reglas por cada perfil o rol por Switch
  - 128 usuarios autenticados por Puerto
  - 512 usuarios por Switch
- La funcionalidad de políticas o perfiles de seguridad debe ser capaz de clasificar o identificar el tráfico por los siguientes criterios de capa 2/3/4:

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 06 74 00 www.fonacot.gob.mx

- Por identificación del campo Type de tramas Ethernet II
- Dirección MAC origen/destino
- Dirección IP origen/destino
- Dirección IPX origen/destino
- Socket IPX origen/destino
- Por el campo de tipo de servicio (Type of Service) en los paquetes IP
- Puerto UDP y TCP origen/destino
- Puerto UDP y TCP origen/destino
- Por tipo de ICMP
- Por tipo de Protocolo IP
- Por identificador del puerto físico del equipo
- Por el TAG de la VLAN

- La funcionalidad de políticas o perfiles de seguridad debe de contar con al menos las siguientes acciones a ejecutar:
  - Asignación de VLAN
  - Filtrado de tráfico (Permitir/Negar)
  - Asignación de Rate-Limiting
  - Rate Shaping
  - Priorización del tráfico
  - Manipulación y reescritura del campo TCI
- Deberá contar con un mecanismo de seguridad que permita detectar amenazas y reaccionar ante la intrusión de la red. Esto basado en modelo de alertas basadas en el traspaso de umbrales definidos por el administrador de la red.
- Deberá contar con herramientas que permitan rastrear a los usuarios de la red y proporcionar información tal como: el switch al que se conecta el usuario, el puerto físico de conexión, la MAC address, la VLAN de trabajo e identidad del usuario.
- El equipo deberá de soportar aprovisionamiento automático a través de perfiles, basados en eventos como el logging o logoff de un usuario, hora del día por medio del uso de scripts o LLDP, permitiendo configurar los parámetros necesarios de manera automática en el puerto para soluciones de telefonía IP, videoconferencia, video vigilancia, autenticación de usuarios.
- Deberá de contar con un mecanismo que permita soportar la migración de máquinas virtuales, configuración de su puerto e inventario de manera automática, el equipo deberá de ser capaz de identificar la máquina virtual a través de su dirección MAC y autenticar la conexión a la red, aplicar la configuración al puerto autenticado y remover la configuración del puerto en donde la máquina virtual ha sido removida, así como de las políticas que se le hayan aplicado a la misma, sin necesidad de reconfigurar los equipos de la red.
- Deberá de contar con un mecanismo de notificaciones de eventos a través de XML, como un cambio en la configuración, cambio de estado, o cualquier evento deseado que quiera ser reportado, a través de un

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

servidor Web externo, esto con la finalidad de alinear la estrategia de las mejores prácticas de TI y contar con una bitácora precisa de los cambios y eventos ocurridos en la red.

- Soporte de las siguientes especificaciones:
  - RFC 1492 TACACS+
  - RFC 1866 HTML
  - RFC 3580 IEEE 802.1x RADIUS
  - RFC 3579 RADIUS EAP
  - RFC 2866 RADIUS Accounting
  - RFC 2865 RADIUS Authentication
  - RFC 4668 RADIUS Authentication Client MIB for IPv6
  - RFC 4670 RADIUS Accounting Client MIB for Ipv6
- Soporte de Listas de Control de Acceso (ACLs) en capas 2/3/4 y Wire-Speed
- Manejo de Guest VLAN para 802.1x
- Soporte de SSL/TLS
- Soporte de mecanismos para la limitar el número de direcciones MAC determinadas por puerto.
- Soporte de mecanismo para prevenir que dispositivos no autorizados tengan acceso a la red basados en su dirección MAC, garantizando sólo aquellos que estén debidamente registrados o asociados a los puertos.
- Soporte de DHCP Snooping o Trusted DHCP Server
- Soporte de Dynamic ARP Inspection o ARP Validation
- Soporte de MD5 para protocolos de enrutamientoistración
- Debe contar un esquema de protección de memoria para cada aplicación, para que se manejen como procesos separados; el sistema operativo deberá ser modular y contar con funciones de monitoreo y reinicio de procesos sin la necesidad de reiniciar el equipo completamente.
- Contar con APIs XML para integración con terceros.
- Contar con la capacidad de soportar scripts CLI a través de lenguajes de programación como Python.
- Soporte de Telnet en modalidad cliente y servidor
- Soporte de SSH2 en modalidad cliente y servidor
- Soporte de SCP en modalidad cliente y servidor
- Soporte de SFTP en modalidad servidor
- Soporte de TFTP
- Soporte de Syslog para envío de al menos para 4 servidores
- Soporte de las siguientes especificaciones:
  - RFC 1650 Ethernet-Like MIB
  - RFC 1901 – 1908 SNMPv2c, SMIv2 and Revised MIB-II
  - RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management Framework
  - RFC 1155 Structure of Management Information (SMIv1)
  - RFC 5905 1 – Network Time Protocol v4
  - RFC 2030 – SNTP, Simple Network Time Protocol v4

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 65 74 00 www.fonacot.gob.mx

  - RFC 2613 SMON MIB
  - RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- Soporte de SNMPv1/v2/v3
- Soporte de gestión vía HTTP y HTTPS
- 4 Grupos de RMON
- Soportar la funcionalidad de muestreo mediante el protocolo sFlow v5 o IPFIX
- Soporte de DDMI
- Manejo de múltiples archivos de configuración
- Manejo de múltiples imágenes de firmware o Sistema operativo
- Soportar la funcionalidad de especificar un periodo de inactividad en las cuentas de administrador local después de haber sido bloqueada por intentos fallidos de la misma y tener la capacidad de habilitarse automáticamente al haber transcurrido el periodo especificado.
- Soportar la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula
  - Letra minúscula
  - Numero
  - Caracteres especiales
- Soportar la funcionalidad de prevenir que un usuario administrador local pueda emplear un password que anteriormente empleó y ya ha caducado.
- Funcionalidad para configurar un modelo de Redes Definidas por Software (SDN) mediante la especificación de estándar abierto OpenFlow 1.0, con el cual desde un Sistema Controlador se manipulen los flujos de datos usando protocolos estándares para que de forma dinámica se configuren las tablas de flujos, esto con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Deberá de contar con la capacidad de manejar comunicación FCoE, iSCI via Data Center Bridging IEEE P802.1Qaz
- Deberá soportar la especificación IEEE VEPA – Direct Attach
- Especificaciones a cumplir y Condiciones de Operación
- Rango de Temperatura de Operación: 0°C - 48°C
- Humedad en condiciones operativas: 10 – 95 % Humedad relativa no condensada
- Altura en condiciones operativas: 0 – 4500 m
- UL 60950-1
- FCC 21CFR 1040.10 (U.S. Laser Safety)
- EN 60825-1+A2:2001 (Lasers Safety)
- FCC CFR 47 part 15 Class A (USA)
- EN 55022:2006+A1:2007 Class A
- EN 61000-3-2 (Harmonics)

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- EN 61000-3-3 2008 (Flicker)
- CISPR 22: 2006 (International Emissions)
- CISPR 24:A2:2003 Class A (International Immunity)
- IEC 61000-4-5:2005
- EN 61000-4-5:2006
- IEC/EN 61000-4-11:2004
- ETSI EN 300 386:2001
- VCCI Class A
- ETSI EN 300 019

2.3.3.5. Switch de acceso Tipo 5

Características Generales

- Switch apilable con desempeño mínimo de 212 Gbps y 157 Mpps con arquitectura no bloqueable, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad.
- El equipo debe contar con al menos la siguiente densidad de puertos:
  - 24 puertos 10/100/1000 BASE-T
  - 2 Puertos de apilamiento dedicado.
  - 1 puerto serial
  - 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda
  - 1 puerto USB para almacenamiento externo
- El equipo deberá soportar el siguiente tipo de interfaces:
  - Gigabit Ethernet: SX, LX, ZX, BX-D, BX-U, 100FX/1000LX, 10/100/1000BASE-T en formato SFP
  - 10 Gigabit Ethernet: SR, LR, ER, LRM y CR en formato SFP+
- Deberá contar con un procesador de 64-bits a 1GHz y al menos 1GB en RAM
- Soporte de los siguientes estándares:
  - IEEE 802.3af / at
  - IEEE 802.3az
- El equipo debe soportar fuentes redundantes.
- El equipo deberá estar diseñado para una altura no mayor a una unidad de rack (1 RU)
- El equipo debe tener una latencia menor a 5 micro segundos
- Soportar al menos 32,000 MAC Address
- Soportar al menos 4094 VLANs
- Soporte de Jumbo Frames
- El equipo debe ser capaz de soportar apilamiento con un ancho de banda de al menos 80 Gbps
- Soporte de apilamiento de hasta 8 unidades
- Deberá tener la capacidad de apilarse con switches de la misma familia de productos aunque sea otro modelo de menor o mayor capacidadades de Capa 2, Switching

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 05 75 00 www.fonacot.gob.mx

- El equipo deberá soportar al menos las siguientes funcionalidades y especificaciones:
  - Soporte de IEEE 802.1D STP
  - Soporte de IEEE 802.1w RSTP
  - Soporte de IEEE 802.1s MSTP
  - Soporte de PVST+, Per VLAN STP
  - Soporte de IEEE 802.3ad LACP, con la capacidad de al menos 120 grupos de agregación cuyo máximo sea de al menos 30 puertos por cada cada grupo.
  - Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
  - Soporte de LLDP-MED
  - Soporte de Cisco Discovery Protocol (CDP) v1 y v2
  - Soporte de IEEE 802.1ag Connectivity Fault Management
  - Soporte del estándar Y.1731 Frame Delay
  - Soporte de ITU G.8032 Ethernet Ring Protection Switching
  - Soporte de PIM Snooping
  - Soporte de Multicast VLAN Registration (MVR)
  - Soporte de IEEE 802.1Q VLAN Tagging
  - Soporte de IEEE 802.1v
  - Soporte de VLANs basadas por Puerto, MAC y Protocolo
  - Contar con la capacidad de trasladar los tags 802.1Q de varias VLANs al tag de una sola VLAN.
  - Soporte de IEEE 802.1AK MVRP
- Deberá de soportar un mecanismo de redundancia a nivel de capa 2, que permita un tiempo de recuperación en caso de caída o restauración de la red en menos de 1 segundo, garantizando disponibilidad y confiabilidad a la red para aplicaciones como voz y video. Este mecanismo deberá de trabajar al menos en topologías de anillo.
- Deberá de contar con un mecanismo correctivo de detección de Loops que permita tomar medidas de manera inmediata ante una falla en la red, diferente a Spanning Tree Protocol.
- Deberá contar con una funcionalidad que permita conjuntar o agregar puertos en al menos 2 switches de tal forma que dicho arreglo proporcione una sóla conexión lógica hacia otro dispositivo, en donde dicho dispositivo puede ser un servidor o algún otro dispositivo de red que puede ser configurado por medio de algún protocolo como LAG o similar.
- Soporte de Port Mirroring tanto local como remoto
- Soportar al menos 120 filtros por puerto espejo, permitiendo una mayor granularidad en el tipo de información que se necesite monitorear.
- Contar con al menos 8 colas (queues) por puerto y soportar los siguientes algoritmos de encolamiento: Weigthed Fair Queuing, Round Robin Priority y Strict Priority Queuing
- Calidad de servicio aplicable a tráfico por clasificación de acuerdo a los siguientes criterios: VLAN ID, dirección MAC, dirección IP, puerto TCP/UDP, 802.1p, DiffServ

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Soportar un rate-limiting con una granularidad de 8 kbps tanto de ingreso como de egreso
- Soporte de rate shapingnalidades de Capa 3
- Soporte IGMP v1/v2/v3
- Ruteo estático unicast y multicast para IPv4
- Deberá soportar al menos 15,000 entradas de IPv4
- Soporte de IP Route Compression
- Soporte de CIDR
- Soporte de ECMP
- Soporte de VRRPv2
- Soporte de BOOTP/DHCP relay agent y DHCP server
- Soporte de RIPv1 y RIPV2
- Soporte de OSPFv2
- Soporte de Autenticación MD5 para OSPF
- Soporte de PIM-SM, PIM-SSM
- Soporte de Policy Based Routing para IPv4 e IPv6
- Soportar al menos 8,000 entradas en IPv6
- Soporte de Virtual Routers, al menos 48
- Soporte de VRFs
- Soporte de ruteo estático unicast para IPv6
- Soporte de RIPng
- Soporte de MLDv1/v2
- Soporte de ICMP sobre IPv6
- Soporte de Traceroute sobre IPv6
- Soporte de Telnet sobre IPv6
- Soporte de SSHv2 sobre IPv6
- Soporte de las siguientes especificaciones para IPv6:
  - RFC 2460 - Internet Protocol,Version 6 (IPv6) Specification
  - RFC 4861 - Neighbor Discovery for IP Version 6
  - RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks
  - RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture
  - RFC 5722 - Handling of Overlapping IPv6
  - RFC 2462 - IPv6 Stateless Address Auto Configuration – Router Requirements
  - RFC 2740 OSPF v3 for IPv6
- El equipo debe contar con protección para contra ataques DoS y man-in-the-middle
- El sistema operativo del equipo debe soportar CLI Scripting, que permita automatizar configuraciones, tales como QoS, ACLs, etc.
- El equipo debe soportar múltiples suplicantes por puerto, y múltiples métodos de autenticación: 802.1x, MAC y Web
- El equipo debe ser capaz de permitir el acceso a la red de los usuarios, a través de autenticación y Kerberos snooping.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Debe contar con la funcionalidad de aplicar políticas de seguridad (perfiles), con base al rol que tenga el usuario de la red en la organización, y debe contar con las siguientes características:
- La creación de roles o perfiles deberá ajustarse a las necesidades del negocio, de tal modo que cada uno cuente con los privilegios específicos para el acceso de los recursos de red y de aplicativos.
- El rol o perfil debe ser asignado por usuario y este debe prevalecer incluso si se mueve de puerto.
- El rol o perfil puede ser asignado de forma dinámica por medio de mecanismos de autenticación RADIUS con base en lo siguiente:
- Por atributos que la propia arquitectura defina tales como campos Filter-ID o VSA.
- Soporte del estándar RFC 3580 por medio de atributos VLAN Tunnels,
- Soportar un modo mixto o híbrido, de acuerdo a los dos esquemas antes solicitados.
- La funcionalidad de políticas o perfiles de seguridad debe contar con al menos las siguientes capacidades:
  - 60 Periles o Roles por Switch
  - 800 Reglas por cada perfil o rol por Switch
  - 128 usuarios autenticados por Puerto
  - 512 usuarios por Switch
- La funcionalidad de políticas o perfiles de seguridad debe ser capaz de clasificar o identificar el tráfico por los siguientes criterios de capa 2/3/4:
  - Por identificación del campo Type de tramas Ethernet II
  - Dirección MAC origen/destino
  - Dirección IP origen/destino
  - Dirección IPX origen/destino
  - Socket IPX origen/destino
  - Por el campo de tipo de servicio (Type of Service) en los paquetes IP
  - Puerto UDP y TCP origen/destino
  - Puerto UDP y TCP origen/destino
  - Por tipo de ICMP
  - Por tipo de Protocolo IP
  - Por identificador del puerto físico del equipo
  - Por el TAG de la VLAN
- La funcionalidad de políticas o perfiles de seguridad debe de contar con al menos las siguientes acciones a ejecutar:
  - Asignación de VLAN
  - Filtrado de tráfico (Permitir/Negar)
  - Asignación de Rate-Limiting
  - Rate Shaping
  - Priorización del tráfico
  - Manipulación y reescritura del campo TCI
- Deberá contar con un mecanismo de seguridad que permita detectar amenazas y reaccionar ante la intrusión de la red. Esto basado en modelo

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 5.2 65 74 00 www.fonacot.gob.mx

de alertas basadas en el traspaso de umbrales definidos por el administrador de la red.

- Deberá contar con herramientas que permitan rastrear a los usuarios de la red y proporcionar información tal como: el switch al que se conecta el usuario, el puerto físico de conexión, la MAC address, la VLAN de trabajo e identidad del usuario.
- El equipo deberá de soportar aprovisionamiento automático a través de perfiles, basados en eventos como el logging o logoff de un usuario, hora del día por medio del uso de scripts o LLDP, permitiendo configurar los parámetros necesarios de manera automática en el puerto para soluciones de telefonía IP, videoconferencia, video vigilancia, autenticación de usuarios.
- Deberá de contar con un mecanismo que permita soportar la migración de máquinas virtuales, configuración de su puerto e inventario de manera automática, el equipo deberá de ser capaz de identificar la máquina virtual a través de su dirección MAC y autenticar la conexión a la red, aplicar la configuración al puerto autenticado y remover la configuración del puerto en donde la máquina virtual ha sido removida, así como de las políticas que se le hayan aplicado a la misma, sin necesidad de reconfigurar los equipos de la red.
- Deberá de contar con un mecanismo de notificaciones de eventos a través de XML, como un cambio en la configuración, cambio de estado, o cualquier evento deseado que quiera ser reportado, a través de un servidor Web externo, esto con la finalidad de alinear la estrategia de las mejores prácticas de TI y contar con una bitácora precisa de los cambios y eventos ocurridos en la red.
- Soporte de las siguientes especificaciones:
  - RFC 1492 TACACS+
  - RFC 1866 HTML
  - RFC 3580 IEEE 802.1x RADIUS
  - RFC 3579 RADIUS EAP
  - RFC 2866 RADIUS Accounting
  - RFC 2865 RADIUS Authentication
  - RFC 4668 RADIUS Authentication Client MIB for IPv6
  - RFC 4670 RADIUS Accounting Client MIB for Ipv6
- Soporte de Listas de Control de Acceso (ACLs) en capas 2/3/4 y Wire-Speed
- Deberá de soportar al menos 4,000 listas de control de acceso para garantizar la seguridad de la red.
- Manejo de Guest VLAN para 802.1x
- Soporte de SSL/TLS
- Soporte de mecanismos para la limitar el número de direcciones MAC determinadas por puerto.
- Soporte de mecanismo para prevenir que dispositivos no autorizados tengan acceso a la red basados en su dirección MAC, garantizando sólo aquellos que estén debidamente registrados o asociados a los puertos.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 5511 52 65 74 00 www.fonacot.gob.mx

- Soporte de DHCP Snooping o Trusted DHCP Server
- Soporte de Dynamic ARP Inspection o ARP Validation
- Soporte de MD5 para protocolos de enrutamiento
- Funcionalidades de Administración
- Debe contar un esquema de protección de memoria para cada aplicación, para que se manejen como procesos separados; el sistema operativo deberá ser modular y contar con funciones de monitoreo y reinicio de procesos sin la necesidad de reiniciar el equipo completamente.
- Contar con APIs XML para integración con terceros.
- Contar con la capacidad de soportar scripts CLI a través de lenguajes de programación como Python.
- Soporte de Telnet en modalidad cliente y servidor
- Soporte de SSH2 en modalidad cliente y servidor
- Soporte de SCP en modalidad cliente y servidor
- Soporte de SFTP en modalidad servidor
- Soporte de TFTP
- Soporte de Syslog para envío de al menos para 4 servidores
- Soporte de las siguientes especificaciones:
  - RFC 1650 Ethernet-Like MIB
  - RFC 1901 – 1908 SNMPv2c, SMIv2 and Revised MIB-II
  - RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management Framework
  - RFC 1155 Structure of Management Information (SMIv1)
  - RFC 5905 1 – Network Time Protocol v4
  - RFC 2030 – SNTP, Simple Network Time Protocol v4
  - RFC 2613 SMON MIB
  - RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- Soporte de SNMPv1/v2/v3
- Soporte de gestión vía HTTP y HTTPS
- 4 Grupos de RMON
- Soportar la funcionalidad de muestreo mediante el protocolo sFlow v5 o IPFIX
- Soporte de DDMI
- Manejo de múltiples archivos de configuración
- Manejo de múltiples imágenes de firmware o Sistema operativo
- Soportar la funcionalidad de especificar un periodo de inactividad en las cuentas de administrador local después de haber sido bloqueada por intentos fallidos de la misma y tener la capacidad de habilitarse automáticamente al haber transcurrido el periodo especificado.
- Soportar la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

  - Letra minúscula
  - Numero
  - Caracteres especiales
  - Soportar la funcionalidad de prevenir que un usuario administrador local pueda emplear un password que anteriormente empleó y ya ha caducado.
  - Funcionalidades Especiales
- Soportar SDN OpenStack, con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Funcionalidad para configurar un modelo de Redes Definidas por Software (SDN) mediante la especificación de estándar abierto OpenFlow, con el cual desde un Sistema Controlador se manipulen los flujos de datos usando protocolos estándares para que de forma dinámica se configuren las tablas de flujos, esto con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Deberá de contar con la capacidad de manejar comunicación FCoE, iSCI via Data Center Bridging IEEE P802.1Qaz
- Deberá soportar la especificación IEEE VEPA – Direct Attach
- Especificaciones a cumplir y Condiciones de Operación
- Rango de Temperatura de Operación: 0°C - 48°C
- Humedad en condiciones operativas: 10 – 95 % Humedad relativa no condensada
- Altura en condiciones operativas: 0 – 4500 m
- UL 60950-1
- FCC 21CFR 1040.10 (U.S. Laser Safety)
- EN 60825-1+A2:2001 (Lasers Safety)
- FCC CFR 47 part 15 Class A (USA)
- EN 55022:2006+A1:2007 Class A
- EN 61000-3-2 (Harmonics)
- EN 61000-3-3 2008 (Flicker)
- CISPR 22: 2006 (International Emissions)
- CISPR 24:A2:2003 Class A (International Immunity)
- IEC 61000-4-5:2005
- EN 61000-4-5:2006
- IEC/EN 61000-4-11:2004
- ETSI EN 300 386:2001
- VCCI Class A
- ETSI EN 300 019

Los switches de acceso deberán distribuirse conforme a la siguiente tabla, mismas que podrán variar según las necesidades del Instituto.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 55 52 65 73 00 www.fonacot.gob.mx

Sede	Ubicación	Switch de Acceso	Cantidad
Oficinas centrales (Insurgentes)	Piso 1	Tipo 1	1
	Piso 2	Tipo 1	1
	Piso 3	Tipo 1	1
	Piso 4	Tipo 1	1
	Piso 5	Tipo 1	1
	Centro de Datos 1	Tipo 1	1
	Centro de Datos 2	Tipo 1	1
	DMZ	Tipo 5	1
	Monitores	Tipo 5	1
Plaza de la Republica	Mezzanine	Tipo 2	2
		Tipo 4	1
	Piso 1	Tipo 2	1
	Piso 2	Tipo 2	1
	Piso 3	Tipo 2	1
	Piso 5	Tipo 2	1
		Tipo 3	1
	Piso 6	Tipo 2	1
	Piso 7	Tipo 2	1
		Tipo 3	1
	Piso 8	Tipo 2	1
		Tipo 3	1
	Piso 9	Tipo 2	1
		Tipo 3	1
Acapulco	Ubicación Única	Tipo 4	1
Aguascalientes	Ubicación Única	Tipo 4	1
Almacen Mar Adriatico	Ubicación Única	Tipo 5	1
Campeche	Ubicación Única	Tipo 4	1
Cancun	Ubicación Única	Tipo 4	1
Cd Acuña	Ubicación Única	Tipo 5	1
Cd del Carmen	Ubicación Única	Tipo 5	1
Cd juarez	Ubicación Única	Tipo 4	1
Cd Obregon	Ubicación Única	Tipo 4	1
Cd Valles	Ubicación Única	Tipo 5	1
Cd Victoria	Ubicación Única	Tipo 5	1
Celaya	Ubicación Única	Tipo 5	1
Chetumal	Ubicación Única	Tipo 5	1

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

Chihuahua	Ubicación Única	Tipo 4	1
		Tipo 4	1
Chilpancingo	Ubicación Única	Tipo 5	1
Coatzacoalcos	Ubicación Única	Tipo 5	1
Colima	Ubicación Única	Tipo 4	1
Congreso del Trabajo	Ubicación Única	No Requerido	0
Cordoba	Ubicación Única	Tipo 5	1
Cozumel	Ubicación Única	Tipo 5	1
Cuautitlan	Ubicación Única	Tipo 5	1
Cuautla	Ubicación Única	Tipo 5	1
Cuernavaca	Ubicación Única	Tipo 4	1
Culiacan	Ubicación Única	Tipo 4	1
Delicias	Ubicación Única	Tipo 5	1
Durango	Ubicación Única	Tipo 4	1
Ecatepec	Ubicación Única	Tipo 5	1
Empalme	Ubicación Única	Tipo 5	1
Ensenada	Ubicación Única	Tipo 5	1
Fresnillo	Ubicación Única	Tipo 5	1
Guadalajara Abastos	Ubicación Única	Tipo 4	1
Guadalajara Federalismo	Ubicación Única	No Requerido	0
Hermosillo	Ubicación Única	No Requerido	0
Irapuato	Ubicación Única	Tipo 4	1
La Paz	Ubicación Única	Tipo 4	1
Lazaro Cardenas	Ubicación Única	Tipo 5	1
Leon	Ubicación Única	Tipo 4	1
Los Mochis	Ubicación Única	Tipo 5	1
Manzanillo	Ubicación Única	Tipo 5	1
Matamoros	Ubicación Única	Tipo 5	1
Mazatlan	Ubicación Única	Tipo 4	1
Merida	Ubicación Única	Tipo 4	1
Metro 6	Ubicación Única	Tipo 4	1
Mexicali	Ubicación Única	Tipo 4	1
Monclova	Ubicación Única	Tipo 5	1
Monterrey	Ubicación Única	No Requerido	0
Monterrey 2	Ubicación Única	Tipo 5	1
Morelia	Ubicación Única	Tipo 4	1
Nogales	Ubicación Única	No Requerido	0
Oaxaca	Ubicación Única	Tipo 4	1

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

Pachuca	Ubicación Única	Tipo 4	1
Piedras Negras	Ubicación Única	Tipo 5	1
Playa del Carmen	Ubicación Única	Tipo 5	1
Portales	Ubicación Única	Tipo 5	1
		Tipo 4	1
Puebla	Ubicación Única	Tipo 4	1
Puerto Vallarta	Ubicación Única	Tipo 4	1
Queretaro	Ubicación Única	Tipo 4	1
Reynosa	Ubicación Única	Tipo 5	1
Saltillo	Ubicación Única	Tipo 4	1
San Jose del Cabo	Ubicación Única	Tipo 5	1
San Juan del Rio	Ubicación Única	Tipo 5	1
Sineif	Ubicación Única	Tipo 5	1
San Luis Potosi	Ubicación Única	Tipo 4	1
Molinos	Ubicación Única	No Requerido	0
Tampico	Ubicación Única	Tipo 4	1
Tapachula	Ubicación Única	Tipo 5	1
Tehuacan	Ubicación Única	Tipo 5	1
Tepic	Ubicación Única	Tipo 4	1
Texcoco	Ubicación Única	Tipo 5	1
Tijuana	Ubicación Única	Tipo 4	1
Tlalnepantla	Ubicación Única	Tipo 4	1
		No Requerido	0
Tlaxcala	Ubicación Única	Tipo 4	1
Toluca	Ubicación Única	Tipo 4	1
Torreon	Ubicación Única	Tipo 4	1
Tuxtepec	Ubicación Única	Tipo 5	1
Tuxtla	Ubicación Única	Tipo 4	1
Uruapan	Ubicación Única	Tipo 5	1
Vallejo	Ubicación Única	No Requerido	0
Veracruz	Ubicación Única	Tipo 4	1
Villahermosa	Ubicación Única	Tipo 4	1
Xalapa	Ubicación Única	No Requerido	0
Zacatecas	Ubicación Única	Tipo 4	1
Zamora	Ubicación Única	Tipo 5	1
Zaragoza	Ubicación Única	Tipo 4	1
		No Requerido	0
Lerma	Ubicación Única	Tipo 5	1

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

2.3.4. Red Inalámbrica

El LICITANTE ganador deberá realizar la implementacion, operación, administración y puesta a punto del servicio de red inalámbrica en las oficinas del Instituto FONACOT, basado en puntos de acceso administrados mediante una controladora.

2.3.4.1. Servicio de red inalámbrica en Edificios Sede.

El servicio consiste en implementar un esquema de red inalámbrica que provea cobertura al 100% de las áreas operativas en los edificios sede del instituto Fonacot: Oficinas Centrales (Sede Insurgentes) y Plaza de la Republica.
La infraestructura que conforme el servicio de red inalámbrica en edificios sede propuesto por el LICITANTE, deberá cumplir con al menos las siguientes características tecnicas:

- Soportar el tratamiento del tráfico en los siguientes esquemas:
  - Centralizado en la Controladora
  - Procesado en cada Punto de Acceso
  - Combinación entre Centralizado en la Controladora y en el Punto de Acceso
- Soportar el protocolo CAPWAP
- Soportar el estándar IEEE 802.1D
- Soportar el estándar IEEE 802.1Q
- Soportar la funcionalidad Proxy ARP
- Soportar e incluir un esquema de ruteo dinámico OSPF sin que esto implique el uso de una licencia adicional.
- Soportar las siguientes acciones para QoS:
  - Rate limit de entrada / salida
  - Prioridad 802.1p
  - Asignar cola de transmisión (queue)
  - Remarcado de paquetes en ToS/DSCP
- Proporcionar un servicio local de DHCP con los siguientes parámetros configurables:
  - Dominio
  - Lease
  - Next Hop o Gateway
  - DNS server
  - WINS server
  - DLS DHCP
- Tener la capacidad para detectar e identificar la interferencia proveniente de otros dispositivos RF de tipo: microondas, bluetooth, bridges de video, etc. para que de forma automática se puedan redirigir las conexiones de clientes a canales más limpios o libres de interferencia.
- Emplear los métodos Packet fairness y Airtime fairness para proporcionar QoS.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Soportar la funcionalidad denominada como Wireless Distribution System (WDS) y cumplir con los siguientes mecanismos:
- Tener la capacidad de formar un entrelazamiento inalámbrico entre Puntos de Acceso para formar una malla con trayectorias redundantes, con la finalidad de extender la cobertura en sitios en donde los Puntos de Acceso no puedan ser cableados.
- Poseer la funcionalidad de unir segmentos de redes alámbricas.
- Capacidad para que los Puntos de Acceso que funcionen como extensión o repetidores puedan también propagar al mismo tiempo el(los) SSID(s) requerido(s).
- Soportar un esquema de Alta Disponibilidad donde las Controladoras operen en modo Activo-Activo, sin necesidad de adquirir licencias o software adicionales para lograr dicha función.
- Contener tráfico de Bonjour y multicast, para evitar la introducción de tráfico no requerido y optimizar la operación de red
- Distribución de cargas entre varios Puntos de Acceso adyacentes para prevenir sobre carga de usuarios.
- Soportar la funcionalidad de Location-based Services e integrarse con herramientas como Aeroscout y Ekahau.
- Poseer la funcionalidad de sincronizarse por medio del protocolo NTP, así como emplear el reloj propio de sistema
- Poder integrar Puntos de Acceso de otras marcas, para brindar servicio y seguridad mediante autenticación de usuarios.
- Para esquemas de alta disponibilidad del servicio, deberá contar con la funcionalidad de permitir nuevas sesiones 802.1x aun cuando la comunicación entre la controladora y el Punto de Acceso este interrumpida.

Funciones de Seguridad

- Permitir el filtrado de direcciones MAC para negar o permitir el acceso a los servicios, las direcciones MAC podrán darse de alta de forma individual e importando un archivo.
- Disociación de clientes en forma manual.
- Soportar los siguientes estándares de cifrado o encripcion:
  - WEP
  - TKIP
  - WPA
  - WPA2
  - WPA-PSK
  - WPA2-PSK
  - AES (CCMP)
  - RC4-40, 104, 128-bit
- Interactuar con servidores de RADIUS con el objetivo de definir perfiles de acceso, basados en atributos como Filter-ID
- Soportar los siguientes métodos de autenticación:
- MAC

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Web o Captive Portal
- IEEE 802.1x
- Soportar RFC 3580
- Soportar la funcionalidad de portal cautivo para autenticación con las siguientes características:
- Autenticación 802.1X
- Uso de Portal cautivo interno
- Uso Portal cautivo externo
- Portal de Invitados con acceso temporal
- Personalización tanto para el portal interno como para el de invitados, de acuerdo a los patrones gráficos y logos requeridos por el Instituto FONACOT.
- El portal Cautivo Interno podrá ser configurado para desplegarse en HTTP o HTTPS
- El portal Cautivo Interno deberá tener la capacidad para presentar diferentes atributos tales como el Número de serie del Punto de Acceso, SSID y MAC Address.
- Soportar los siguientes métodos de autenticación 802.1x:
  - EAP-TLS
  - EAP-MD5
  - EAP-FAST
  - EAP-SIM
  - EAP-TTLS
  - PEAP
- Capacidad para ocultar los SSID's configurados.
- Bloquear tráfico entre dispositivos asociados al mismo SSID
- Permitir una distinción de privilegios por el tipo de usuario dentro del mismo SSID, dichos privilegios deberán abarcar desde el filtrado de tráfico de capa 2, capa 3 y capa 4, de acuerdo a los siguientes criterios:
  - Source MAC address
  - Destination MAC address
  - IPv4 Source IP address
  - IPv4 Destination IP address
  - Source layer 4 port
  - Destination layer 4 port
  - IPv4 Source socket
  - IPv4 Destination socket
  - IP type
  - ICMP packet type and code
  - ToS/DSCP marking
  - 802.1p priority
  - Ethertype
- Limitar ancho de banda tanto a nivel de usuario como por tipo de tráfico, así como manejo de prioridades aplicando calidad de servicio a los mismos a nivel de capa 2 y capa 3.

Av. Insurgentes Sur 452 Col. Roma Sur, D.F. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

- Permitir filtrado de tráfico desde la Controladora y en los Puntos de Acceso de tal forma que este filtrado pueda radicar en los Puntos de Acceso, ya que en caso de un evento en el cual este pierda comunicación con la Controladora, el Punto de Acceso sea capaz de seguir soportando dicha aplicación de reglas.
- El filtrado de tráfico también deberá ser soportado para tráfico de Multicast
- Soportar la funcionalidad de actuar como WIDS/WIPS en base a los siguientes requerimientos:
- Detección y clasificación de Puntos de Acceso bajo diferentes categorías como Puntos de Accesos Vecinos o Externos, Autorizados, Ilegítimos o Prohibidos.
- Dicha detección deberá de informar datos de los Puntos de Acceso, tales como Dirección MAC, SSID y el Fabricante o Marca del equipo en cuestión.
- Proveer la funcionalidad de clasificar Puntos de Acceso no categorizados como Puntos de Acceso Vecinos o Externos en forma manual de ser requerido, o en su caso ser clasificados como Puntos de Acceso Ilegítimos.
- Capacidad para llevar a cabo la mitigación de amenazas basada en countermeasures que puedan trabajar por limitación de inundación de tramas, por envío de tramas que eviten a los dispositivos adjuntarse a dispositivos no permitidos y por agregación de dispositivos no permitidos a una lista negra.
- Capacidad para elegir los siguientes tipos de mitigación de amenazas o countermeasures:
  - Prevenir a dispositivos permitidos para hacer roaming sobre Puntos de Acceso no permitidos tales como Vecinos o Externos, Ilegítimos o Prohibidos.
  - Prevenir a los dispositivos en participar en redes de tipo Ad-Hoc.
  - Remover dispositivos que estén generando algún tipo de ataque de DoS.
  - Eliminar tramas responsables que generen un ataque de inundación de tráfico.
- Reconocimiento de las siguientes amenazas:
  - Conexiones Ad-Hoc
  - Cracking de llaves WPA-WEP
  - Aplicaciones de tipo surveillance como Netstumbler
  - Ataques de DoS
  - Puntos de Acceso tipo Honeypot
  - Detección de fuentes de interferencia como por ejemplo hornos de microondas o algún otro dispositivo que opere en la banda de los 2.4 GHz.
  - Puntos de Acceso tipo spoofing
- La funcionalidad WIDS/WIPS deberá proveer reportes con el siguiente tipo de información:
- Fecha y hora en de detección de amenaza

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 5241 65 74 00 www.fonacot.gob.mx

- MAC Address del dispositivo fuente
- Tipo de amenza y categoria
- Intensidad de señal de la fuente de amenza (dBm)
- Access Point que realiza medida de contención
- Tipo de medida aplicada
- Clientes enviados a Lista Negra
- Detección de Rogue APs por método closed loop alámbrico / inalámbrico para reducción de falsos positivos

Funcionalidades de Administración y Monitoreo

- Contará con un Dashboard que presente los principales eventos en forma textual, gráfica y estadística de la red inalámbrica:
- Estatus de Access Point
- Clientes
- Sesiones activas de administradores
- Access Point por canal
- Licenciamiento
- WLANs inseguras
- Access Point sin categorizar
- Amenazas activas
- Eventos
- Soportar la función para gestionar usuarios que administren el sistema con privilegios de lectura/escritura y solo lectura, ya sea por autenticación local o remota, así como un tipo de usuario administrador adicional que solo pueda tener los privilegios para gestionar las cuentas de invitados y esta sea la única función a la que tenga acceso.
- Soportar SNMP v2c/v3
- La controladora deberá soportar los siguientes esquemas de administración:
  - GUI o Web
  - CLI
  - Consola
- Soportar el backup y restore de Imagen de Controladora, por los siguientes medios:
  - FTP
  - Local
  - Flash
- La actualización del firmware de la Controladora podrá realizarse a través de GUI (Web) y por CLI
- Poseer una función de actualización de firmware y almacenamiento de imágenes de respaldo (snapshot), para recuperar la controladora en caso de que el proceso falle o bien la imagen se encuentre dañada o corrupta
- Tener la función de realizar respaldos de la configuración en forma manual o calendarizada y que estos puedan ser enviados en forma automática a

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

un servidor de almacenamiento por medio de un protocolo como FTP o SCP.

- Capacidad de envío de logs de acuerdo a su grado de severidad a un servidor Syslog, correspondientes a eventos de los Puntos de Acceso, Controladora, cambios de configuración y de los principales servicios proporcionados por la Controladora.
- Mostrar la siguiente información:
  - Puntos de Acceso Activos
  - Estadísticas WDS
  - Estadísticas de Balanceo de Cargas
  - Estadísticas de Alta Disponibilidad
  - Inventario de los Puntos de Acceso
- Mostrar la siguiente información con respecto a ruteo:
  - Forwarding Table
  - OSPF Linkstate
  - OSPF Neighbor
- Realizar un Inventario de los Puntos de Acceso que incluya:
  - Dirección IP/Máscara de Red/Gateway
  - Dirección MAC del Puerto Ethernet.
  - Versión de hardware y software
  - Antenas empleadas
  - Telnet or SSH (estado activo/inactivo)
  - DTIM period
  - Beacon Period
  - RTS Threshold
  - Canal(es) de Transmisión
  - Potencia de Transmisión (dB)
  - Rx Diversity
  - Tx Diversity
  - Preambulo (long, short)
  - 11n Channel Width
  - 11n Guard Interval
  - 11n Channel Bonding
- Herramientas de troubleshooting tales como PING, Traceroute, captura de paquetes en tiempo real.
- Proporcionar un histórico de sesiones de usuarios, conocido como Call Detail Records (CDR).

Como parte del servicio de Red Inalambrica, el LICITANTE ganador deberá realizar las siguientes actividades:

- Proveer todo lo necesario relacionado con hardware y software para la instalación y puesta a punto del esquema de alta disponibilidad de las controladoras con las que se administraran todos los Access Points que conformen el servicio de Red Inalámbrica.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Mantener a la última versión disponible la controladora y los Access Points (firmware) durante toda la vigencia del servicio.
- Realizar los cambios, ajustes y configuraciones necesarias, en los Access Points y en controladora.
- Administrar altas, bajas y cambios en los equipos y controladoras.
- Proveer cualquier accesorio, componente y/o material misceláneo necesario para la instalación y el funcionamiento de los Access Points y controladoras.
- Mantener operando correctamente el servicio de Red Inalámbrica durante toda la vigencia del servicio.
- Entregar reportes mensuales ó a solicitud del area técnica del Instituto FONACOT, relaiconados con el servicio de Red Inalámbrica, como, por ejemplo: velocidad promedio de usuarios, fallas, etc.
- A solicitud expresa del area tecnica, el LICITANTE ganador deberá realizar estudios de cobertura de red inalámbrica de cualquier sucursal del Instituto FONACOT. Los resultados de dicho estudio deberán permitir definir la infraestructura necesaria para implementar servicios de red inalámbrica adicionales, en estos casos, la infraestructura requerida se solicitará expresamente por el administrador del contrato bajo el concepto de Servicios Bajo Demanda.

2.3.4.2. Servicio de red inalámbrica en Localidades.

El servicio consiste en implementar un esquema de red inalámbrica que provea cobertura a las áreas operativas en las localidades del instituto Fonacot a nivel nacional. La infraestructura que conforme el servicio de red inalámbrica propuesto por el LICITANTE, deberá cumplir con al menos las siguientes características tecnicas:

- Soportar el tratamiento del tráfico en los siguientes esquemas:
  - Centralizado en la Controladora
  - Procesado en cada Punto de Acceso
  - Combinación entre Centralizado en la Controladora y en el Punto de Acceso
- Soportar el protocolo CAPWAP
- Soportar el estándar IEEE 802.1D
- Soportar el estándar IEEE 802.1Q
- Soportar la funcionalidad Proxy ARP
- Soportar e incluir un esquema de ruteo dinámico OSPF sin que esto implique el uso de una licencia adicional.
- Soportar las siguientes acciones para QoS:
  - Rate limit de entrada / salida
  - Prioridad 802.1p
  - Asignar cola de transmisión (queue)
  - Remarcado de paquetes en ToS/DSCP
- Proporcionar un servicio local de DHCP con los siguientes parámetros configurables:
  - Dominio

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 65 72 00 www.fonacot.gob.mx

- Lease
- Next Hop o Gateway
- DNS server
- WINS server
- DLS DHCP

- Tener la capacidad para detectar e identificar la interferencia proveniente de otros dispositivos RF de tipo: microondas, bluetooth, bridges de video, etc. para que de forma automática se puedan redirigir las conexiones de clientes a canales más limpios o libres de interferencia.
- Emplear los métodos Packet fairness y Airtime fairness para proporcionar QoS.
- Soportar la funcionalidad denominada como Wireless Distribution System (WDS) y cumplir con los siguientes mecanismos:
- Tener la capacidad de formar un entrelazamiento inalámbrico entre Puntos de Acceso para formar una malla con trayectorias redundantes, con la finalidad de extender la cobertura en sitios en donde los Puntos de Acceso no puedan ser cableados.
- Poseer la funcionalidad de unir segmentos de redes alámbricas.
- Capacidad para que los Puntos de Acceso que funcionen como extensión o repetidores puedan también propagar al mismo tiempo el(los) SSID(s) requerido(s).
- Soportar un esquema de Alta Disponibilidad donde las Controladoras operen en modo Activo-Activo, sin necesidad de adquirir licencias o software adicionales para lograr dicha función.
- Contener tráfico de Bonjour y multicast, para evitar la introducción de tráfico no requerido y optimizar la operación de red
- Distribución de cargas entre varios Puntos de Acceso adyacentes para prevenir sobre carga de usuarios.
- Soportar la funcionalidad de Location-based Services e integrarse con herramientas como Aeroscout y Ekahau.
- Poseer la funcionalidad de sincronizarse por medio del protocolo NTP, así como emplear el reloj propio de sistema
- Poder integrar Puntos de Acceso de otras marcas, para brindar servicio y seguridad mediante autenticación de usuarios.
- Para esquemas de alta disponibilidad del servicio, deberá contar con la funcionalidad de permitir nuevas sesiones 802.1x aun cuando la comunicación entre la controladora y el Punto de Acceso este interrumpida.

Funciones de Seguridad

- Permitir el filtrado de direcciones MAC para negar o permitir el acceso a los servicios, las direcciones MAC podrán darse de alta de forma individual e importando un archivo.
- Disociación de clientes en forma manual.
- Soportar los siguientes estándares de cifrado o encripcion:
  - WEP
  - TKIP

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

  - WPA
  - WPA2
  - WPA-PSK
  - WPA2-PSK
  - AES (CCMP)
  - RC4-40, 104, 128-bit
- Interactuar con servidores de RADIUS con el objetivo de definir perfiles de acceso, basados en atributos como Filter-ID
- Soportar los siguientes métodos de autenticación:
- MAC
- Web o Captive Portal
- IEEE 802.1x
- Soportar RFC 3580
- Soportar la funcionalidad de portal cautivo para autenticación con las siguientes características:
- Autenticación 802.1X
- Uso de Portal cautivo interno
- Uso Portal cautivo externo
- Portal de Invitados con acceso temporal
- Personalización tanto para el portal interno como para el de invitados, de acuerdo a los patrones gráficos y logos requeridos por el Instituto FONACOT.
- El portal Cautivo Interno podrá ser configurado para desplegarse en HTTP o HTTPS
- El portal Cautivo Interno deberá tener la capacidad para presentar diferentes atributos tales como el Número de serie del Punto de Acceso, SSID y MAC Address.
- Soportar los siguientes métodos de autenticación 802.1x:
  - EAP-TLS
  - EAP-MD5
  - EAP-FAST
  - EAP-SIM
  - EAP-TTLS
  - PEAP
- Capacidad para ocultar los SSID's configurados.
- Bloquear tráfico entre dispositivos asociados al mismo SSID
- Permitir una distinción de privilegios por el tipo de usuario dentro del mismo SSID, dichos privilegios deberán abarcar desde el filtrado de tráfico de capa 2, capa 3 y capa 4, de acuerdo a los siguientes criterios:
  - Source MAC address
  - Destination MAC address
  - IPv4 Source IP address
  - IPv4 Destination IP address
  - Source layer 4 port
  - Destination layer 4 port

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel.: 5241 5200 www.fonacot.gob.mx

- IPv4 Source socket
- IPv4 Destination socket
- IP type
- ICMP packet type and code
- ToS/DSCP marking
- 802.1p priority
- Ethertype

- Limitar ancho de banda tanto a nivel de usuario como por tipo de tráfico, así como manejo de prioridades aplicando calidad de servicio a los mismos a nivel de capa 2 y capa 3.
- Permitir filtrado de tráfico desde la Controladora y en los Puntos de Acceso de tal forma que este filtrado pueda radicar en los Puntos de Acceso, ya que en caso de un evento en el cual este pierda comunicación con la Controladora, el Punto de Acceso sea capaz de seguir soportando dicha aplicación de reglas.
- El filtrado de tráfico también deberá ser soportado para tráfico de Multicast
- Soportar la funcionalidad de actuar como WIDS/WIPS en base a los siguientes requerimientos:
- Detección y clasificación de Puntos de Acceso bajo diferentes categorías como Puntos de Accesos Vecinos o Externos, Autorizados, Ilegítimos o Prohibidos.
- Dicha detección deberá de informar datos de los Puntos de Acceso, tales como Dirección MAC, SSID y el Fabricante o Marca del equipo en cuestión.
- Proveer la funcionalidad de clasificar Puntos de Acceso no categorizados como Puntos de Acceso Vecinos o Externos en forma manual de ser requerido, o en su caso ser clasificados como Puntos de Acceso Ilegítimos.
- Capacidad para llevar a cabo la mitigación de amenazas basada en countermeasures que puedan trabajar por limitación de inundación de tramas, por envío de tramas que eviten a los dispositivos adjuntarse a dispositivos no permitidos y por agregación de dispositivos no permitidos a una lista negra.
- Capacidad para elegir los siguientes tipos de mitigación de amenazas o countermeasures:
  - Prevenir a dispositivos permitidos para hacer roaming sobre Puntos de Acceso no permitidos tales como Vecinos o Externos, Ilegítimos o Prohibidos.
  - Prevenir a los dispositivos en participar en redes de tipo Ad-Hoc.
  - Remover dispositivos que estén generando algún tipo de ataque de DoS.
  - Eliminar tramas responsables que generen un ataque de inundación de tráfico.
- Reconocimiento de las siguientes amenazas:
  - Conexiones Ad-Hoc
  - Cracking de llaves WPA-WEP

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Aplicaciones de tipo surveillance como Netstumbler
- Ataques de DoS
- Puntos de Acceso tipo Honeypot
- Detección de fuentes de interferencia como por ejemplo hornos de microondas o algún otro dispositivo que opere en la banda de los 2.4 GHz.
- Puntos de Acceso tipo spoofing

- La funcionalidad WIDS/WIPS deberá proveer reportes con el siguiente tipo de información:
- Fecha y hora en de detección de amenaza
- MAC Address del dispositivo fuente
- Tipo de amenza y categoria
- Intensidad de señal de la fuente de amenza (dBm)
- Access Point que realiza medida de contención
- Tipo de medida aplicada
- Clientes enviados a Lista Negra
- Detección de Rogue APs por método closed loop alámbrico / inalámbrico para reducción de falsos positivos

Funcionalidades de Administración y Monitoreo

- Contará con un Dashboard que presente los principales eventos en forma textual, gráfica y estadística de la red inalámbrica:
- Estatus de Access Point
- Clientes
- Sesiones activas de administradores
- Access Point por canal
- Licenciamiento
- WLANs inseguras
- Access Point sin categorizar
- Amenazas activas
- Eventos
- Soportar la función para gestionar usuarios que administren el sistema con privilegios de lectura/escritura y solo lectura, ya sea por autenticación local o remota, así como un tipo de usuario administrador adicional que solo pueda tener los privilegios para gestionar las cuentas de invitados y esta sea la única función a la que tenga acceso.
- Soportar SNMP v2c/v3
- La controladora deberá soportar los siguientes esquemas de administración:
  - GUI o Web
  - CLI
  - Consola
- Soportar el backup y restore de Imagen de Controladora, por los siguientes medios:
  - FTP

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

  - Local
  - Flash
- La actualización del firmware de la Controladora podrá realizarse a través de GUI (Web) y por CLI
- Poseer una función de actualización de firmware y almacenamiento de imágenes de respaldo (snapshot), para recuperar la controladora en caso de que el proceso falle o bien la imagen se encuentre dañada o corrupta
- Tener la función de realizar respaldos de la configuración en forma manual o calendarizada y que estos puedan ser enviados en forma automática a un servidor de almacenamiento por medio de un protocolo como FTP o SCP.
- Capacidad de envío de logs de acuerdo a su grado de severidad a un servidor Syslog, correspondientes a eventos de los Puntos de Acceso, Controladora, cambios de configuración y de los principales servicios proporcionados por la Controladora.
- Mostrar la siguiente información:
  - Puntos de Acceso Activos
  - Estadísticas WDS
  - Estadísticas de Balanceo de Cargas
  - Estadísticas de Alta Disponibilidad
  - Inventario de los Puntos de Acceso
- Mostrar la siguiente información con respecto a ruteo:
  - Forwarding Table
  - OSPF Linkstate
  - OSPF Neighbor
- Realizar un Inventario de los Puntos de Acceso que incluya:
  - Dirección IP/Máscara de Red/Gateway
  - Dirección MAC del Puerto Ethernet.
  - Versión de hardware y software
  - Antenas empleadas
  - Telnet or SSH (estado activo/inactivo)
  - DTIM period
  - Beacon Period
  - RTS Threshold
  - Canal(es) de Transmisión
  - Potencia de Transmisión (dB)
  - Rx Diversity
  - Tx Diversity
  - Preambulo (long, short)
  - 11n Channel Width
  - 11n Guard Interval
  - 11n Channel Bonding
- Herramientas de troubleshooting tales como PING, Traceroute, captura de paquetes en tiempo real.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

- Proporcionar un histórico de sesiones de usuarios, conocido como Call Detail Records (CDR).

Como parte del servicio de Red Inalambrica, el LICITANTE ganador deberá realizar las siguientes actividades:

- Proveer todo lo necesario relacionado con hardware y software para la instalación y puesta a punto del esquema de alta disponibilidad de las controladoras con las que se administraran todos los Access Points que conformen el servicio de Red Inalámbrica.
- Mantener a la última versión disponible la controladora y los Access Points (firmware) durante toda la vigencia del servicio.
- Realizar los cambios, ajustes y configuraciones necesarias, en los Access Points y en controladora.
- Administrar altas, bajas y cambios en los equipos y controladoras.
- Proveer cualquier accesorio, componente y/o material misceláneo necesario para la instalación y el funcionamiento de los Access Points y controladoras.
- Mantener operando correctamente el servicio de Red Inalámbrica durante toda la vigencia del servicio.
- Entregar reportes mensuales ó a solicitud del area técnica del Instituto FONACOT, relaiconados con el servicio de Red Inalámbrica, como, por ejemplo: velocidad promedio de usuarios, fallas, etc.
- A solicitud expresa del area tecnica, el LICITANTE ganador deberá realizar estudios de cobertura de red inalámbrica de cualquier sucursal del Instituto FONACOT. Los resultados de dicho estudio deberán permitir definir la infraestructura necesaria para implementar servicios de red inalámbrica adicionales, en estos casos, la infraestructura requerida se solicitará expresamente por el administrador del contrato bajo el concepto de Servicios Bajo Demanda.

Los sitios donde se requiere el servicio de Red Inalambrica son los siguientes, mismos que podrán variar segun las necesidades del Instituto.

Item	Localidad
1	ACAPULCO
2	AGUASCALIENTES
3	Lerma
4	CAMPECHE
5	CANCÚN
6	CD. DEL CARMEN
7	CD. JUÁREZ
8	CD. OBREGÓN
9	CELAYA
10	CHIHUAHUA

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 4553 52 65 74 00 www.fonacot.gob.mx

11	CHILPANCINGO
12	METRO 6
13	COATZACOALCOS
14	COLIMA
15	CONGRESO
16	CUERNAVACA
17	CULIACÁN
18	DELICIAS
19	DURANGO
20	GUADALAJARA ABASTOS
21	GUADALAJARA FEDERALISMO
22	HERMOSILLO
23	LA PAZ
24	LÁZARO CÁRDENAS
25	LEÓN
26	LOS MOCHIS
27	MANZANILLO
28	MAZATLÁN
29	MÉRIDA
30	MEXICALI
31	MIXCOAC
32	MONCLOVA
33	MONTERREY
34	MONTERREY II
35	MORELIA
36	NOGALES
37	OAXACA
38	PACHUCA
39	PORTALES
40	PUEBLA
41	PUERTO VALLARTA
42	QUERÉTARO
43	REYNOSA
44	SALTILLO
45	SAN LUIS POTOSÍ
46	TAMPICO
47	TEPIC
48	TIJUANA
49	TLALNEPANTLA
50	TLAXCALA

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

51	TOLUCA
52	TORREÓN
53	TUXTLA GUTIÉRREZ
54	URUAPAN
55	VALLEJO
56	VERACRUZ
57	VILLAHERMOSA
58	XALAPA
59	ZACATECAS
60	ZARAGOZA
61	Almacen Mar Adriatico

2.3.5.Archivos Compartidos en Red.

El LICITANTE realizará las actividades para la administración de los servicios de FileServer y FTP. Actualmente estos servicios se encuentran operando en Oficinas Centrales del Instituto FONACOT bajo la plataforma del Sistema Operativo de MS Windows Server 2016 .
El servicio deberá operar en infraestructura del LICITANTE ganador debiéndose migrar bajo las siguientes particularidades:

2.3.5.1.FILESERVER.

- El LICITANTE ganador deberá configurar el servicio para operar utilizando Replicación DFS (Distributed File System) lo cual permita la replicación como estrategia de recuperación ante desastres
- El servicio debera operar basado en 1 nodo virtual en OC (sede Insurgentes)
- El LICITANTE ganador deberá realizar la administración de los recursos configurando las particiones para alojar los datos del File Server en formato NTFS, así como la utilización de certificados SSL y estableciendo Quotas para limitar almacenamiento; estos límites de almacenamiento y los usuarios con acceso al éste servicio serán establecidos conforme a las necesidades del Instituto FONACOT.
- El servicio deberá permitir el uso de WorkFolders con acceso desde dispositivos Android, iOS y equipos de cómputo con versiones de sistema operativo Windows 7 o superiores, debiéndose poder filtrar y no permitir subir archivos de música, imágenes y video.
- El servicio de WorkFolders deberá contar con una capacidad de almacenamiento de mínimo de 2GB por usuario
- El servicio de File Server deberá contar con la opción de recuperación de archivos borrados en la red, por parte del usuario, contando con al menos

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 5584 52 65 24 00 www.fonacot.gob.mx

una versión diaria de la información. Así como permitir obtener información de la tendencia del uso del servicio

- Las versiones para recuperación estarán disponibles dentro de un límite de 1 TB y podrá ser modificado conforme a las necesidades del Instituto FONACOT.
- El servicio deberá contemplar la creación de Checkpoints para las máquinas virtuales, permitiendo su utilización en caso de falla en los equipos virtualizados. Estas copias deberán de realizarse cuando menos una vez al mes o cuando se realicen cambios en la configuraciones del servicio.
- Todas las actividades necesarias relacionadas con la migración, instalación, puesta a punto, operación y administración de estos servicios para los sitios que corresponda son responsabilidad del LICITANTE ganador.
- En función de la migración del servicio de FileServer este deberá mantenerse operando en las Oficinas Centrales del Instituto FONACOT (Sede Insurgentes).
- La infraestructura que el licitante ganador disponga para otorgar el servicio de FileServer deberá de mantener rangos menores al 80% diario, en lo que respecta al uso del procesador, memoria física y espacio de almacenamiento de todas las unidades de disco que componen el servicio por cada servidor instalado.
- Esto implica que el servicio de monitoreo debe configurar alertas con un umbral 80% en CPU, memoria y discos.

2.3.5.2. FTP

- El servicio deberá de autentificar a los usuarios para su acceso a la información por medio credenciales de dominio y cuentas locales, no permitiéndose los accesos anónimos.Para realizar lo anterior, el Instituto FONACOT proporcionara todas las facilidades al licitante ganador para integrarse con el servicio de Active Directory Institucional
- Para alojar los datos del FTP el LICITANTE ganador deberá configurar las particiones de almacenamiento en formato NTFS
- El LICITANTE ganador deberá garantizar la integridad, confidencialidad y disponibilidad de la información contenida en las carpetas durante y posteriormente a la migración del servicio.
- El LICITANTE ganador deberá realizar el respaldo de la información cuando menos de forma semanal manteniendo los dos inmediatos anteriores respaldos.
- El servicio deberá contemplar la creación de Checkpoints para las máquinas virtuales, permitiendo su utilización en caso de falla en los equipos virtualizados. Estas copias deberán de realizarse cuando menos

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

una vez al mes o cuando se realicen cambios en las configuraciones del servicio.

- En función de la migración del servicio de FTP, este deberá operar en las oficinas centrales del Instituto FONACOT (Sede Insurgentes)
- La infraestructura que que el licitante ganador disponga para otorgar el servicio de FTP deberá de mantener rangos menores al 80% diario, en lo que respecta al uso del procesador, memoria física y espacio de almacenamiento de todas las unidades de disco que componen el servicio por cada servidor instalado.
- Esto implica que el servicio de monitoreo debe configurar alertas con un umbral 80% en CPU, memoria y discos.

Todo el licenciamiento necesario de la plataforma de Microsoft será proporcionado por el área técnica del Instituto FONACOT para la implementación de los servicios

GESTIÓN DE LA SEGURIDAD.

El Instituto FONACOT requiere el servicio de gestión de la Seguridad alineado a estándares, mejores prácticas internacionales y disposiciones establecidas por la administración pública federal en materia de seguridad informática, con el objeto de que la implantación, operación, monitoreo de la seguridad se proporcione con altos niveles de servicio. El LICITANTE deberá aplicar la proactividad (prevención) necesaria para reducir el riesgo de ataques e incidentes sobre los componentes de seguridad involucrados en el otorgamiento del servicio solicitado.

El personal que designe el area tecnica del Instituto FONACOT deberá contar con acceso de sólo lectura a los equipos de seguridad utilizados para la prestación del servicio y en los casos que el administrador del contrato solicite se requiera, en acuerdo con el LICITANTE ganador, se deberá proporcionar acceso total a los equipos destinados a soportar el servicio, con el fin de supervisar y validar la configuración de los mismos.

Realizar, con base en estándares de seguridad, las acciones para el reforzamiento o endurecimiento de las configuraciones de parámetros de seguridad (hardening, políticas, reglas, etc.) de los elementos de infraestructura involucrados en el servicio solictado, en función de las vulnerabilidades conocidas, además de aquellas que sean solicitadas explícitamente por el area técnica del Instituto FONACOT.

Identificar y notificar vulnerabilidades, ataques, virus, malware y todo aquello que pueda impactar la seguridad informática del Instituto FONACOT, efectuado las acciones correctivas necesarias de forma remota o en sitio a fin de corregir la posible falla de seguridad.

2.3.6. Servicio de Contención Perimetral.

El LICITANTE ganador deberá implementar una solución de contención perimetral para proteger las Oficinas Centrales Sedes (Insurgentes y Plaza de la Republica) y sucursales

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 5553 52 65 74 00 www.fonacot.gob.mx

del Instituto FONACOT, mediante equipos firewall de ultima generación, que puedan proporcionar al menos las siguientes funciones: Firewall, Control e Identificación de Aplicaciones, VPNs Site to Site basadas en IPSec y SSL, IPS, Control Contra Amenazas, Control de Acceso y Transmisión de datos, asi como la Generación de Reportes. Todos los equipos que conformen la solución deberán ser administrados mediante una consola centralizada con herramientas graficas que permita simplificar la gestión y edición de políticas de una manera segura y sencilla.

La solución de contención perimetral propuesta por el LICITANTE deberá considerar esquemas de alta disponibilidad en modo activo-activo. para el caso de Oficinas Centrales y Plaza de la Republica. Es responsabilidad del LICITANTE considerar la instalación, configuración, puesta a punto y administración del esquema de contención propuesto.

La solución deberá tener la capacidad de generar políticas de seguridad a partir de la identificación de aplicaciones independientemente del protocolo, puerto de comunicación, cifrado o tácticas evasivas, asimismo, deberá identificar nombres de usuario y/o direcciones IP, y utilizar esta información para tener visibilidad, aplicar políticas.

Los equipos propuestos por el LICITANTE para otorgar el servicio de contención perimetral deberan cumplir con al menos las siguientes carateristicas técnicas:

2.3.6.1. Firewall Tipo 1

- El equipo debe estar basado en una plataforma Appliance del mismo fabricante
- Deberá contar con al menos 4 puertos 10/100/1000, y 6 puertos Gigabit SFP
- Deberá contar con 2 fuentes de energía eléctrica redundantes
- Deberá realizar las funciones de firewall conforme a los siguientes puntos:
  - Operar de manera simultánea en modo sniffer tanto en la capa 2 (nivel físico) como en la capa 3 (nivel lógico) del modelo OSI para efectuar la inspección del tráfico de datos de la red vía un puerto espejo
  - Efectuar ruteo virtual para al menos 10 ruteadores virtuales
  - Manejar tráfico entre diferentes zonas de seguridad y subredes, soportando al menos 80 zonas de seguridad y un mínimo de 10 firewalls virtuales.
  - Cada firewall virtual deberá soportar como mínimo:
    - 1,000,000 sesiones simultaneas
    - 1000 reglas de seguridad
    - 1,000 reglas de NAT
    - 2,000 túneles VPN IPSec
- Soportar al menos 4,094 redes virtuales basadas en el protocolo 802.1q por todo el equipo.
- Operar NAT por origen, destino, dirección ip y puertos

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. 1553 52 65 74 00 www.fonacot.gob.mx

- Soportar como mínimo los protocolos: PPoE, BGP, OSPF, rip2, DHCP Server y Relay
- Soportar los protocolos de cifrado: ike, 3des (128, 192 y 256 bits), aes, sha1 y md5.
- Identificar usuarios mediante LDAP, Directorio Activo, Radius y direccion IP
- Identificar aplicaciones como facebook, twitter, web 2.0, peer to peer. Ésta identificación deberá ser de manera independiente al puerto lógico y/o aplicaciones que usan los puertos 80 y 443 (identificación de aplicaciones que viajen a través de un túnel SSL o que utilicen tácticas evasivas)
- Capacidad para visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas para viajar cifradas, tales como ultrasurf, skype y ataques mediante el puerto 443.
- Permitir elaborar políticas de seguridad con base al protocolo y puerto
- Incluir tecnología superior a stateful firewalling
- Crear firmas para identificar las aplicaciones desarrolladas por el INSTITUTO FONACOT
- Descifrar de sesiones SSL para identificar las aplicaciones que se transmiten dentro de túneles SSL
- Crear políticas para el manejo de aplicaciones desconocidas basadas en TCP/UDP
- Identificar aplicaciones incluso cuando no utilicen puertos estándares. (En el caso de protocolos desconocidos se deberá asignar firmas propias)
- Descripción y control de tráfico ssh
- Descifrar aplicaciones dinámicas dentro de sesiones de proxy HTTP
- Controlar tráfico IPv4 e IPv6, (En IPv6 incluir visibilidad e inspección de amenazas en aplicaciones y control de contenido)
- Soportar IPv6 en interfaces trabajando en capa 2 y capa 3
- Deberá realizar el control e identificación de aplicaciones conforme a los siguientes puntos:
  - Permitir, negar, calendarizar, inspeccionar políticas de uso con base en aplicaciones:
  - Definición de hasta 8 clases de tráfico, con la finalidad de controlar aplicaciones cuyo consumo pueda ser excesivo como el streaming.
  - Permitir el monitoreo del uso de aplicaciones.
- Las funciones de VPN IPSec y SSL deberá realizarlas conforme a los siguientes puntos:
  - Soportar como mínimo 2000 túneles VPN IPSec con un rendimiento de al menos 2Gbps de troughput.
  - Aplicar políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles SSL.
  - Contar con SSL fall back y descifrado SSL (entrada y salida).
  - Contar con un software cliente de VPN SSL para los sistemas operativos Windows 7, Windows 8.1, Windows 10 y MAC OSX V10.10 o superior.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

  - Permitir la creación de políticas para tráfico VPN SSL
  - Soportar al menos 15,000 sesiones concurrentes vía SSL
  - Realizar la autenticación de VPN SSL a través de LDAP, Secure id y/o Base de Datos Propia
- La función de IPS Control Contra Amenazas, deberá efectuarse de acuerdo a lo siguiente:
  - Soportar protección contra malware en contenido HTML, Java script, Software Espía y Gusanos.
  - Ofrecer protección contra descargas involuntarias usando HTTP de archivos ejecutables maliciosos
  - Efectuar escaneo de virus en HTTP, SMTP y POP3
  - Ejecutar la inspección de archivos comprimidos que usan algoritmo deflate (zip, gzip, etc).
  - Soportar bloqueo de archivos por tipo (Tener registrados como mínimo 50 tipos)
  - Adaptar firmas Phone-home de software espía y explotación de vulnerabilidades.
  - Realizar la actualización de firmas de ataques de forma diaria, semanal y de emergencia.
  - Protección contra amenazas de Malware y Spyware
  - Rendimiento como mínimo de 2Gbps de Troughput.
  - Incluya mecanismos de IPS basados en:
    - Análisis de patrones de estado
    - Análisis de decodificación de protocolo
    - Análisis para detección de anomalías de protocolo
    - Análisis heurístico
    - IP desfragmentación
    - Reensamblado de paquetes de TCP
- Permitir el diseño de firmas de vulnerabilidades
- Haber pasado pruebas de los laboratorios NSS con al menos un 90% de efectividad para lo cual deberán incluir el reporte correspondiente
- Identificación de botnet por comportamiento
- Interceptar archivos ejecutables y realiza ejecución en un entorno Sanbox, para determinar si son archivos legítimos o malware tratando de entrar a la red
  - Deberá realizar el control de acceso y transmisión de datos conforme a lo siguiente:
- Administrar el tráfico de aplicaciones, permitiendo la ejecución de aplicaciones autorizadas Identificar nuevas aplicaciones.
- Crear políticas basadas en la visibilidad y control de quién está usando qué aplicaciones, a través de la integración con servicios de directorio.
- Autenticación vía LDAP, Directorio Activo, e directory y Base de Datos locales
- Crear políticas basadas por aplicación, categoría de aplicación, sub-categoría, tecnología y factor de riesgo.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Crear políticas basadas en el control por usuario, grupos de usuarios o dirección IP.
- Crear políticas basadas en Traffic shaping por aplicación, usuario, fuente, destino, Túnel VPN-IPSec-SSL.
- Controlar sin instalación de cliente de software, en equipos que soliciten salida a internet para que antes de iniciar la navegación, se despliegue un portal de autenticación residente en el firewall (captive portal) con soporte a autenticación por client certifícate.
- Soporte autenticación Kerberos
- Protección contra ataques de negación de servicios.
- Control de host diferentes a Windows, vía autenticación basada en web
  - La Generación de Reportes deberá considerar lo siguiente:
- Proporcionar un resumen gráfico de aplicaciones utilizadas, y amenazas encontradas diariamente.
- Permitir el control de transferencia de datos no autorizados con herramienta para realizar patrones definidos por usuario.
- Contar con la funcionalidad para la exportación de bitácoras (logs) de filtrado, vista de tráfico URL y amenazas
- Permitir la administración vía web, cli, syslog, snmp2.
- Administración basada en roles.
- Permitir la creación de reportes personalizados.
- Contar con herramienta para crear filtros de monitoreo de las sesiones históricas en el firewall ya sea por aplicación, IP origen y destino.
- Capacidad para generar un reporte gráfico que permita visualizar los cambios en el uso de aplicaciones en la red con respecto a un periodo de tiempo anterior
- Generación de reportes con mapas geográficos generados en tiempo real para la visualización de orígenes y destinos del tráfico generado.
- Proporcionar como mínimo los siguientes reportes:
  - Utilización de ancho de banda de entrada y salida por aplicación (TOP 10)
  - No. De Sesiones por aplicación (TOP 10)
  - Comparativo semanal de aplicaciones corriendo en la red que pudieran incrementar o decrementar su utilización (top 10)
  - utilización (en bytes) por aplicación (top 10).
  - Origen y destino del tráfico por aplicación-usuario (TOP 10)
  - Eventos / Ataques por: Origen, Categoría, Amenaza, Protocolo. (TOP 10)
  - Nivel de riesgo de la red.
  - Principales aplicaciones que circulan por el Firewall (TOP 25).
  - Principales direcciones IP destino por protocolo (TOP 25).
  - Las principales direcciones IP para cada uno de los protocolos y aplicaciones (TOP 50)

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Deberá incluir una tecnología de identificación de malware moderno contando con la detección de comportamientos maliciosos, detección de tácticas de evasión y aprendizaje de maquina (machine learning).
- Deberá incluir la inspección de malware en día cero para documentos tipo Ejecutables, dll, Office (Word, Excel, Powerpoint) , pdf, apk, jar (Java), y Adobe Flash.
  - Bidirectional Forwarding Detection (BDF)
- Deberá identificar usuarios a través de integración con Active Directory, LDAP, eDirectory.
- Reporte de aplicaciones tipo SAAS.
- Funcionalidad de prevención de robo de credenciales detectando el momento en que los usuarios envían credenciales corporativas validas a un sitio. Este procedimiento puede realizarse de acuerdo a un grupo de usuarios de LDAP e identificación de usuarios activos en la red.

2.3.6.2. Firewall Tipo 2

- El equipo debe estar basado en una plataforma Appliance del mismo fabricante
- Deberá contar con al menos 8 puertos 10/100/1000
- Deberá efectuar detección de falla mediante supervisión de rutas y monitoreo de interfaces
- Deberá realizar las funciones de firewall conforme a los siguientes puntos:
  - Operar de manera simultánea en modo sniffer tanto en la capa 2 (nivel físico) como en la capa 3 (nivel lógico) del modelo OSI para efectuar la inspección del tráfico de datos de la red vía un puerto espejo
  - Efectuar ruteo virtual para al menos 3 ruteadores virtuales
- Manejar tráfico entre diferentes zonas de seguridad y subredes, soportando al menos 10 zonas de seguridad
- El firewall debe soportar como mínimo:
  - 64,000 sesiones simultaneas
  - 250 reglas de seguridad
  - 125 reglas de NAT
  - 500 túneles VPN IPSec
- Soportar al menos 246 redes virtuales basadas en el protocolo 802.1q
- Operar NAT por origen, destino, dirección ip y puertos
- Soportar como mínimo los protocolos: PPoE, BGP, OSPF, rip2, DHCP Server y Relay
- Soportar los protocolos de cifrado: ike, 3des (128, 192 y 256 bits), aes, sha1 y md5.
- Identificar usuarios mediante LDAP, Directorio Activo, Radius y dirección IP

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Identificar aplicaciones como facebook, twitter, web 2.0, peer to peer. Ésta identificación deberá ser de manera independiente al puerto lógico y/o aplicaciones que usan los puertos 80 y 443 (identificación de aplicaciones que viajen a través de un túnel SSL o que utilicen tácticas evasivas)
- Capacidad para visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas para viajar cifradas, tales como ultrasurf, skype y ataques mediante el puerto 443.
- Permitir elaborar políticas de seguridad con base al protocolo y puerto
- Incluir tecnología superior a stateful firewalling
- Crear firmas para identificar las aplicaciones desarrolladas por el INSTITUTO FONACOT
- Descifrar de sesiones SSL para identificar las aplicaciones que se transmiten dentro de túneles SSL
- Crear políticas para el manejo de aplicaciones desconocidas basadas en TCP/UDP
- Identificar aplicaciones incluso cuando no utilicen puertos estándares. (En el caso de protocolos desconocidos se deberá asignar firmas propias)
- Descripción y control de tráfico sshv
- Descifrar aplicaciones dinámicas dentro de sesiones de proxy HTTP
- Controlar tráfico IPv4 e IPv6, (En IPv6 incluir visibilidad e inspección de amenazas en aplicaciones y control de contenido)
- Soportar IPv6 en interfaces trabajando en capa 2 y capa 3
- Deberá realizar el control e identificación de aplicaciones conforme a los siguientes puntos:
  - Permitir, negar, calendarizar, inspeccionar políticas de uso con base en aplicaciones:
  - Definición de hasta 8 clases de tráfico, con la finalidad de controlar aplicaciones cuyo consumo pueda ser excesivo como el streaming.
  - Permitir el monitoreo del uso de aplicaciones.
- Las funciones de VPN IPSec y SSL deberá realizarlas conforme a los siguientes puntos:
  - Soportar como mínimo 25 túneles VPN IPSec con un rendimiento de al menos 100Mbps de troughput.
  - Aplicar políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles SSL.
  - Contar con SSL fall back y descifrado SSL (entrada y salida).
  - Contar con un software cliente de VPN SSL para los sistemas operativos Windows 7, Windows 8.1, Windows 10 y MAC OSX V10.10 o superior.
  - Permitir la creación de políticas para tráfico VPN SSL
  - Soportar al menos 4,200 sesiones concurrentes vía SSL
  - Realizar la autenticación de VPN SSL a través de LDAP, Secure id y/o Base de Datos Propia
- La función de IPS Control Contra Amenazas, deberá efectuarse de acuerdo a lo siguiente:

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Soportar protección contra malware en contenido HTML, Java script, Software Espía y Gusanos.
- Ofrecer protección contra descargas involuntarias usando HTTP de archivos ejecutables maliciosos
- Efectuar escaneo de virus en HTTP, SMTP y POP3
- Ejecutar la inspección de archivos comprimidos que usan algoritmo deflate (zip, gzip, etc).
- Soportar bloqueo de archivos por tipo.
- Adaptar firmas Phone-home de software espía y explotación de vulnerabilidades.
- Realizar la actualización de firmas de ataques de forma diaria, semanal y de emergencia.
- Protección contra amenazas de Malware y Spyware
- Rendimiento como mínimo de 500 Mbps de Troughput.
- Incluya mecanismos de IPS basados en:
  - Análisis de patrones de estado
  - Análisis de decodificación de protocolo
  - Análisis para detección de anomalías de protocolo
  - análisis heurístico
  - IP desfragmentación
  - Reensamblado de paquetes de TCP
- Permitir el diseño de firmas de vulnerabilidades
- Haber pasado pruebas de los laboratorios NSS con al menos un 90% de efectividad para lo cual deberán incluir el reporte correspondiente
- Identificación de botnet por comportamiento
- Interceptar archivos ejecutables y realiza ejecución en un entorno Sanbox, para determinar si son archivos legítimos o malware tratando de entrar a la red

- Deberá realizar el control de acceso y transmisión de datos conforme a lo siguiente:
  - Administrar el tráfico de aplicaciones, permitiendo la ejecución de aplicaciones autorizadas Identificar nuevas aplicaciones.
  - Crear políticas basadas en la visibilidad y control de quién está usando qué aplicaciones, a través de la integración con servicios de directorio.
  - Autenticación vía LDAP, Directorio Activo y Base de Datos locales
  - Crear políticas basadas por aplicación, categoría de aplicación, sub-categoría, tecnología y factor de riesgo.
  - Crear políticas basadas en el control por usuario, grupos de usuarios o dirección IP.
  - Crear políticas basadas en Traffic shaping por aplicación, usuario, fuente, destino, Túnel VPN-IPSec-SSL.
  - Controlar sin instalación de cliente de software, en equipos que soliciten salida a internet para que antes de iniciar la navegación, se

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

despliegue un portal de autenticación residente en el firewall (captive portal) con soporte a autenticación por client certifícate.
  - Soporte autenticación Kerberos
  - Protección contra ataques de negación de servicios.
  - Control de host diferentes a Windows, vía autenticación basada en web
- La Generación de Reportes deberá considerar lo siguiente:
  - Proporcionar un resumen gráfico de aplicaciones utilizadas, y amenazas encontradas diariamente.
  - Permitir el control de transferencia de datos no autorizados con herramienta para realizar patrones definidos por usuario.
  - Contar con la funcionalidad para la exportación de bitácoras (logs) de filtrado, vista de tráfico URL y amenazas
  - Permitir la administración vía web, cli, syslog, snmp2.
  - Administración basada en roles.
  - Permitir la creación de reportes personalizados.
  - Contar con herramienta para crear filtros de monitoreo de las sesiones históricas en el firewall ya sea por aplicación, IP origen y destino.
  - Capacidad para generar un reporte gráfico que permita visualizar los cambios en el uso de aplicaciones en la red con respecto a un periodo de tiempo anterior
  - Generación de reportes con mapas geográficos generados en tiempo real para la visualización de orígenes y destinos del tráfico generado.
  - Proporcionar como mínimo los siguientes reportes:
    - Utilización de ancho de banda de entrada y salida por aplicación (TOP 10)
    - No. De Sesiones por aplicación (TOP 10)
    - Comparativo semanal de aplicaciones corriendo en la red que pudieran incrementar o decrementar su utilización (top 10)
    - utilización (en bytes) por aplicación (top 10).
    - Origen y destino del tráfico por aplicación-usuario (TOP 10)
    - Eventos / Ataques por: Origen, Categoría, Amenaza, Protocolo. (TOP 10)
    - Nivel de riesgo de la red.
    - Principales aplicaciones que circulan por el Firewall (TOP 25).
    - Principales direcciones IP destino por protocolo (TOP 25).
    - Las principales direcciones IP para cada uno de los protocolos y aplicaciones (TOP 50)
- Deberá incluir una tecnología de identificación de malware moderno contando con la detección de comportamientos maliciosos, detección de tácticas de evasión y aprendizaje de maquina (machine learning).

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 5511 52 05 74 00 www.fonacot.gob.mx

- Deberá incluir la inspección de malware en día cero para documentos tipo Ejecutables, dll, Office (Word, Excel, Powerpoint) , pdf, apk, jar (Java) y Adobe Flash.
- Bidirectional Forwarding Detection (BDF)
- Deberá identificar usuarios a través de integración con Active Directory, LDAP, eDirectory.
- Reporte de aplicaciones tipo SAAS.
- Funcionalidad de prevención de robo de credenciales detectando el momento en que los usuarios envían credenciales corporativas validas a un sitio. Este procedimiento puede realizarse de acuerdo a un grupo de usuarios de LDAP e identificación de usuarios activos en la red.

Los equipos de contención perimetral deberán distribuirse conforme a la siguiente tabla:

Item	Localidad	Cantidad Solicitada	Tipo de Firewall solicitado
1	OFICINAS CENTRALES VPN MPLS	2 (HA)	Tipo 1
2	OFICINAS CENTRALES INTERNET	2 (HA)	Tipo 1
3	PLAZA DE LA REPUBLICA VPN MPLS	2 (HA)	Tipo 1
4	PLAZA DE LA REPUBLICA INTERNET	2 (HA)	Tipo 1
5	Hermosillo	1	Tipo 2
6	GUADALAJARA ABASTOS	1	Tipo 2
7	Veracruz	1	Tipo 2
8	MONTERREY	1	Tipo 2
9	INE	2	Tipo 2

2.3.6.3. Filtrado de contenido Web

El LICITANTE ganador deberá realizar las actividades necesarias para la administración, de la herramienta de filtrado WEB

Actualmente el servicio se encuentra operando en las oficinas centrales del Instituto FONACOT en un esquema de un servidor para administración y reportes junto con un Appliance modelo V5000 capacidad de 2100 licencias vigentes.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1553 52 65 74 00 www.fonacot.gob.mx

El servicio deberá operar conforme las siguientes particularidades:

La administración y reportes de la solucion debera estar concentrada en un servidor dedicado y con acceso Web, en el mismo servidor debe estar también el acceso a la administración del appliance que formen parte de la solución ofertada.

El LICITANTE deberá considerar efectuar la validación de resolución de DNS´s externos e internos y en caso de fallas, dar seguimiento con el proveedor del servicio de Internet y/o personal del área técnica del Instituto FONACOT.

El LICITANTE ganador deberá configurar la solución para permitir migrar/actualizar las políticas de uso que actualmente están en funcionamiento en el Instituto FONACOT, con el objeto de conservar y garantizar el cumplimiento de las políticas o normas de seguridad con relación a los sitios/categorías en la navegación Web establecidas por el área técnica del Instituto FONACOT.

EL LICITANTE deberá configurar la solución para generar y entregar reportes de forma mensual y/o a petición del área técnica del Instituto FONACOT pudiendo ser estos resúmenes ejecutivos, reportes detallados, gráficas y/o tablas.

Filtrado de contenido Web

La solución de filtrado Web ofertada deberá ser conforme se describe a continuación:

- La administración y reportes de la solucionde filtrado Web debe concentrarse en un solo equipo, en el mismo también tiene que estar la administración del appliance involucrado en la solución ofertada.
- El appliance dedicado al filtrado Web no podrán ser compartido
- El LICITANTE ganador deberá configurar la solución para que las 24 horas del día, en conjunto con la información de la red de inteligencia del fabricante, descubra de manera oportuna y dinámica, amenazas Web, sitios web en tiempo real con alto riesgo para la organización, tecnologías y técnicas para la identificación de datos, asi como detectar y bloquear por tipo y tamaño archivos embebidos y/o descargados.
- Deberá soportar modos de operacion como proxy transparente o proxy explícito.
  - El modo de operación proxy transparente debe incluir: Soporte para usar WCCP (Web Cache Content Protocol) y PBR (Policy Based Routing).
  - El modo de operación proxy explicito debe incluir lo siguiente: configuración manual de browser y/o soporte para auto configuración del proxy mediante el uso de PAC, WPAC y políticas de Active Directory. La generacion de politicas de Active Directory seran responsabilidad del Instituto FONACOT
- Considerando la perspectiva descrita en el punto anterior la solución deberá tener la capacidad de identificar y administrar lo siguiente:

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 65 74 00 www.fonacot.gob.mx

- Usuarios autorizados para acceder a sitios web específicos, contenido o aplicaciones sensibles en tiempo real.
- Datos críticos e importantes para la organización que deberán ser protegidos contra fugas intencionales o accidentales.
- Como los usuarios están comunicando datos sensibles y como los recursos en línea son utilizados de manera más segura y productiva por la organización.
- Donde los usuarios están permitidos acceder en línea y a donde los datos sensibles pueden ser enviados.
- Aprovechar el potencial de las nuevas herramientas web sociales, de comunicación y colaboración como Facebook, LinkedIn, Twitter y otros servicios basados en la nube, evitando amenazas de malware, ataques basados en la web que eluden el software antivirus o contenido inapropiado ni fuga de información confidencial.

• La solución de filtrado Web ofertada debe incluir al menos las siguientes capacidades/funcionalidades:

- Filtrado de navegación Web basado en Proxy
- Personalización de las páginas de bloqueo enviadas por los dispositivos instalados para este fin dentro de las instalaciones del Instituto FONACOT.
- Capacidad de filtrar trafico http y https
- Capacidad de sincronizar su configuración (Políticas/Permisos/Excepciones/Usuarios) con centros de datos del fabricante para que equipos de usuarios que salen de la red del Instituto FONACOT continúen protegidos.
- Contar con software cliente (Endpoint) que forcé la configuración de la navegación e impida al usuario modificar los parámetros de proxy en sus navegadores.

• La solución de filtrado Web deberá estar integrada con el dominio de Active Directory del Instituto FONACOT.

• La solución de filtrado/seguridad Web deberá tener la capacidad para aplicar políticas en base a:

- Usuarios
- Grupos
- Unidades Organizaciones
- Direcciones IP
- Rangos de direcciones IPs

• La solución de filtrado/seguridad Web deberá tener la capacidad de entregar reportes basados en la combinación de apartados como:

- Objetos del AD (usuarios, grupos, OUs, etc.)
- Consumo de datos (de subida, de bajada, totales)
- Dia, mes, año, periodos.
- Bloqueo, permitido.

La solución propuesta debe considerar un esquema de filtrado por regiones y administrada centralizadamente conforme a la siguiente distribución:

Región	Servicio
Norte	Filtrado Web

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

Noreste	Filtrado Web
Occidente	Filtrado Web
Sureste	Filtrado Web
Plaza de la Republica CDMX	Filtrado Web
Oficinas Centrales CDMX	Filtrado Web

El licitante debera considerar que en cada una de las regiones antes mencionadas se debera implementar un appliance físico o virtual.

2.3.7. CABLEADO ESTRUCTURADO

El LICITANTE ganador realizará las actividades para la instalación y mantenimiento de los nodos de cableado estructurado a nivel nacional, conservando la certificación Systimax del sistema de cableado implementado en el Instituto FONACOT. Los materiales suministrados para el sistema de cableado estructurado deberán ser totalmente nuevos, libres de todo defecto o corrosión y del mismo fabricante del cableado que actualmente se encuentra instalado en el Instituto FONACOT. En los casos que se requiera, El LICITANTE deberá considerar el suministro e instalación de patch panel, jacks, faceplates, organizadores de cables, charolas de fijación, racks, gabinetes, organizadores, tuberías, canalizaciones, escalerillas y cualquier material misceláneo que se requiera para la instalación.

2.3.7.1. Instalación de nodos nuevos

El servicio consiste en instalar nodos nuevos en cualquier oficina del Instituto FONACOT a nivel nacional, de acuerdo a especificaciones, desde el patch panel hasta la placa para la conexión del equipo, se deberá considerar instalar cableado UTP categoría 6a bajo la norma EIA/TIA 568B para el caso de apertura de nuevas oficinas. El LICITANTE ganador deberá realizar el etiquetado de todos los componentes del sistema de cableado tales como racks o gabinetes, cables, puertos, paneles, placas, etc.

2.3.7.2. Reubicación de nodos existentes

El servicio consiste en reubicar cualquier componente de nodos ya instalados en cualquier oficina del Instituto FONACOT a nivel nacional, de acuerdo a especificaciones, desde el patch panel hasta la placa para conexión del equipo.

2.3.7.3. Mantenimiento de nodos de red

El servicio consiste en realizar el mantenimiento de los nodos de red que se encuentren dañados a solicitud de la convocante, en cualquier oficina del Instituto FONACOT a nivel nacional, llevando acabo la reposición de accesoarios de acoplamineto, conectorizacion y montaje de los mismos.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 65 74 00 www.fonacot.gob.mx

2.3.7.4. Instalación de Fibra Óptica

El servicio consiste en instalar fibra óptica nueva tipo multimodo con al menos 2 hilos en cualquier Oficina del Instituto FONACOT Es responsabilidad del LICITANTE considerar el suministro e instalación de cualquier componente relacionado con el tendido de fibra óptica tales como charolas, paneles, conectores, patchcord, canalización, etc. El LICITANTE deberá considerar un máximo de 150m por cada cable de fibra óptica instalado.

2.3.7.5. Movimientos de infraestructura.

El servicio consiste en instalar y/o desinstalar equipo activo, gabinetes, racks, organizadores y/o patch panel en cualquier localidad del Instituto FONACOT a nivel nacional para su traslado y puesta en operación o bien para su baja del inventario. Esto puede ser requerido para lugares diferentes dentro de un área metropolitana o entidad federativa.

2.3.8. SERVICIO DE ADMINISTRACIÓN DE ENERGÍA REGULADA (UPS)

El licitante ganador se obliga a implementar el servicio de energia regulada a fin de brindar un respaldo de energía eléctrica a los equipos de redes y comunicaciones, así como PC's en todas las localidades del Instituto FONACOT.

La solución propuesta debe considerar el suministro del equipamiento, la instalación y puesta a punto, actividades que deberán ser realizadas por personal del LICITANTE dentro de los periodos establecidos en los niveles de servicio respectivos. Cabe aclarar que todas las actividades se deben efectuar en ventanas de servicio que no afecten la operación normal del Instituto FONACOT.

El LICITANTE debe considerar accesorios, material, consumibles, mano de obra, conectores, ductería, refacciones, componentes, adecuaciones y configuraciones necesarias para la adecuada implementación y operación del sistema de administración de energía regulada, así como cualquier otro elemento para mantener la continuidad del servicio.

para la puesta a punto del servicio, el licitante deberá realizar la instalación de cableado eléctrico desde los centros de carga hasta el sistema de administración de energía regulada (UPS)

El LICITANTE deberá entregar al area técnica del Instituto la memoria técnica en medio electrónico, incluyendo al menos los siguientes aspectos:

Diagrama de conexión del sistema de administración de energía regulada,
Diagrama de conexión del sistema de tierra física y acondicionamiento eléctrico (en caso de haberse requerido)

Validación del tiempo de respaldo del sistema de administración de energía regulada
Fotografías de instalación del sistema de administración de energía regulada, sistema de tierra física y acondicionamiento eléctrico.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

La entrega al destino final de los equipos será de la total responsabilidad del LICITANTE, los costos que se generen con motivo de la entrega del equipo corren por cuenta del LICITANTE, por lo que éste asume la responsabilidad total por el aseguramiento y gastos asociados que se generen por el manejo y traslados de los activos que se suministren con motivo de este servicio.

Es responsabilidad del LICITANTE, efectuar todas las pruebas de operación e integración de todos los elementos que conforman la solución ofertada, con la finalidad de asegurar la adecuada interoperabilidad y funcionalidad de dichos elementos.

Para el caso de las Oficinas Centrales sede Insurgentes del Instituto FONACOT, el licitante debera considerar como parte del servicio, todos los elementos y/o componentes de enfriamiento que permitan que el servicio de energia regulada implementado en dicho sitio opere bajo las condiciones de temperatura adecuadas.

Los equipos que conformen el servicio de administración de energía regulada deberán cumplir con al menos las siguientes características técnicas:

Equipos de energía regulada de hasta 10 KVA:

Tecnología true on-line doble conversión
Frecuencia de entrada y de salida 50-60 Hz
Calidad de regulación de voltaje en línea y batería +/- 1%
Voltaje de salida 120 VAC
Factor de cresta en corriente 3 a 1
Temperatura de operación de 0° a 40° C
Humedad relativa de 0 a 95%.
Interruptor de bypass interno para mantenimiento y bypass automático.
Tarjeta de comunicación SNMP.
Interfase de comunicación RS232 en conector db9 y/o USB.
Base o soporte para que el equipo propuesto pueda ser utilizado como torre o en rack.
Normas y certificaciones:

- UL 1778, CSA, FCC clase A(2),

Los equipos con capacidad mayor 16KV adicionalmente deberán cumplir con las siguientes caracteristicas:

Debe ser configurable para alcanzar un nivel de redundancia interna de n+1
Debe proporcionar altos niveles de disponibilidad mediante redundancia al permitir la configuración con un módulo de potencia exceso respecto de la cantidad requerida para ofrecer soporte a la carga conectada.
Debe tener módulos de inteligencia redundantes.
Debe proporcionar niveles altos de disponibilidad a las cargas conectadas a la ups y ofrecer vías redundantes de comunicación con las funciones clave de la unidad ups.
Debe aumentar la disponibilidad y permitir la recuperación inmediata y sin inconvenientes tras fallas aisladas de módulos en configuración n+1 y/o a través del desvío (bypass)
Debe ofrecer altos niveles de disponibilidad mediante baterías redundantes y/o baterías externas

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 05 74 00 www.fonacot.gob.mx

Debe contar con módulos de potencia reemplazables en caliente.
Debe garantizar que llegue un suministro puro e ininterrumpido a los equipos protegidos durante el recambio de módulos de potencia en configuración n+1 y/o a través del desvío (bypass)
Debe permitir el diseño modular.
Debe proporcionar velocidad de servicio, la funcionalidad de auto diagnóstico y la capacidad de reemplazar módulos en el sitio.
Calidad de Regulación de Voltaje en línea y batería +/-3% (de L-N)

Los equipos de administración de energía regulada deberán distribuirse conforme a la siguiente tabla,misma que podrá variar según las necesidades del Instituto.

Ubicación.	Tipo.	Cantidad
UPS Tipo 9		
Oficinas Centrales	Tipo 9 100 KVA	1
UPS Tipo 8		
Oficinas Centrales	Tipo 8 40 KVA	1
UPS Tipo 7		
Plaza de la Republica	Tipo 7 30 KVA	1
Plaza de la Republica	Tipo 7 30 KVA	1
Tlalnepantla	Tipo 7 30 KVA	1
UPS Tipo 6		
Hermosillo	Tipo 6 20 KVA	1
Monterrey	Tipo 6 20 KVA	1
Molinos	Tipo 6 20 KVA	1
Portales	Tipo 6 20 KVA	1
Vallejo	Tipo 6 20 KVA	1
Mérida	Tipo 6 20 KVA	1
Metro Seis	Tipo 6 20 KVA	1
Zaragoza	Tipo 6 20 KVA	1
Toluca	Tipo 6 20 KVA	1
UPS Tipo 5		
Acapulco	Tipo 5 16 KVA	1
Guadalajara	Tipo 5 16 KVA	1
Cancún	Tipo 5 16 KVA	1
Aguascalientes	Tipo 5 16 KVA	1
Chihuahua	Tipo 5 16 KVA	1

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

Culiacán	Tipo 5 16 KVA	1
La Paz	Tipo 5 16 KVA	1
Mazatlán	Tipo 5 16 KVA	1
Pachuca	Tipo 5 16 KVA	1
Puebla	Tipo 5 16 KVA	1
Querétaro	Tipo 5 16 KVA	1
San Luis Potosí	Tipo 5 16 KVA	1
Tampico	Tipo 5 16 KVA	1
Tijuana	Tipo 5 16 KVA	1
Tuxtla Gtz.	Tipo 5 16 KVA	1
Veracruz	Tipo 5 16 KVA	1
Villahermosa	Tipo 5 16 KVA	1
Cuernavaca	Tipo 5 16 KVA	1
Durango	Tipo 5 16 KVA	1
Torreón	Tipo 5 16 KVA	1
Campeche	Tipo 5 16 KVA	1
León	Tipo 5 16 KVA	1
Mexicali	Tipo 5 16 KVA	1
Morelia	Tipo 5 16 KVA	1
Oaxaca	Tipo 5 16 KVA	1
GDL Federalismo	Tipo 5 16 KVA	1
Saltillo	Tipo 5 16 KVA	1
UPS Tipo 4		
Tlaxcala	Tipo 4 10 KVA	1
Colima	Tipo 4 10 KVA	1
Zacatecas	Tipo 4 10 KVA	1
Puerto Vallarta	Tipo 4 10 KVA	1
Cd Juárez	Tipo 4 10 KVA	1

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

Cd Obregón	Tipo 4 10 KVA	1
Celaya	Tipo 4 10 KVA	1
Tepic	Tipo 4 10 KVA	1
Congreso	Tipo 4 10 KVA	1
UPS Tipo 3		
Cd del Carmen	Tipo 3 8KVA	1
Los Mochis	Tipo 3 8KVA	1
Manzanillo	Tipo 3 8KVA	1
Monclova	Tipo 3 8KVA	1
Nogales	Tipo 3 8KVA	1
Reynosa	Tipo 3 8KVA	1
Xalapa	Tipo 3 8KVA	1
UPS Tipo 2		
Chilpancingo	Tipo 2 5KVA	1
Coatzacoalcos	Tipo 2 5KVA	1
Lázaro Cárdenas	Tipo 2 5KVA	1
Chetumal	Tipo 2 5KVA	1
Cozumel	Tipo 2 5KVA	1
Cuautitlán	Tipo 2 5KVA	1
Ensenada	Tipo 2 5KVA	1
Fresnillo	Tipo 2 5KVA	1
Matamoros	Tipo 2 5KVA	1
Piedras negras	Tipo 2 5KVA	1
Playa del Carmen	Tipo 2 5KVA	1
Tapachula	Tipo 2 5KVA	1
Texcoco	Tipo 2 5KVA	1
Zamora	Tipo 2 5KVA	1
Monterrey 2	Tipo 2 5KVA	1
Cd Valles	Tipo 2 5KVA	1

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

Uruapan	Tipo 2 5KVA	1
Lerma	Tipo 2 5KVA	1
UPS Tipo 1		
Almacén mar adriático	Tipo 1 3 KVA	1
Ciudad victoria	Tipo 1 3 KVA	1
Córdoba	Tipo 1 3 KVA	1
Cuautla	Tipo 1 3 KVA	1
Ecatepec	Tipo 1 3 KVA	1
Empalme	Tipo 1 3 KVA	1
Irapuato	Tipo 1 3 KVA	1
San José del cabo	Tipo 1 3 KVA	1
San juan del rio	Tipo 1 3 KVA	1
Tehuacán	Tipo 1 3 KVA	1
Tuxtepec	Tipo 1 3 KVA	1
Delicias	Tipo 1 3 KVA	1
Cd Acuña	Tipo 1 3 KVA	1
Guasave	Tipo 1 3 KVA	1

2.3.9. SOPORTE TÉCNICO.

El soporte técnico considera las actividades para atender y solucionar los distintos requerimientos, incidentes y/o problemas relacionados con los componentes de infraestructura involucrados en la prestación de los servicios suministrados por el LICITANTE.

Las actividades de soporte tecnico deberán ser ejecutadas por personal que cumpla con el siguiente perfil:

Estudios concluidos a nivel licenciatura de alguna de las carreras técnicas. Se deberá presentar en la propuesta técnica copia de carta pasante, certificado, constancia, titulo y/o cédula profesional. Se deberá presentar currículo Vitae del personal de soporte técnico propuesto que incluya, al menos los siguientes puntos:

- Nombre(s) y apellido(s)
- Nivel de estudios
- Experiencia mínima de 5 años en actividades de soporte de servicios de TIC
- Puesto de trabajo dentro de la empresa
- Proyectos en los que ha participado, con la siguiente información mínima para cotejar: nombre de la empresa o institución, contacto, teléfono, correo electrónico
- Carta de al menos un cliente firmada por el responsable del proyecto, avalando que dicho personal ha demostrado contar con la capacidad técnica para proporcionar servicios similares a los solicitados.

Av. Insurgentes Sur 452 Col. Roma Sta. Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Copia legible de identificación oficial.
- El Curriculo deberá venir firmado por el personal propuesto.

Se deberá acreditar que el personal propuesto es parte de la plantilla contratada por el LICITANTE, por lo tanto, se debe de presentar el alta ante el IMSS.

Cumplir con las siguientes certificaciones emitidas por el fabricante de la tecnología o por centro autorizado de entrenamiento del fabricante correspondiente el personal que se asigne por el LICITANTE para cubrir este perfil deberá cumplir en conjunto con las acreditaciones requeridas; no es requisito que cada una de las personas cumpla con la totalidad de las acreditaciones solicitadas:

No.	Servicio	Certificación Requerida	Fabricante
1	Monitoreo de Infraestructura	Certificación Técnica	Fabricante de solución propuesta
2	Switching	Extreme certified specialist – switching (ECS) Extreme certified specialist-routing (ECS) Extreme certified specialist –policy (ECS) Extreme certified expert – networking (ECE)	Enterasys / Extreme
3	Archivos compartidos en red,	Certificación MCSA Windows server 2012 o superior.	Microsoft
4	Contención Perimetral	Certificación Técnica	Fabricante de solución propuesta
5	Filtrado de contenidos	AP-Web Administrator.	Forcepoint

El soporte técnico se realizará cuantas veces sea necesario en función de los requerimientos que se soliciten o presenten durante la vigencia del contrato, mismos que se podrán otorgar de manera remota o en sitio en las localidades del Instituto FONACOT o. La naturaleza, escalamiento o criticidad del requerimiento impera o prevalece sobre la asistencia remota, a fin de que se puedan realizar las acciones de soporte directamente en sitio.

El LICITANTE deberá asignar 1 persona con perfil de soporte técnico en el inmueble de oficinas centrales del Instituto FONACOT (Sede Insurgentes), para cubrir un horario de 9:00 a 18:00 hrs de lunes a viernes. Sábados guardia remota de 9:00 a 17:00 hrs. el resto del personal del LICITANTE deberá operar de forma remota de forma remota

Conforme a los niveles de servicio establecidos en este anexo técnico, es responsabilidad del LICITANTE considerar la cantidad de personal que estime necesario para el desarrollo de las actividades de soporte técnico a nivel nacional.

El Instituto FONACOT se reserva en todo momento el derecho para evaluar por los medios y formas que considere pertinentes al personal asignado por el LICITANTE para otorgar el

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

servicio, así como solicitar su sustitución por así considerarlo conveniente. En caso de que la solicitud de sustitución del personal se derive de una falta que afecte la imagen y/o la confidencialidad de la información del Instituto FONACOT, el LICITANTE ganador se obliga a cooperar con el área técnica del Instituto FONACOT para el descargo de pruebas y evidencias en las que hubiese incurrido su personal.

Al ingreso del nuevo personal se deberá presentar la notificación respectiva. La persona que ingrese como sustituto deberá cumplir con los mismos requisitos definidos en el perfil correspondiente, por lo que se deberá entregar la documentación pertinente para su validación.

El soporte técnico incluye de manera general los conceptos de administración de servicios ; monitoreo, switching; red inalámbrica, gestión de la seguridad, UPS, cableado estructurado; documentación; mantenimiento preventivo y mantenimiento correctivo. El personal de soporte realizará las siguientes actividades, mismas que son de manera enunciativa, más no limitativa, por lo que el área técnica del Instituto FONACOT se reserva el derecho para solicitar funciones adicionales, las cuales se vinculen con el otorgamiento del servicio requerido en este anexo técnico:

Realizar la evaluación sobre los bienes o servicios afectados.
Proponer y ejecutar soluciones temporales conocidas o nuevas a fin de permitir la continuidad en las operaciones de los usuarios, en el menor tiempo posible.
Llevar a cabo las acciones pertinentes para solucionar los requerimientos, incluyendo la administración de garantías con terceros.
Documentar toda acción realizada en la atención de los requerimientos de acuerdo a las políticas y herramientas sistematizadas para la administración de los requerimientos que defina el área técnica del Instituto FONACOT.
Proporcionar, alimentar y/o actualizar la información pertinente para disponer de las bases de datos de conocimiento y de configuraciones del Instituto FONACOT, la cual se conformará de manera progresiva durante el servicio, incrementando la capacidad resolutiva de soporte.
Elaborar reportes de capacidad, disponibilidad, usabilidad, entre otros. El área técnica del Instituto FONACOT podrá solicitar cualquier información que considere pertinente relacionada con la prestación del servicio.
Realizar la instalación, configuración y puesta a punto de la infraestructura (hardware y software) involucrada en el servicio requerido, para la continuidad de servicios de TIC.
Ejecutar los cambios de políticas, permisos y configuraciones de infraestructura involucrada en el servicio requerido.
Administrar los activos de red para permitir la conectividad de equipos de computo y telefonos IP Instituciones.
Proporcionar el soporte para las conexiones tipo VPN site to site entre los equipos de seguridad proporcionados por el licitante ganador y un tercero. El suministro de los medios de comunicación (enlaces y líneas telefónicas) para acceso remoto no será responsabilidad del LICITANTE ganador
.
Proporcionar soporte especializado a usuarios que requieran la configuración de acceso a internet a través de la red inalámbrica del Instituto FONACOT en sus dispositivos móviles. El LICITANTE deberá considerar que el personal de soporte técnico asignado para estas actividades deberá ser especialista en al menos en los sistemas operativos IOS, Android, Windows Phone, entre otros.

EdP

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 5551 52 65 74 00 www.fonacot.gob.mx

Realizar las actividades para la instalación y configuración del software solicitado en este anexo.
Elaborar y ejecutar planes de trabajo, análisis, diagnóstico, pruebas y evaluación del impacto para atender un requerimiento que involucre la infraestructura considerada en el servicio, de conformidad a las políticas y procesos que defina el área técnica del Instituto FONACOT.

Supervisar el comportamiento de la infraestructura y analizar las tendencias de consumo de recursos de la infraestructura involucrada en el servicio requerido.
Efectuar y documentar las altas, bajas y cambios (ABC) de parámetros de usuarios, tales como filtros, políticas, reglas, permisos, configuraciones, entre otros dentro de la infraestructura involucrada en el servicio requerido.
Ejecutar las acciones para el respaldo y restauración de información y configuraciones de la infraestructura involucrada en el servicio requerido.
Realizar los trabajos de conexión y desconexión de componentes de cableado estructurado ya existente de acuerdo a los requerimientos del área técnica del Instituto FONACOT.
Realizar mantenimiento correctivo al cableado estructurado de acuerdo a los requerimientos del área técnica del Instituto FONACOT. Esto podrá incluir cambio de faceplates, jacks, ponchado de cable, etiquetado, escaneo, organización de cables, canalizaciones y ajustes en la fijación de rack y/o gabinetes automatizados.
Realizar la reubicación de equipo activo, componentes, charolas, barras de contactos, gabinetes, racks, organizadores y/o patch panel dentro de una misma oficina del Instituto FONACOT, esto podrá incluir, en los casos aplicables: la baja de servicios y aplicaciones, el apagado, desconexión/conexión, montaje/desmontaje, reacomodo del equipo, accesorios y dispositivos que integren cada bien.
Elaborar y/o actualizar la memoria técnica referente al cableado estructurado.
Habilitar/ Deshabilitar nodos de red en cualquier oficina del Instituto FONACOT.

.

Operar las herramientas y/o mecanismos de monitoreo provistos.
Realizar el monitoreo en un esquema de 7x24x365, considerando:

- Registro y seguimiento de las caídas, intermitencias y/o afectaciones de los activos involucrados en los servicios requeridos .
- Identificación y contención de actividades sospechosas confirmadas que se intenten filtrar hacia la red LAN o WAN vía local, Internet o VPN, por medio de los Firewalls involucrados en el servicio requerido.
- Definición en coordinación con el personal del área técnica del Instituto FONACOT la matriz de notificación de alertas y alarmas.

Como parte del soporte tecnico, el LICITANTE deberá considerar los siguientes puntos.

-

Realizar los servicios encaminados a solucionar cualquier incidente o problema que impida o degrade la operación normal de los activos o servicios objeto de este anexo.

- Las partes, componentes o refacciones que se utilicen para proveer el servicio deberán ser de la misma marca, tecnología y de características técnicas equivalentes o superiores a los originales, sin ningún costo adicional para la convocante, las cuales serán garantizadas por el LICITANTE ganador por un mínimo de 30 días naturales posterior a su instalación. La convocante se reserva el derecho de su aceptación cuando no sea posible contar con una pieza de tales características, lo cual debe acreditarse plenamente.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- o
- o En el caso de equipos ofrecidos en respaldo requieran de controladores o software específico para su funcionamiento, éstos deberán ser entregados por el LICITANTE ganador bajo su total responsabilidad observando las normas y leyes aplicables sobre derecho intelectual e industrial.
- o El LICITANTE ganador otorgará una garantía de hasta treinta días naturales posteriores al servicio proporcionado, aceptando su responsabilidad por las causas y efectos que se generen por omisión o vicios ocultos, entre otros.
- o En caso de que la reparación de los equipos amerite la salida del domicilio, el LICITANTE ganador asume la responsabilidad total por el aseguramiento y gastos asociados que se generen por el manejo, retiro, reintegro y traslados de los bienes relacionados con el otorgamiento del servicio.
- o Revisiones periódicas y planeación de capacidad para emitir recomendaciones de re-configuración.
- o Intermediación de administración con el licitante de acceso WAN.
- o Aislamiento de fallas relacionadas con la infraestructura involucrada en el otorgamiento del servicio .
- o Efectuar altas, bajas y cambios en la configuración lógica de los equipos de seguridad involucrados en el otorgamiento del servicio requerido, previo análisis de impacto. El tiempo para realizar las modificaciones será como máximo de 24 horas desde que se levanta la solicitud.
- o El LICITANTE ganador será responsable del control, mantenimiento y actualización de la memoria técnica de los equipos de seguridad involucrados en el otorgamiento del servicio requerido. Garantizar, en todo momento, que la memoria técnica se encuentre documentada y actualizada.

El soporte técnico se deberá otorgar considerando la siguiente cobertura:
Soporte para la atención y solución de requerimientos referentes a los equipos considerados en la infraestructura suministrada por el LICITANTE ganador: cubrirá un horario de operaciones de 7x24x365.

2.3.10. SERVICIOS BAJO DEMANDA

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

Los servicios que suministre el LICITANTE ganador bajo este concepto deberán cumplir con las características técnicas que se describen en este anexo técnico y estas se deberán tomar como referencia para el suministro de equipos y soluciones, considerando que en función al constante desarrollo tecnológico, los activos a entregar durante elperiodo que abarca el servicio, deberán ser provistos con caracteristicas iguales o supertiores, y que en ninguno de los casos deberán ser por debajo de las características técnicas establecidas en este anexo técnico, debiéndose proveer todas

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

las interfaces, cables de corriente, componentes, dispositivos, software operativo del hardware, drivers, etc., que permitan su adecuada operacion.

Para los servicios bajo demanda, se tomaran como referencia los costos unitarios presentados en la propuesta económica del LICITANTE ganador, independientemente de la fecha en que se solicite el servicio. El pago de este servicio se realizará mensualmente.

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

2.4. PLAN DE RETORNO

El LICITANTE ganador desarrollará un plan de retorno, mismo que será sujeto a revisiones del área técnica del Instituto FONACOT. El plan de retorno iniciará 30 dias naturales previos a la conclusion del contrato y deberá contener al menos los siguientes puntos:

- Integración de documentación técnica:
  - Documentación que describa la configuración de componentes de hardware y software relacionado con los servicios de este anexo
  - Documentación que describa la operación de procesos, respaldos, restauraciones y monitoreo de todos los componentes de infraestructura (hardware y software).
  - Diagrama de infraestructura (hardware y software)
  - Archivos de configuración.
  - Listado de usuarios y privilegios de todos los componentes de infraestructura (hardware y software).
- Como parte del Plan de Retorno el LICITANTE ganador se obliga a apoyar durante los 30 dias previos a la conclusion del contrato en la implementación y puesta a punto de todos los componentes de infraestructura (hardware y software) para continuidad del servicio ya sea por parte del Instituto FONACOT o de un nuevo prestador de servicio.

2.5. POLÍTICAS

El LICITANTE ganador se sujetará al marco normativo y mecanismos de control que el Instituto FONACOT defina para el seguimiento, aseguramiento de calidad y requerimientos de auditoría de los servicios, sin costo adicional para el Instituto FONACOT.

Para la administración y provisión de los servicios objeto del presente anexo técnico, el LICITANTE deberá apegarse a los modelos descritos en las normas ISO 20000 e ISO 27001. El área técnica del Instituto FONACOT se reserva el derecho de validar el cumplimiento de estos modelos, así como la infraestructura, documentación, procesos y prácticas involucradas con los servicios objeto del presente anexo técnico, por sí mismo o por medio de un tercero, con la frecuencia y profundidad que considere necesario, para lo cual el LICITANTE ganador se obliga a dar todas las facilidades y asignar los recursos que sean

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

necesarios. Para solventar las observaciones encontradas en las auditorias, el LICITANTE ganador entregará planes de trabajo detallados con las acciones correctivas y preventivas respectivas, el cumplimiento de estos planes de trabajo formará parte integrante de la evaluación de los servicios objeto del presente contrato. Si la auditoria pudiera afectar los niveles de servicio, la misma será planificada de común acuerdo entre el área técnica del Instituto FONACOT y el LICITANTE ganador.

El LICITANTE ganador se obliga a realizar la transferencia de conocimientos sobre la operación de los servicios materia de este anexo técnico. El Instituto FONACOT se reserva la facultad para que la transferencia de conocimientos se otorgue a personal propio del área técnica del Instituto FONACOT o de terceros.

2.6. GESTIÓN DEL SERVICIO.

El Instituto FONACOT ha adoptado modelos de gestión de servicios de tecnología (ISO 20000, ITIL), administración de proyectos (PMO) y seguridad de la información (ISO27001), por lo que el LICITANTE ganador deberá cuidar en todo momento que el modelo de gestión de los servicios esté alineado a los modelos de operación y procesos que se definan.

Será responsabilidad del LICITANTE ganador dar seguimiento al desempeño de los procesos que se describen a continuación.

2.6.1. ESCRITORIO DE SERVICIO.

El Instituto FONACOT cuenta con un Escritorio de Servicio, por medio del cual los usuarios realizan solicitudes relacionadas con los sistemas y servicios informáticos, los cuales son registrados, clasificados y asignados a grupos resolutores para la correspondiente solución, usando actualmente la herramienta Itop

A todo requerimiento registrado en el Escritorio de Servicio le corresponde un número de reporte. Los reportes se harán del conocimiento del personal del LICITANTE ganador a través dela herramienta del Escritorio de Servicio utilizada por el Instituto FONACOT. Cualquier gestión que realice el personal del LICITANTE ganador para la atención de los requerimientos, deberá ser registrada en el historial individual del reporte almacenado en dicha herramienta.

El Instituto FONACOT otorgará la transferencia de herramientas que permita al personal del LICITANTE ganador para interactuar con la herramienta del escritorio de servicio.

El LICITANTE ganador deberá proveer, con recursos propios, todas las herramientas de trabajo y logística que juzgue necesarias para el desempeño de su personal a fin de atender los requerimientos relacionados con la infraestructura involucrada con el otorgamiento de los servicios requeridos. El LICITANTE ganador proveerá al menos los siguientes recursos a su personal:

- Equipo de cómputo personal, accesorios y dispositivos periféricos.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Software base (Sistemas Operativos), aplicativos de creación y manejo de documentos, así como todas las licencias de uso respectivas para su uso. Es responsabilidad del LICITANTE ganador mantener actualizadas las PC´s o Lap tops en hardware y software de acuerdo a las actualizaciones que se realicen por parte del Instituto FONACOT en su infraestructura, a fin de mantener la compatibilidad operacional.

- Software antivirus y programas para detección y eliminación de "troyanos", "spywares", "back doors" y cualquier tipo de "malware", debidamente actualizado.

- Elementos de papelería y consumibles para los equipos de cómputo (papel, libretas, tóner para impresora, etc).

- Equipos de telefonía celular, radios trunking y cualquier otro medio de comunicación que el LICITANTE juzgue necesarios para la correcta operación de los distintos perfiles de trabajo. De manera obligada, al menos el 80% del personal del LICITANTE ganador para otorgar el servicio requerido en este anexo técnico, deberán de contar con dispositivos móviles.

- Servicio de mensajería, paquetería, valija, etc.

- Serán responsabilidad total del LICITANTE los gastos de traslados, alimentación y seguridad social que se generen por motivo del personal asignado para la prestación del servicio.

Las funciones que deberá considerar el LICITANTE ganador para interactuar con el Escritorio de Servicio del Instituto FONACOT son:

- El LICITANTE ganador deberá en conjunto con el área técnica del Instituto FONACOT definir una matriz de escalación, la cual contenga al menos la información de los contactos (nombre, perfil, nivel de escalación, teléfono oficina, teléfono móvil) para su localización en todo momento, así como los tiempos establecidos para su escalación. Por su parte, el área técnica del Instituto FONACOT proporcionará una matriz de escalación de contactos y responsables de la administración del servicio a fin de coordinar la restauración de los servicios. Dichos niveles de escalación serán configurados en la herramienta del Instituto FONACOT.
- Registrar los avances, el tipo de fallas presentadas y la forma como se solucionaron, en la herramienta del Instituto FONACOT.

2.6.2. ADMINISTRACIÓN DE INCIDENTES

El objetivo de la administración de incidentes es restablecer lo antes posible la operación normal del servicio, minimizar el impacto negativo sobre las operaciones del negocio, así como asegurarse de que se mantiene el mejor nivel de servicio posible, la mejor calidad y disponibilidad, en función a los niveles de servicio descritos en este anexo técnico.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

2.6.3. ADMINISTRACIÓN DE PROBLEMAS

El LICITANTE ganador a través del proceso de Administración de Problemas reducirá el número y la severidad de los incidentes y problemas alrededor de la infraestructura involucrada en el otorgamiento del servicio, identificando la causa que los originan (conocer el error), documentando la solución y generando las acciones necesarias (como solicitudes de cambio) para evitar que vuelvan a ocurrir.

El LICITANTE ganador realizará actividades para alimentar la Base de Datos de Conocimiento (KDB – Knowledge Data Base) del Instituto FONACOT. En esta Base de Datos se deberán almacenar de manera estructurada las soluciones, procedimientos, resoluciones temporales (WA – Workaround), etc; y estará disponible para facilitar la atención y resolución de las eventualidades que ocurran en la infraestructura relacionada con los servicios proporcionados. El área técnica del Instituto FONACOT, proporcionara al LICITANTE ganador el procedimiento para acceder a la Base de Datos de Conocimiento.

2.6.4. ADMINISTRACIÓN Y CAMBIOS DE LA CONFIGURACIÓN

El LICITANTE ganador deberá llevar a cabo las actividades relacionadas con cambios sobre la infraestructura y servicios, considerando, por lo menos, lo siguiente:

- Coordinar procesos y procedimientos para todos los cambios, diferenciando los cambios estándar (cambios sin mayor impacto que puedan realizarse sin análisis de impacto previo) y los cambios de impacto (RFCh, aquéllos que por el nivel de impacto deban ser analizados previo a su implantación).
- Identificar los prerrequisitos para los cambios estándar.
- Preparar análisis de impacto, plan de trabajo para implementación (señalando las relaciones y tareas de otras áreas y/o proveedores del Instituto FONACOT, así como fechas propuestas para la ejecución), beneficios del cambio, los riesgos de no efectuarlo, a fin de presentarlo para aprobación por parte del área técnica del Instituto FONACOT y en su caso atender las recomendaciones resultantes. Como parte del plan de trabajo el LICITANTE ganador deberá prever los ajustes a políticas, procedimientos, memorias técnicas, planes de transferencia de conocimientos (si fuera necesario), así como planes de retorno en caso de fallas.
- El LICITANTE será responsable de operar, controlar y mantener el control de activos requeridos para los diferentes ambientes de servicio, conservando un control de versiones sobre los cambios realizados a la infraestructura (hardware y software) así como de sus configuraciones, mismas que se mantendrán documentadas en CMDB de la herramienta del Escritorio de Servicio del Instituto FONACOT.

2.6.5.SERVICIOS DE COORDINACIÓN.

Para realizar la coordinación y seguimiento de las actividades referentes a los servicios requeridos en este anexo técnico, el LICITANTE ganador deberá asignar al menos una persona, de acuerdo con los siguientes términos:
Perfil requerido del Coordinador:

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 05 74 00 www.fonacot.gob.mx

- Estudios concluidos a nivel licenciatura. Se deberá presentar en la propuesta técnica copia de la cédula profesional o titulo profesional que avale esta situación.
- Certificado en ITIL V3 nivel Intermediate en operation support and analysis (OSA) o service operation (SO), Se deberá presentar en la propuesta técnica copia y original del certificado correspondiente para cotejo. Si durante la vigencia del contrato se liberara una o más versiones de ITIL, se deberá actualizar al personal asignado para cubrir este perfil.
- Experiencia mínima de tres años como responsable de la administración de servicios de TIC. Se deberá presentar en la propuesta técnica copia del currículo vitae donde se muestren los siguientes puntos:
    - Nombre(s) y apellido(s)
    - Nivel de estudios
    - Experiencia mínima de 3 años como responsable de la administración de servicios de TIC a través del desempeño del rol de Director o Gerente de Proyecto similar al solicitado.
    - Antigüedad y puesto de trabajo dentro de la empresa
    - Proyectos en los que ha participado
    - Carta de al menos un cliente firmada por el responsable del proyecto, avalando que dicho personal ha demostrado contar con la capacidad técnica para proporcionar servicios similares a los solicitados y desempeñado el rol de Director o Gerente de Proyecto.
    - Copia legible de identificación oficial.
    - El Curriculo debera venir firmado por el personal propuesto.

Se deberá acreditar que el personal propuesto es parte de la plantilla contratada por el LICITANTE, por lo tanto, se debe de presentar el alta ante el IMSS.

- Certificación vigente como Project Management Professional, emitida por el Project Management Institute (PMI) Se deberá presentar en la propuesta técnica copia y original (para su cotejo) del certificado que avale esta situación.

El personal con este perfil deberá realizar al menos las siguientes funciones, por lo que el área técnica del Instituto FONACOT se reserva el derecho para solicitar funciones adicionales, las cuales se vinculen con el otorgamiento del servicio requerido en este anexo técnico:

- Asegurar el adecuado cumplimiento en el otorgamiento del servicio requerido.
- Verificar el cumplimiento de los niveles de servicio establecidos en esta convocatoria.
- Elaborar y presentar los RFCh para su aprobación, de conformidad a las políticas y procedimientos que establezca el Instituto FONACOT.
- Establecer la comunicación entre todas y cada una de las partes involucradas en la atención de los requerimientos.
- Ser el enlace con el Instituto FONACOT para el seguimiento de los requerimientos que se soliciten durante la vigencia del contrato.
- Elaborar o gestionar procedimientos operativos, scripts para registro de requerimientos, reportes o informes, a fin de atender los requerimientos involucrados en el servicio.

Av. Insurgentes Sur 452 Col. Roma Sur, D.F. Cuauhtemoc, C.P. 06760, Mexico D.F
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- Proponer medidas y mecanismos de mejora continua para el otorgamiento de los servicios de TIC y la atención de requerimientos.
- Elaborar y/o actualizar la documentación relativa a la prestación del servicio.
- Cumplir con las políticas y procedimientos autorizados por el Instituto FONACOT.
- Participar en las reuniones de trabajo que convoque el Instituto FONACOT.
- Elaborar procesos y procedimientos operativos.
- Mantener actualizado el control de activos de la infraestructura involucrada en los servicios requeridos, considerando al menos los siguientes puntos:
    - Ubicación.
    - Tipo de Equipo.
    - Marca.
    - Descripción.
    - Números de serie.
    - Responsable.
    - Fecha en que se entrega a la Entidad.
    - Fecha de baja de las instalaciones de la Entidad.
    - Modelo.

Este personal cubrirá un horario de 9:00 a 18:00 horas de lunes a viernes de forma remota De conformidad a las necesidades del Instituto FONACOT se podrá requerir la asistencia de este personal. Las funciones del personal con perfil de Coordinador se valuarán con base en el cumplimiento de proyectos que sean requeridos por el Instituto FONACOT, los cuales pueden recaer en las esferas de acción o responsabilidad del mismo coordinador o del personal para el soporte técnico. Para el seguimiento de estos proyectos se tomará como base la documentación referencial que avale la conclusión de los proyectos.

2.7. ASPECTOS GENERALES

La infraestructura que suministre el LICITANTE ganador para proporcionar los servicios solicitados deberá cumplir con las características técnicas solicitadas.

La entrega al destino final de los equipos es de la total responsabilidad del LICITANTE ganador, los costos que se generen con motivo de la entrega del equipo corren por cuenta del LICITANTE ganador, por lo que éste asume la responsabilidad total por el aseguramiento y gastos asociados que se generen por el manejo y traslados de los activos que se suministren con motivo de los servicios requeridos.

El licenciamiento Microsoft que se requiera para la operación de los servicios solicitados en este anexo técnico será proporcionado por el área técnica del Instituto FONACOT.

Toda documentación entregable, deberá apegarse a los formatos, metodologías y lineamientos que definirá el área técnica del Instituto FONACOT con el LICITANTE ganador.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 05 73 00 www.fonacot.gob.mx

3. MANUALES, CATALOGOS Y FOLLETOS

El LICITANTE deberá entregar 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 este Anexo Técnico.

El LICITANTE deberá entregar 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 inglés.
- Información impresa obtenida de Internet, la cual incluya la dirección URL en idioma español o inglés

4. PATENTES, MARCAS Y DERECHOS

Con fundamento en lo dispuesto en la Ley Federal del Derecho de Autor y en virtud de la naturaleza de los servicios requeridos por el Instituto FONACOT, el LICITANTE está de acuerdo en que al Instituto FONACOT le corresponde la propiedad de los documentos, respaldos, scripts, archivos de configuración e información que se requiera para la prestación de los servicios objeto del presente anexo.

El LICITANTE asume la responsabilidad total en caso de que al proporcionar los servicios materia de este anexo, infrinjan derechos de propiedad intelectual e industrial de terceros sobre patentes, marcas y derechos de autor, entre otros, por lo que el LICITANTE se obliga y acepta eximir al Instituto FONACOT de cualquier responsabilidad civil o penal.

5. MUESTRAS

NO APLICA

6. PRUEBAS Y DESARROLLO A EFECTUAR A LAS MUESTRAS

NO APLICA

7. LUGAR, PLAZO Y HORARIO DE LA PRESTACIÓN DEL SERVICIO

El plazo del servicio sera del 01 de julio al 31 de diciembre de 2022.

El servicio se deberá otorgar considerando las siguientes ubicaciones y coberturas:

- El horario para la prestación de los servicios para los edificios que se ubican en los edificios de Insurgentes Sur, Plaza de la Republica será de 8:00 a 21:00 horas de lunes a viernes y de 8:00 a 17:00 hrs, sábados de forma remota
- El horario para la prestación de los servicios para los edificios que se ubican en las Direcciones Regionales, Estatales, Plaza, Modúlos y/o Representaciones será de 8:00 a 20:00 horas de lunes a viernes hora local y de 8:00 a 17:00 hrs, también hora local.

Los horarios antes descritos pueden varia conforme a las necesidades del Instituto FONACOT.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

Los domicilios de las ubicaciones antes descritas, se detallan en el Anexo "Domicilios"

8. PLAZO PARA LA SUSPENSIÓN DEL SERVICIO

El plazo para la suspensión del servicio será de 10 días naturales. 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.

9. PAGO

Con fundamento en el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, los pagos del servicio se realizarán en moneda nacional dentro de los 20 días naturales posteriores posteriores a la presentación del Comprobante Fiscal Digital por Internet CFDI (factura electrónica impresa y archivo XML) y previa validación y aceptación de la misma, por parte por el Administrador del Contrato o persona autorizado por este, de la Subdirección General de Tecnología de la Información y Comunicación conforme a sus respectivas responsabilidades y recibidos los servicios a entera satisfacción del Administrador del contrato, a fin de proceder con el pago vía transferencia electrónica.

El pago de los servicios se realizara mensualmente, considerando meses calendario por lo servicios efectivamente devengados.

Las facturas electrónicas (formato CFDI, PDF y su archivo .XML), deberán cumplir con los requisitos fiscales vigentes, en moneda nacional, la cual deberá ser enviada a la dirección de correo electrónico del Administrador del contrato horacio.sanchez@fonacot.gob.mx.

10. ENTREGABLES

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

Los entregables, incluye los siguientes puntos, no obstante, el área técnica del Instituto FONACOT se reserva el derecho para solicitar reportes adicionales, las cuales se vinculen con el otorgamiento del servicio requerido en este anexo técnico.

10.1. ENTREGABLES INICIALES

Entregable	Descripción	Periodo de entrega
Memoria Técnica	Descripción detallada la implementación y parametrización de cada uno de los servicios base de este anexo técnico.	Maximo los 30 días hábiles posteriores a la conclusión de la implementación

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 65 72 00 www.fonacot.gob.mx

		de todos los servicios
Cartas de entrega / recepción de servicios	El LICITANTE ganador deberá entregar documento en hoja membretada y firmada por el administrador del contrato por parte del LICITANTE, con la descripción de la infraestructura puesta a punto de cada uno de los servicios. Y fecha de su liberación	Maximo a los 5 días hábiles posteriores a la liberación de cada servicio.

10.2. ENTREGABLES MENSUALES

Durante los primeros cinco días hábiles de cada mes, el LICITANTE deberá entregar los reportes con la Información Soporte para el pago de la Factura correspondientes al mes vencido anterior.

Servicios	Reporte	Periodo de Entrega
La información corresponderá en cada caso al servicio que aplique, el área técnica del instituto FONACOT se reserva el derecho para solicitar reporte adicionales, los cuales se vinculen con el otorgamiento del servicio requerido en este anexo técnico	• Graficas de Disponibilidad, Capacidad de infraestructura por servicio. • Resumen ejecutivo de del estatus de los diferentes reportes registrados en la Mesa de Servicio • Inventario de infraestructura (Actualización DMDB) • Reporte Ejecutivo de las actividades relevantes realizadas durante el mes por servicio. • Reporte de respaldos realizados • Alarmas y Logs en Infraestructura instalada que presenten fallas o inconsistencias • Desempeño Servidores: CPU, Memoria, Disco Duro • Reporte ejecutivo de la capacidad de espacio de almacenamiento ocupado por los distintos servicios. • Memorias técnicas de cableado • Planes de trabajo de proyectos ejecutados • Tabla de Resumen de Pagos • Resumen de Infraestructura Solicitada bajo demanda • Reporte de Disponibilidad de Servicios Bajo Demanda •	Durante los 5 días hábiles posteriores al mes vencido

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

En caso de incumplimiento a cualquiera de los entregables antes señalados, se aplicarán las penas convencionales a que haya lugar.

10.3. ENTREGABLES FINALES

10.3.1.Memoria técnica

Previo a la finalización del servicio deberá entregar con 30 días naturales previos al término del contrato, el LICITANTE ganador se obliga a entregar al área técnica del Instituto FONACOT el Plan de Retorno con al menos la siguiente información:

a. Documentación que describa la configuración de componentes de hardware y software relacionado con los servicios de este anexo
b. Documentación que describa la operación de procesos, respaldos, restauraciones y monitoreo de todos los componentes de infraestructura (hardware y software).
c. Diagrama de infraestructura (hardware y software) y archivos de configuración correspondientes.
d. Listado de usuarios y privilegios de todos los componentes de infraestructura (hardware y software).
e. Análisis de capacidad (Capacity Planning) de todos los componentes de infraestructura (hardware y software).
f. Manuales de gestión del servicio.
g. Plan de trabajo para el retiro de toda la infraestructura propiedad del LICITANTE, considerando iniciar a partir del siguiente dia natural posterior a la conclusion del contrato.
h. Proceso del borrado seguro de la infraestructura involucrada en el otorgamiento del servicio.
i. Apoyar en la implementación y puesta a punto de todos los componentes de infraestructura (hardware y software) para continuidad del servicio por parte del Instituto FONACOT o de un nuevo licitante del servicio.

11. NIVELES DE SERVICIO

El LICITANTE ganador deberá cumplir con los siguientes niveles de servicio siendo estos aplicables a los servicios que a continuación se detallan, se puntualiza que no se consideraran prorrogas para la entrega de algún servicio, por retrasos imputables a terceros.

11.1. INICIO DE OPERACIONES

- A partir del siguiente dia natural del fallo, el LICITANTE deberá iniciar operaciones considerando los siguientes alcances:
  - Asignación de personal con perfil de Coordinador conforme a lo establecido en el punto SERVICIOS DE COORDINACION.
  - Asignación de personal con perfil de soporte técnico conforme a lo establecido en el punto SOPORTE TECNICO.

11.2. PUESTA A PUNTO DEL SERVICIO INTEGRAL ADMINISTRADO

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel.: 55) 52 05 74 00 www.fonacot.gob.mx

- Máximo a los 15 días naturales posteriores a la notificacion de fallo, el LICITANTE ganador deberá concluir la implementacion y puesta a punto de los siguientes servicios:
  - Monitoreo de infraestructura.
  - Switches de acceso.
  - Servicio de red inalámbrica en edificios Sede.
  - Servicio de red inalámbrica en localidades
  - Archivos compartidos en red
  - Filtrado de contenidos web
  - Herramienta de administración de la red.
  - Esquema de alta disponibilidad Tipo A.
  - Esquema de alta disponibilidad Tipo B.
  - Servicio de administración de energía regulada (UPS).

Es responsabilidad del licitante ganador mantener la continuidad de los servicios durante el periodo de implementacion y puesta a punto de los nuevos servicios.

Los servicios no especificados en este rubro, se realizarán bajo demanda específica del administrador del contrato del Instituto FONACOT, por lo que los niveles de servicio para la puesta a punto en producción, o migración en su caso, se definirán con base en un plan de trabajo entregado por el LICITANTE ganador, mismo que deberá ser aprobado por el área técnica del Instituto FONACOT.

11.3. CABLEADO ESTRUCTURADO

El LICITANTE ganador será responsable de atender los requerimientos de cableado estructurado, conforme a los tiempos que se indican en la siguiente tabla:

Cableado estructurado	Tiempo de atención
-Instalación de nodos nuevos. -Reubicación de nodos existentes. -Instalación de Fibra Óptica. -Mantenimiento de nodos de red	6 horas dentro del horario de labores del Instituto FONACOT, para oficinas centrales, sede alterna y localidades metropolitanas 12 horas dentro del horario de labores del Instituto FONACOT. Para las localidades foráneas ,

Los tiempos de atención para los servicios de cableado estructurado consideran cualquier actividad necesaria para que el LICITANTE ganador proporcione un plan de actividades que establezca el tiempo de solución, mismo que deberá ser aceptado por el área técnica.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

11.4. SERVICIOS BAJO DEMANDA

El LICITANTE ganador dispondrá máximo de 30 días hábiles a partir de la solicitud expresa del administrador del contrato para la puesta a punto de los servicios bajo demanda que se requieran.

11.5. INCIDENTES POR FALLAS

El LICITANTE será responsable de solucionar los incidentes que por cualquier causa genere la interrupción de los servicios informáticos o imposibilite la operación de algún equipo contenido en los servicios solicitados en este anexo técnico.
El LICITANTE dispondrá de los siguientes tiempos para la solución de incidentes:

Prioridad	Descripción	Tiempo de solución
Alta	Servicios : Contención perimetral. Monitoreo de infraestructura. Filtrado de contenidos web Archivos compartidos en red.	4 horas.
	Equipos: Firewalls. Switches principales (CORE TIPO A Y B). Switches de acceso. Red inalámbrica. Energía regulada (UPS.)	2 horas para equipo operando en Oficinas Centrales y Plaza de la República. 4 horas para equipo operando en localidades metropolitanas dentro del horario de labores del Instituto FONACOT. 8 horas para equipo operando en las localidades foráneas dentro del horario de labores del Instituto FONACOT.
Media	Servicios:	6 horas dentro del horario de labores del Instituto FONACOT.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

Prioridad	Descripción	Tiempo de solución
	Herramientas de administración de la red. .	
	Equipos: Energía regulada (UPS.)	4 horas para equipo operando en oficinas centrales y sede alterna, dentro del horario de labores del Instituto FONACOT 6 horas para equipo operando en localidades metropolitanas dentro del horario de labores del Instituto FONACOT. 8 horas para equipo operando en las localidades foráneas, dentro del horario de labores del Instituto FONACOT.

Los tiempos de solución consideran cualquier acción que requiera realizar el LICITANTE ganador para restablecer la operación normal del servicio o equipo correspondiente, incluyendo el suministro de equipos de respaldo.

El tiempo de solución, comienza a contabilizarse a partir de que el personal de soporte técnico recibe la notificación a través de la herramienta del escritorio de servicio del Instituto FONACOT.

11.6. Cambios Estándar

Prioridad	Ventana de servicio	Tiempo de solución
Alta	8:00 a 21:00 horas de lunes a viernes y de 8:00 a las 17:00 horas los sábados y domingos.	20 minutos
Media	8:00 a 21:00 horas de lunes a viernes y de 8:00 a las 17:00 horas los sábados y domingos.	60 minutos

Tiempo de solución, es el tiempo que transcurre desde que el personal de soporte técnico recibe a través de la herramienta del escritorio de servicio del Instituto FONACOT la solicitud y la solución, quede debidamente documentada en dicha herramienta.

Los cambios estándares se definirán de manera conjunta entre el LICITANTE ganador y el personal técnico del Instituto FONACOT considerando que la prioridad se determinara por

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

el tipo de servicio. Los acuerdos podrán ser revisados y modificados en el momento que estime pertinente el área técnica del Instituto FONACOT.

El LICITANTE ganador se obligará a cumplir con los Acuerdos de Nivel Operacional (OLA´s) que se lleguen a definir durante la vigencia del contrato con la finalidad de asegurar la continuidad de los servicios informáticos y su otorgamiento de conformidad con los niveles de servicio establecidos. Los OLA´s se podrán celebrar entre el LICITANTE ganador, el área técnica del Instituto FONACOT y otros proveedores de TIC que designe el Instituto FONACOT, definiendo los niveles de operación que entre ellos deben ofrecerse; se deberá tomar como punto de partida los esquemas operativos, los procesos formalizados y las fronteras de responsabilidad que de ellos derivan. El área técnica del Instituto FONACOT se reserva el derecho de realizar modificaciones de los OLA´s, de emitir su aprobación y de solicitar su actualización en caso de que así lo considere necesario. El cumplimiento de estos acuerdos será exclusiva responsabilidad del LICITANTE ganador y de los otros proveedores y no eximirán de las penalizaciones y deducciones a que haya lugar.

11.7. Solicitud de Cambio (RFCh)

Los RFCh se evaluarán con base en los tiempos establecidos en el plan de trabajo que haya sido previamente autorizado por el personal técnico del Instituto FONACOT. Su seguimiento se otorgará con base en la "Solicitud de Cambio (RFCh)" y la documentación referencial que avale la conclusión de los cambios aprobados por el área técnica del Instituto FONACOT.

12. GARANTÍA DE CUMPLIMIENTO DEL CONTRATO

Conforme a los artículos 48 fracción II y 49 Fracción II de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 103 de su Reglamento, el LICITANTE ganador deberá garantizar mediante fianza expedida por institución mexicana autorizada legalmente para ello, el fiel y exacto cumplimiento del contrato, por un importe del 10% (diez por ciento) del monto total máximo del ejercicio fiscal correspondiente, sin considerar el Impuesto al Valor Agregado, ésta deberá expedirse a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores (Instituto FONACOT) y entregarse en la Dirección de Recursos Materiales y Servicios Generales, a más tardar dentro de los diez días naturales posteriores a la firma del contrato, la no entrega de la garantía será motivo de recisión del contrato.

13. GARANTÍA DE RESPONSABILIDAD CIVIL

El LICITANTE ganador se obliga a proporcionar al administrador del contrato la póliza expedida por institución autorizada por las Leyes Mexicanas a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores, por un importe mínimo de $1,000,000.00 (Un millón de pesos 00/100 M.N.) que garantice la protección de daños y perjuicios que pudieran presentarse como resultado de las actividades propias del LICITANTE ganador por la ejecución de los servicios que se contraten derivados del presente contrato, la cual deberá ser entregada dentro de los 4 días hábiles siguientes a la emisión del Fallo correspondiente.

14. PENA CONVENCIONAL Y DEDUCTIVA

14.1. PENA CONVENCIONAL

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

En términos de lo previsto por los artículos 53 de **La Ley**, 95 y 96 de **El Reglamento**, el Instituto FONACOT, según corresponda aplicará al LICITANTE ganador las penas convencionales por cada día natural de atraso en el incumplimiento de las siguientes obligaciones:

14.1.1. INICIO DE OPERACIONES

Asignación de personal con perfil de Coordinador conforme a lo establecido en el punto SERVICIOS DE COORDINACION.
Asignación de personal con perfil de soporte técnico conforme a lo establecido en el punto SOPORTE TECNICO para la administración de los servicios informáticos que se encuentran en operación en el Instituto FONACOT.

Considerando que el no contar con personal con perfil de coordinación y soporte técnico afectaría el inicio de operaciones del servicio, se aplicará una pena convencional por causa imputable al LICITANTE ganador, del 1% por cada día de atraso sobre el monto total del contrato considerando el costo señalado en la propuesta económica.

14.1.2. PUESTA A PUNTO DEL SERVICIO INTEGRAL ADMINISTRADO

- Switches de acceso.
- Servicio de red inalámbrica en edificio Sede.
- Servicio de red inalámbrica en localidades.
- Esquema de alta disponibilidad Tipo A.
- Esquema de alta disponibilidad Tipo B

Por atraso imputable al LICITANTE ganador en la puesta a punto de los servicios antes mencionados, se aplicará una pena convencional del 3% por cada día de atraso sobre el costo total mensual del servicio correspondiente, considerando los costos señalados en la propuesta económica.

- Archivos Compartidos en Red.

- Filtrado de contenidos Web.

Por atraso imputable al LICITANTE ganador en la puesta a punto de los servicios anteriores, se aplicará una pena convencional del 10% por cada día de atraso sobre el costo total mensual del servicio correspondiente, considerando los costos señalados en la propuesta económica.

- Herramienta de administración de la red.
- Servicio de administración de energía regulada (UPS).

Por atraso imputable al LICITANTE ganador en la puesta a punto de los servicios anteriores, se aplicará una pena convencional del 5% por cada día de atraso sobre el costo total

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

mensual del servicio correspondiente, considerando los costos señalados en la propuesta económica.

- Cableado estructurado
  - Por atraso imputable al LICITANTE ganador en la entrega del plan de actividades, se aplicará una pena convencional del 3% por cada día de atraso sobre el costo total de la cantidad de nodos solicitados en el requerimiento.
  - Por atraso imputable al LICITANTE ganador en los tiempos establecidos en el plan de actividades que haya sido previamente autorizado por el personal técnico del Instituto FONACOT, se aplicará una pena convencional del 5% por cada día de atraso sobre el costo total de la cantidad de nodos solicitados en el requerimiento
- Servicio bajo demanda.

  Por atraso imputable al LICITANTE ganador en la puesta a punto del servicio bajo demanda, se aplicará una pena convencional del 10% por cada día de atraso sobre el costo unitario correspondiente, tomando en consideración los costos establecidos en su propuesta económica.

- Solicitud de Cambio (RFCh).

Por atraso imputable al LICITANTE ganador, en el cumplimiento del plan de trabajo autorizado por el personal técnico del Instituto FONACOT, se aplicará una pena convencional del 1% diario sobre el costo mensual del servicio Soporte Tecnivo, considerando el costo señalado en la propuesta económica.

14.1.3. SERCVICIO O EQUIPOS NO OTORGADOS

Cuando el servicio o el equipo no sea otorgado por causas imputables al LICITANTE ganador, no procederá pago alguno, asimismo, se aplicará una pena convencional del 5% por cada día de atraso del costo mensual del servicio, considerando los costos en la propuesta económica por los conceptos o bienes involucrados.

El pago, quedará condicionado, proporcionalmente, al pago y/o deducción que el prestador de servicio deba efectuar por concepto de penas convencionales mediante pago en efectivo o con cheque certificado en la caja del inmueble ubicado en Avenida Insurgentes Sur No. 452 planta baja, Col Roma Sur, Delegación Cuauhtémoc, C.P. 06760, CDMX., la que emitirá el recibo correspondiente, en el entendido de que en el supuesto que sea rescindido el contrato, no procederá el cobro de dicha penalización, ni la contabilización de la misma para hacer efectiva la garantía de cumplimiento del contrato. Lo anterior, sin perjuicio del derecho de que la Convocante pueda optar entre exigir el cumplimiento del contrato o rescindirlo, de conformidad a lo establecido en el Artículo 54 de **La Ley**.

Para el pago de las penas convencionales, la Convocante informará por escrito al prestador de servicio el cálculo de la pena convencional correspondiente, indicando el número de días de atraso, así como la base para su cálculo y el monto a que se hizo acreedor.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. 4551 52 65 74 00 www.fonacot.gob.mx

Para efectuar este pago, el prestador de servicio 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.

La acumulación de dichas penas no excederá del importe de la garantía del cumplimiento del contrato, es decir del 10% (diez por ciento) antes de I.V.A., de conformidad con el Artículo 53 de **La Ley** y 96 de **El Reglamento**.

14.2. DEDUCTIVAS.

En los términos de lo previsto en el artículo 53 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el área técnica del Instituto FONACOT aplicará al LICITANTE ganador las deducciones a los conceptos del servicio que en su caso presenten deficiencias.

Disponibilidad de servicios.

La siguiente tabla muestra los porcentajes de deducción que se aplicarán sobre el costo mensual de los servicios correspondientes señalados en la propuesta económica:

Calidad de Servicios Lograda (Disponibilidad)		
Límite inferior	**Limite Superior**	**Porcentaje de la mensualidad a retener como deducción**
99.7%	100%	0%
99.3%	99.6999%	5%
99.1%	99.2999%	10%
98.9%	99.0999%	15%
98.7%	98.8999%	20%
98.5%	98.6999%	25%
98.3%	98.4999%	30%
98.1%	98.2999%	35%
97.9%	98.0999%	40%
97.7%	97.8999%	45%

D= Porcentaje de disponibilidad durante el periodo.

El área técnica del Instituto FONACOT considerará de forma mensual la disponibilidad (D) de los servicios contemplando los tiempos establecidos en las coberturas limitada o amplia (TC) y Tiempos Fuera (TF) acumulados de acuerdo a la siguiente fórmula:

$$D = \frac{(TC - TF) \times 100}{TC}$$

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

Por falta de disponibilidad de un servicio que afecte u ocasione indisponibilidad o degradación de más servicios, se aplicara la deductiva correspondiente por cada uno de los servicios afectados o inaccesibles

Incidentes por fallas

La siguiente tabla muestra los porcentajes de deducción que se aplicarán sobre el costo total mensual del servicio Soporte Técnico considerando los costos señalados en la propuesta económica.

Calidad de Servicios Lograda (Cambio Estándar)		
Límite inferior	**Limite Superior**	**Porcentaje de deducción**
97%	100%	0%
94%	96.999%	10%
91%	93.999%	15%
88% o menor	90.999%	20%

El área técnica del Instituto FONACOT considerará la siguiente fórmula para obtener el porcentaje de deducción mensual relacionado con la solución de incidentes por fallas que se encuentren fuera del nivel de servicio solicitado.

$$D = \frac{(ST - SF) \times 100}{ST}$$

D= Deducción.
ST= Solicitudes totales mensuales
SF= Solicitudes totales mensuales fuera de nivel de servicio

Cambios Estándar.

La siguiente tabla muestra los porcentajes de deducción que se aplicarán sobre el costo total mensual del servicio Soporte Técnico considerando los costos señalados en la propuesta económica

Calidad de Servicios Lograda (Cambio Estándar)		
Límite inferior	**Limite Superior**	**Porcentaje de deducción**
97%	100%	0%
94%	96.999%	10%
91%	93.999%	15%
88% o menor	90.999%	20%

El área técnica del Instituto FONACOT considerará la siguiente fórmula para obtener el porcentaje de deducción mensual relacionado con las solicitudes de cambios estándar que se encuentren fuera del nivel de servicio solicitado.

$$D = \frac{(ST - SF) \times 100}{ST}$$

D= Deducción.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

ST= Solicitudes totales mensuales
SF= Solicitudes totales mensuales fuera de nivel de servicio

15. NORMAS APLICABLES

Normas de redes

UL 60950-1, CAN/CSA C22.2, No. 60950-1, FCC 47 CFR Part 15 (Class A), ICES-003 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZ CISPR-22 (Class A)

Normas para firewall

CE, CB, FCC, UL/cUL, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, CVE Compatibility, IPv6 Ready, ICSA Firewalls.

Normas UPS

CSA, FCC part 15 class A,
UL1778

Actualmente el Instituto cuenta con procesos y funciones base para la administración de servicios de TI, según el marco de mejores prácticas de ITIL (Information Technology Infrastructure Library por sus siglas en ingles), y en proceso de implementación del MGSI (Marco de Gestión de Seguridad de la Información), por lo que el LICITANTE deberá reflejar dicha experiencia en el currículum de su empresa en el "soporte al servicio" , "entrega del servicio" y "seguridad de la Información" fundamentado cuando menos en estos estándares en proyectos similares. Lo anterior con objeto de facilitar la adaptación de estos y contribuir con la transferencia de conocimientos y prácticas al Instituto.

El LICITANTE ganador deberá implementar y administrar los servicios de este anexo técnico basado en las normas del punto anterior para mantener la confidencialidad, integridad y disponibilidad de la infomación en los servicios y bloquear toda aquella actividad o flujo ajeno o perjudicial para el Instituto FONACOT como de sus empleados y colaboradores.

Para la administración y provisión de los servicios objeto del presente anexo técnico, el LICITANTE deberá adoptar los modelos descritos en las normas ISO 20000 e ISO 27001. El Instituto FONACOT se reserva el derecho de auditar el cumplimiento de estos modelos, así como la infraestructura, documentación, procesos y prácticas involucradas con los servicios objeto de la presente licitación, por sí mismo o por medio de un tercero, con la frecuencia y profundidad que considere necesario, para lo cual el LICITANTE ganador se obliga a dar todas las facilidades y asignar los recursos que sean necesarios. Para solventar las observaciones encontradas en las auditorias, el LICITANTE ganador entregará planes de trabajo detallados con las acciones correctivas y preventivas respectivas, el cumplimiento de estos planes de trabajo formará parte integrante de la evaluación de los servicios objeto del presente contrato. Si la auditoria pudiera afectar los niveles de servicio, la misma será planificada de común acuerdo entre el Instituto FONACOT y el LICITANTE ganador.

16. CONFIDENCIALIDAD

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

El LICITANTE ganador se sujetará al marco normativo y mecanismos de control que el Instituto FONACOT defina para el seguimiento, aseguramiento de calidad y requerimientos de auditoría de los servicios, sin costo adicional para el Instituto FONACOT.

El LICITANTE ganador se obliga a guardar bajo términos de confidencialidad y reserva la información de la cual pueda tomar conocimiento con relación a las operaciones, actividades o negocios del Instituto FONACOT o cualquier otra que estuviera a su alcance como resultado del otorgamiento del servicio requerido; por lo que el LICITANTE ganador se obliga asimismo y a su personal, a cumplir con las condiciones establecidas en el Anexo "Confidencialidad", mismo que se deberá incluir en la propuesta técnica debidamente firmada por el representante legal del LICITANTE ganador.

Toda la documentación que con motivo de la prestación de los servicios, el Instituto FONACOT entregue al LICITANTE ganador, así como toda la información que el LICITANTE ganador 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 Propiedad Industrial, debiendo 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.

17. ADMINISTRADOR DEL CONTRATO

De acuerdo a lo establecido en el penúltimo párrafo del artículo 84 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el Mtro. Horacio Sánchez Tinoco, Subdirector General de Tecnología de la Información y Comunicación, será el responsable de administrar y verificar el cumplimiento del contrato.

17.1. MODIFICACIONES QUE SE RESERVA EL ADMINISTRADOR DEL CONTRATO

De conformidad a las estrategias y necesidades operacionales, el administrador del contrato del Instituto FONACOT se reserva los siguientes derechos sobre los objetos considerados en el servicio requerido en el presente Anexo técnico:
Modificación de la base instalada de hardware y software:

- La modificación de base instalada se refiere a sustituir un activo considerado en el presente Anexo técnico, por algún otro bien de características similares o superiores. Lo anterior, con la finalidad de que este último sea considerado como objeto de los servicios requeridos en este anexo técnico.
- La sustitución será a petición expresa del administrador del contrato del Instituto FONACOT. No se considerará ninguna modificación en los costos unitarios en la facturación por este concepto.
- En el caso de que la modificación signifique disminución en la cantidad de equipos, se considerarán los descuentos respectivos en la factura del mes vencido, tomando como base los costos unitarios de la unidad correspondiente.
- Modificación de ubicación de equipos:

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

- La modificación de la ubicación se refiere al cambio de domicilio en el que se encuentre operando el equipo y que puede ser dentro de la misma ciudad o incluso cambio de ciudad dentro del territorio de la República Mexicana. No se considerará ninguna modificación en los importes en la facturación.
- Sustitución del Personal
- El administrador del contrato del Instituto FONACOT podrá solicitar su sustitución por así considerarlo conveniente en cualquier momento durante la vigencia del contrato. En caso de que la solicitud de sustitución del personal se derive de una falta que afecte la imagen y/o la confidencialidad de la información del Instituto FONACOT, el LICITANTE ganador se obligará a cooperar con el administrador del contrato del Instituto FONACOT para el descargo de pruebas y evidencias en las que hubiese incurrido su personal.

El administrador del contrato podrá solicitar la baja de servicios que ya no requiera el Instituto FONACOT en cualquier momento durante toda la vigencia del servicio.

Anexo "Domicilios"

No.	Región	Sucursal	Domicilio
1	Metropolitana	Oficinas Centrales	Insurgentes Sur 452, Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, Distrito Federal.
2	Metropolitana	Plaza de la Republica (Plaza de la Republica)	Plaza de la República No. 32, Planta Baja, Col. Tabacalera, Del. Cuauhtémoc, C.P. 06030, Distrito Federal.
3	Metropolitana	Mixcoac	Molinos esquina Santiago Rebull No. 61 Col. Mixcoac C.P. 3910 Del. Benito Juarez, Distrito Federal.
4	Metropolitana	Modulo Chilpancingo (Insurgentes)	Insurgentes Sur 452, Planta Baja, Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, Distrito Federal.
5	Metropolitana	Portales	Municipio Libre No. 83, Col. Portales, Del. Benito Juárez, C.P. 03300, México, Distrito Federal.
6	Metropolitana	Tlalnepantla	Av. Sor Juana Inés de Cruz, No. 22 Despacho 106-4, Colonia Centro de Tlalnepantla, C.P. 5400, Tlalnepantla de Baz Estado de México
7	Metropolitana	Cuautitlán Izcalli	Av. Huhuetoca s/n, SORIANA, Loc. 6, Col. Claustro de San Miguel, Cuautitlán Izcalli, Estado de México.
8	Metropolitana	Vallejo	Norte 45 No. 853-B, Col. Industrial Vallejo, Del. Gustavo A. Madero, C.P. 02300, México, Distrito Federal.
9	Metropolitana	Ecatepec	Vía Morelos No. 24, Col. Jajalpa, C.P. 55090, Ecatepec, Estado de México.
10	Metropolitana	Congreso Del Trabajo	Av. Ricardo Flores Magón No. 44, Col. Guerrero, Del. Cuauhtémoc, C.P. 06300, México, Distrito Federal.
11	Metropolitana	Zaragoza	Blvd. Puerto Aéreo No. 81, 1er piso, Col. Federal, Del. Venustiano Carranza, C.P. 15700, México, Distrito Federal.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, Mexico D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

12	Metropolitana	Chalco	Boulevard Cuauhtémoc, MZ. 53 LT. 6, Local 2, Col. Emiliano Zapata, Chalco de Covarrubias, Estado de México, C.P. 56608.
13	Metropolitana	Texcoco	Prolongación 16 de Septiembre No. 310, Loc. 30, Col. Barrio de San Pablo Centro, C.P 56116, Texcoco, Estado de México.
14	Metropolitana	Coapa	Av. Canal de Miramontes 3280, locales 27, 28, 29, 30, Coaplaza, Col. Villacoapa, Del. Tlalpan, C.P. 14390
15	Metropolitana	Plaza de la República	Plaza de la República No. 32, Planta Baja, Col. Tabacalera, Del. Cuauhtémoc, C.P. 06030, Distrito Federal.
16	Norte	Chihuahua	Calle Séptima y Allende No. 1002, Zona Centro, C.P. 31000, Chihuahua, Chihuahua.
17	Norte	Delicias	Circuito Plaza de la Republica 4 Norte Colonia Centro Entre calle Central y calle 2da. Norte C.P. 33000.
18	Norte	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.
19	Norte	Mexicali	Av. Reforma No. 692, sección primera de la Ciudad de Mexicali, Baja California Norte.
20	Norte	Tijuana	Blvd. Díaz Ordaz No.14910, Col. Las Brisas, Plaza Las Brisas, Tijuana, Baja California Norte.
21	Norte	Ensenada	Av. Delante fracción A y B, Lt. 007, Mza. 025, Col. Carlos Pacheco, C.P. 22890, Municipio de Ensenada, Baja California Norte.
22	Norte	Hermosillo	Blvd. Luis Donaldo Colosio No. 323, Col. Valle Grande, C.P. 83205, Hermosillo, Sonora.
23	Norte	Cd. Obregón	Durango No. 245 Sur, Col. Centro, C.P. 85000, Ciudad Obregón, Sonora.
24	Norte	Empalme	Plaza Reforma, Loc.5, Col. Moderna, C.P.85330, Empalme, Sonora.
25	Norte	Nogales	Av. de los Nogales No. 277, Loc. 3, 4 y 5, Plaza Coyoacán, Col. Colinas del Yaqui, C.P. 84093, Nogales, Sonora.
26	Norte	Culiacán	Gral. José Aguilar Barraza No. 1297 Poniente, Col. Centro, C.P. 80029, Culiacán, Sinaloa.
27	Norte	Mazatlán	Av. Ejército Mexicano No. 1401-A, Col. Ferrocarrilera, C.P. 82010, Mazatlán, Sinaloa.
28	Norte	Los Mochis	Av. Cuauhtémoc No. 201 Poniente, Col. Bienestar, C.P. 81280, Los Mochis, Sinaloa.
29	Norte	La Paz	Calz. Forjadores de Sudcalifornia No. 286, Col. Bellavista, C.P. 23078, La Paz, Baja California Sur.
30	Norte	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.
31	Noreste	Monterrey	Av. Manuel L. Barragán No. 325 Norte, Col. Residencial Anáhuac, Plaza Fiesta Anáhuac, C.P. 66457, San Nicolás de los Garza Monterrey, NL.
32	Noreste	Monterrey II	Av. Ruiz Cortines y General Bonifacio Salinas 600, Col. León XIII, C.P. 67120 Guadalupe N.L. Sucursal Soriana Lindavista.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

33	Noreste	Nuevo Laredo	Calle Héroe de Nacataz y Reynosa s/n, anexo al Centro Cívico, Zona Centro, CP 88000, Nuevo Laredo, Tamaulipas.
34	Noreste	San Luis Potosí	Independencia No. 1630, Col. Barrio San Miguelito, C.P. 78339, San Luis Potosí, San Luis Potosí.
35	Noreste	Zacatecas	Blvd. José López Portillo No. 303, edificio STPS, Col. Dependencias Federales, C.P. 98618, Zacatecas, Zacatecas.
36	Noreste	Fresnillo	Paseo del Mineral No. 1018, Col. Luis Donaldo Colosio, C.P. 99000, Fresnillo, Zacatecas.
37	Noreste	Durango	Aquiles Serdán No. 954, planta alta, Zona Centro, C.P. 34000, Durango, Durango.
38	Noreste	Saltillo	Blvd. Isidro López Zertuche No. 2567-A, Col. Universidad, C.P. 25260, Saltillo, Coahuila.
39	Noreste	Ciudad Acuña	Libramiento Emilio Mendoza Cisneros No. 1315, centro comercial MERCO, Col. Benjamín Canales, C.P. 26236, Cd. Acuña, Coahuila.
40	Noreste	Monclova	Calle de la Fuente No. 221, Loc. 4 y 5, Plaza Blanca, Col. Telefonistas, C.P. 25700, Monclova, Coahuila.
41	Noreste	Piedras Negras	Blvd. Eliseo Mendoza Berrueto s/n, Plaza Comercial, Loc. 5, Col. San Felipe Norte, C.P. 26070, Piedras Negras, Coahuila.
42	Noreste	Torreón	Av. Morelos No. 138 Poniente, Col. Centro, C.P. 27000, Torreón, Coahuila.
43	Noreste	Gómez Palacio	Av. Hidalgo No. 113 Sur, Loc. 4, Col. Centro, Gómez Palacio, Durango.
44	Noreste	Tampico	Av. Hidalgo No. 2401, Col. Reforma, C.P. 89140, Tampico, Tamaulipas.
45	Noreste	Reynosa	Aldama No. 1100, Loc. 26, Centro Comercial Río Grande, Col. Centro, C.P. 88500, Reynosa, Tamaulipas.
46	Noreste	Ciudad Victoria	Matamoros No. 237, oficinas de la STPS, Col. Centro, C.P. 87000, Ciudad Victoria, Tamaulipas.
47	Noreste	Matamoros	Ave. Prolongación González No. 2035 Col. Parque Industrial, Plaza Comercial Soriana Laguneta, C.P. 87479, Matamoros, Tamaulipas.
48	Sureste	Mérida	Paseo Montejo No. 492-A por la 43, Col. Centro, C.P. 97000, Mérida, Yucatán.
49	Sureste	Campeche	Av. 16 de Septiembre s/n, Palacio Federal, Col. Centro, C.P. 24000, Campeche, Campeche.
50	Sureste	Cancún	Av. Tulum, Retorno 1, Lote 3, Manzana 1, Súper manzana 22, Col. Centro, C.P. 77500, Benito Juárez, Quintana Roo.
51	Sureste	Chetumal	Av. Othón Pompeyo Blanco No. 204, 1er piso, Col. Centro, C.P. 77000, Chetumal, Quintana Roo.
52	Sureste	Cozumel	Plaza del Sol, Mercado de Artesanía, Local Planta Alta 8 Andador 5ta. Avenida Sur No. 1 Col. Centro C.P. 77600.
53	Sureste	Playa Del Carmen	Av. Benito Juárez, Lt. 3, Loc. 12, Plaza Papagayos, Col. Centro, C.P. 77710, Playa del Carmen, Quintana Roo.
54	Sureste	Tuxtla Gutiérrez	3a Norte Poniente No. 1395, entre la 12 y 13 Poniente Norte, Col. Moctezuma, C.P. 29030, Tuxtla Gutiérrez, Chiapas.
55	Sureste	Tapachula	4a calle Ote. No. 6, Col. Centro, C.P. 30700, Tapachula, Chiapas.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, México D.F.
Tel. (55) 52 65 74 00 www.fonacot.gob.mx

56	Sureste	Veracruz	Av. Independencia No. 787-D, P.B., Col. Centro, C.P. 91700, Veracruz, Veracruz.
57	Sureste	Córdoba	Calle 5 No. 308, despacho 2, Col. Centro, C.P. 94500, Córdoba, Veracruz.
58	Sureste	Xalapa	Diego Leño s/n, Palacio Federal, Col. Centro, C.P. 91000, Xalapa, Veracruz.
59	Sureste	Poza Rica	Av. 20 de noviembre No. 110, Local 4 en Plaza Fuente, Col. Cazones, C.P. 93230. Poza Rica, Veracruz.
60	Sureste	Villahermosa	Benito Juárez No. 118-120, Col. Centro, C.P. 86000, Villahermosa, Tabasco.
61	Sureste	Cd. Del Carmen	Av. 10 de Julio No. 117 Col. Francisco y Madero CP. 24190 Cd. Del Carmen, Campeche.
62	Sureste	Coatzacoalcos	Av. Juárez No. 511, Col. Centro, C.P. 96400, Coatzacoalcos, Veracruz.
63	Occidente	Guadalajara	Av. Lázaro Cárdenas No. 2305, edificio H, Loc. 102, Plaza Comercial Abastos, Col. Las Torres, C.P. 44920, Guadalajara, Jalisco.
64	Occidente	Federalismo	Av. Federalismo Norte 696 Sector Hidalgo, Entre Calle Cardenal y Alondra, Col. Artesanos, C.P. 44200, Guadalajara, Jalisco.
65	Occidente	Manzanillo	Blvd. Lázaro Cárdenas No. 1721, Col. Playa Azul las Brisas, C.P. 28218, Manzanillo, Colima.
66	Occidente	Colima	Av. Ignacio Sandoval No. 350 Loc. 3,4,6 Col. Lomas de Circunvalación C.P. 28010.
67	Occidente	Aguascalientes	Av. López Mateos Oriente No. 520, Col. Barrio de la Purísima C.P. 20259, Aguascalientes, Aguascalientes.
68	Occidente	Tepic	Av. Tecnológico No. 3983, Loc. 8, 9 y 10, Practiplaza Oriente, C.P. 63173, Tepic, Nayarit.
69	Occidente	Puerto Vallarta	Av. Francisco Villa No. 1474, P.B., Col. Los Sauces, C.P. 48328, Puerto Vallarta, Jalisco.
70	Occidente	León	Juan José Torres Landa Oriente 1007, Loc. 14 y 15, Col. Puerta San Rafael, León, Guanajuato.
71	Occidente	Celaya	Blvd. Adolfo López Mateos No. 932 Poniente, Col Centro, C.P. 38000, Celaya, Guanajuato.
72	Occidente	Irapuato	Av. Guerrero No. 1871, Local 2, (entre Orquídea y Jazmín), Col. Gámez, C.P. 36650.
73	Occidente	Morelia	Av. Lázaro Cárdenas No. 2000, Col. Chapultepec Sur, C.P. 58260, Morelia, Michoacán.
74	Occidente	Lázaro Cárdenas	Av. Melchor Ocampo No. 73-A Altos, Col. 2o Sector FIDELAC, C.P. 60950, Lázaro Cárdenas, Michoacán.
75	Occidente	Uruapan	Emilio Carranza No. 14- 4, Plaza Paraíso, C.P. 60000, Uruapan, Michoacán.
76	Occidente	Zamora	Zamora Amado Nervo Poniente No. 70, Col. Centro, C.P. 59600, Zamora, Michoacán.
77	Occidente	Querétaro	Av. Universidad Oriente No. 142, Col. Centro, C.P. 76000, Querétaro, Querétaro.
78	Occidente	San Juan Del Rio	16 Septiembre No. 8, Loc. 1, Col. Centro, C.P. 76800, San Juan del Río, Querétaro.

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 65 74 00 www.fonacot.gob.mx

79	Centro	Pachuca	Carr. Pachuca- Tulancingo No. 1000, Loc. D9 al D12, Plaza Universidad, Col. Abundio Martínez, C.P 42184, Mineral de la Reforma, Hidalgo.
80	Centro	Tizayuca	Carretera México- Pachuca Km. 50, oficina de CANACINTRA Tizayuca, Zona Industrial Tizayuca, C.P. 43800, Tizayuca, Hidalgo.
81	Centro	Cuernavaca	Plan de Ayala No. 1200, Col. Chapultepec, C.P. 62450, Cuernavaca, Morelos.
82	Centro	Cuautla	Galeana No. 33, Loc. 101, planta alta, Col. Centro, C.P. 62740, Cuautla, Morelos.
83	Centro	Acapulco	Av. Costera Miguel Alemán No. 1803, Frac. Magallanes, C.P. 39690, Acapulco, Guerrero.
84	Centro	Chilpancingo	Priv. de Jacarandas S/N, P.B., puerta 4 STPS, Col. Burócratas, C.P. 39090, Chilpancingo, Guerrero.
85	Centro	Puebla	Calle 9 Norte No. 208, Col. Centro, C.P. 72000, Puebla, Puebla.
86	Centro	Tlaxcala	Av. Ocotlán No. 15, Col. Ocotlán, C.P. 90100, Tlaxcala, Tlaxcala.
87	Centro	Tezuitlan	El Encanto, entrada al Hospital General Sección 3ra. No. 20, C.P. 73954, Chignautla, Puebla.
88	Centro	Tehuacán	Calle 1 Norte No. 618, Loc. 8, 9 y 10, Plaza Montecarlo, Col. Francisco Sarabia, C.P. 75730, Tehuacán, Puebla.
89	Centro	Oaxaca	Carbonera No. 902, Esquina González Ortega, Col. Barrio Trinidad de las Huertas, C.P. 68120, Oaxaca, Oaxaca.
90	Centro	Salina Cruz	Av. Manuel Ávila Camacho No. 50, Palacio Federal, Salina Cruz, Oaxaca.
91	Centro	Tuxtepec	Av. 20 de Noviembre s/n, Col. La Piragua, C.P. 68300, Tuxtepec, Oaxaca.
92	Centro	Toluca	Ignacio Allende Sur No. 116, Col. Centro, C.P. 50000, Toluca, Estado de México.
93	Centro de Datos Alterno	Santa Fe	Prolongacion Paseo de la Reforma No.5396, Cuajimalpa, C.P. 05000, Ciudad de Mexico
94	Centro de Datos Principal	Querétaro	Privada Princesa No. 4, Parque Industrial El Marques, C.P. 76246, Km 195.5, Autopista Mexico-Queretaro

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtemoc, C.P. 06760, México D.F.
Tel. (55) 52 65 73 00 www.fonacot.gob.mx

Elaboró	Autorizó
Lic. José Guillermo Araujo Rodríguez **Director de Infraestructura Tecnológica**	**Mtro. Horacio Sánchez Tinoco** **Subdirector General de Tecnologías de la Información y Comunicación**

edP

Av. Insurgentes Sur 452 Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, México D.F.
Tel. 1551 52 65 74 00 www.fonacot.gob.mx

ANEXO II
COTIZACIÓN

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

"FORMATO DE COTIZACIÓN"

Número (Anexo)	Descripción	Cantidad	Precio unitario mensual	Total
2.3.1	Servicio de Monitoreo de infraestructura	1	$ 138,600.00	$ 138,600.00
2.3.2	Servicio de Switching			
2.3.2.1	· Herramienta de administración de la red	1	$ 23,128.20	$ 23,128.20
2.3.2.2	· Esquema de Alta Disponibilidad en Switches CORE Tipo A	2	$ 193,824.33	$ 387,648.66
2.3.2.3	· Esquema de Alta Disponibilidad en Switches CORE Tipo B	2	$ 238,377.38	$ 476,754.76
2.3.3	Switches de acceso			
2.3.3.1	* Switch de acceso Tipo 1	7	$ 98,617.44	$ 690,322.06
2.3.3.2	* Switch de acceso Tipo 2	10	$ 6,838.77	$ 68,387.67
2.3.3.3	* Switch de acceso Tipo 3	4	$ 5,936.76	$ 23,747.04
2.3.3.4	* Switch de acceso Tipo 4	40	$ 5,423.07	$ 216,922.68
2.3.3.5	* Switch de acceso Tipo 5	42	$ 5,066.47	$ 212,791.70
2.3.4	Red inalámbrica			
2.3.4.1	Servicio de red inalambrica en edificio SEDE	2	$ 29,570.85	$ 59,141.70
2.3.4.2	Servicio de red inalambrica en localidades.	61	$ 1,461.58	$ 89,156.38
2.3.5	Archivos Compartido en Red			
2.3.5.1	FILESERVER	1	$ 38,312.82	$ 38,312.82
2.3.5.2	FTP	1	$ 29,312.59	$ 29,312.59
			SUBTOTAL (A)	**$ 2,454,226.26**

Número (Anexo)	Descripción	Cantidad	Precio unitario mensual	Total
2.3.6	Servicio de Contención perimetral			
2.3.6.1	· Firewall tipo 1	8	$ 45,379.56	$ 363,036.46
2.3.6.2	· Firewall tipo 2	6	$ 29,312.21	$ 175,873.25
2.3.6.3	Filtrado de contenidos Web	1	$ 169,871.59	$ 169,871.59
			SUBTOTAL (B)	**$ 708,781.29**

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Número (Anexo)	Descripción	Precio Unitario por Evento (Bajo Demanda)	Precio unitario (Bajo Demando)	Total
2.3.7	**Cableado Estructurado**			
2.3.7.1	Instalación de nodos nuevos	1	$ 7,712.55	$ 7,712.55
2.3.7.2	Reubicación de nodos existentes	1	$ 4,773.60	$ 4,773.60
2.3.7.3	Mantenimiento de nodos de red	1	$ 1,800.00	$ 1,800.00
2.3.7.4	Instalación de fibra óptica	1	$ 47,576.88	$ 47,576.88
2.3.7.5	Movimiento de infraestructura	1	$ 23,400.00	$ 23,400.00
			SUBTOTAL (C)	**$ 85,263.03**

Número (Anexo)	Descripción	Cantidad	Precio unitario mensual	Total
2.3.8	**Administración de energía regulada**			
	UPS Tipo 1, 3KVA	14	$ 1,353.17	$ 18,944.35
	UPS Tipo 2, 5 KVA	18	$ 2,977.85	$ 53,601.26
	UPS Tipo 3, 8KVA	7	$ 10,816.58	$ 75,716.05
	UPS Tipo 4, 10KVA	9	$ 13,165.10	$ 118,485.91
	UPS Tipo 5, 16KVA	27	$ 15,008.09	$ 405,218.30
	UPS Tipo 6, 20KVA	9	$ 30,361.89	$ 273,256.98
	UPS Tipo 7,30KVA	3	$ 31,297.10	$ 93,891.29
	UPS Tipo 8,40KVA	1	$ 50,075.36	$ 50,075.36
	UPS Tipo 9,100KVA	1	$ 75,113.04	$ 75,113.04
			SUBTOTAL (D)	**$ 1,164,302.53**

SUBTOTAL (A + B + C + D)	$ 4,412,573.11
IVA	$ 706,011.70
TOTAL	**$ 5,118,584.81**

(Monto total con Letra)

Cinco millones ciento diesciocho mil quinientos ochenta y cuatro Pesos 81/M.N

Tecnología en Seguridad & Comunicaciones S.A. de C.V

RFC: **TSC 050331 163**

OFICINA: Patricio Sanz No. 526 Col. Del Valle C.P. 03100 Ciudad de México **Tels. (55) 5534 4705/ (55) 3868 0820**

DATACENTER: Boulevard de los Reyes No. 6204 Edificio Torre A7 Piso 4, Tlaxcalancingo, San Andrés Cholula, Puebla C.P. 72820

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".
Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Los costos de los servicios de instalación configuración y puesta a punto deberán estar incluidos en su propuesta económica.
Su propuesta económica deberá contener fecha, firma del representante legal RFC, y vigencia de la cotización.

ATENTAMENTE.

Ing. Gerardo Diaz Sierra.
Representante Legal.
Tecnología en Seguridad y Comunicaciones S.A. de C.V.

TRABAJO
RECIBIDO
17 MAY 2022
17:30 horas
SUBDIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Tecnología en Seguridad & Comunicaciones S.A. de C.V
RFC: **TSC 050331 163**
OFICINA: Patricio Sanz No. 526 Col. Del Valle C.P. 03100 Ciudad de México **Tels. (55) 5534 4705/ (55) 3868 0820**
DATACENTER: Boulevard de los Reyes No. 4204 Edificio Torre A7 Piso 4, Tlaxcalancingo, San Andrés Cholula, Puebla C.P. 72820

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".
Vigencia de la cotización: 1 mes a partir de la entrega de la misma.

Ciudad de México a 17 de mayo de 2022.

CUESTIONARIO

SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES

1.- ¿El proveedor cuenta con documento actualizado expedido por el SAT en el que se emita opinión sobre el cumplimiento de sus obligaciones fiscales en sentido positivo?

SI | No

*Tecnología en Seguridad y Comunicaciones **SI cuenta** con documento actualizado expedido por el SAT en el que se emita opinión sobre el cumplimiento de sus obligaciones fiscales en sentido positivo.*

2.- ¿El proveedor cuenta con documento Opinión del Cumplimiento de obligaciones fiscales en materia de seguridad social en sentido positivo?

SI | No

*Tecnología en Seguridad y Comunicaciones **SI cuenta** con documento Opinión del Cumplimiento de obligaciones fiscales en materia de seguridad social en sentido positivo.*

3.- ¿El proveedor cuenta con constancia de situación fiscal en Materia de Aportaciones Patronales y entero de descuentos, emitida por el Instituto del Fondo Nacional de la Vivienda para los Trabajadores?

SI | No

*Tecnología en Seguridad y Comunicaciones **SI cuenta** con constancia de situación fiscal en Materia de Aportaciones Patronales y entero de descuentos, emitida por el Instituto del Fondo Nacional de la Vivienda para los Trabajadores.*

4.- ¿El proveedor cuenta con la infraestructura y personal suficiente para llevar a cabo el servicio?

SI | No

*Tecnología en Seguridad y Comunicaciones **SI cuenta** con la infraestructura y personal suficiente para llevar a cabo el servicio.*

Tecnología en Seguridad & Comunicaciones S.A. de C.V
RFC: **TSC 050331 163**
OFICINA: Patricio Sanz No. 526 Col. Del Valle C.P. 03100 Ciudad de México **Tels. (55) 5534 4705/ (55) 3868 0820**
Tlaxcalancingo, San Andrés Cholula, Puebla C.P. 72820

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".
Vigencia de la cotización: 1 mes a partir de la entrega de la misma.

Ciudad de México a 17 de mayo de 2022.

5. ¿El proveedor cumple en su talidad con las condiciones técnica y administrativas del anexo técnico?

SI	No

*Tecnología en Seguridad y Comunicaciones **SI cumple** en su talidad con las condiciones técnica y administrativas del anexo técnico.*

6. ¿El proveedor tiene la capacidad de operar y cumplir con lo establecido en el Anexo Técnico a nivel Nacional?

SI	No

*Tecnología en Seguridad y Comunicaciones **SI tiene** la capacidad de operar y cumplir con lo establecido en el Anexo Técnico a nivel Nacional.*

ATENTAMENTE.

Ing. Gerardo Diaz Sierra.
Representante Legal.
Tecnología en Seguridad y Comunicaciones S.A. de C.V.

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUICACIONES

Anexo técnico

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Contenido

1. INFORMACION GENERAL 4
1.1. ANTECEDENTES 4
1.2. OBJETIVO DEL SERVICIO 4

2. DESCRIPCIÓN DEL SERVICIO INTEGRAL ADMINISTRADO 5
2.1. ALCANCE DEL SERVICIO 5
2.2. IMPLEMENTACIÓN DEL SERVICIO 5
2.2.1. CONTINUIDAD OPERATIVA 5
2.3. ESPECIFICACIONES DEL SERVICIO 6
2.3.1. Servicio de Monitoreo de Infraestructura 6
2.3.2. Servicio de Switching. 9
2.3.3. Switches de acceso 31
2.3.4. Red Inalámbrica 70
2.3.5. Archivos Compartidos en Red 84
2.3.6. Servicio de Contención Perimetral 86
2.3.7. CABLEADO ESTRUCTURADO 98
2.3.8. SERVICIO DE ADMINISTRACIÓN DE ENERGÍA REGULADA (UPS) 99
2.3.9. SOPORTE TÉCNICO 104
2.3.10. SERVICIOS BAJO DEMANDA 108
2.4 PLAN DE RETORNO 109
2.5. POLÍTICAS 109
2.6. GESTIÓN DEL SERVICIO 110
2.6.1. ESCRITORIO DE SERVICIO 110
2.6.2. ADMINISTRACIÓN DE INCIDENTES 111
2.6.3. ADMINISTRACIÓN DE PROBLEMAS 112
2.6.4. ADMINISTRACIÓN Y CAMBIOS DE LA CONFIGURACIÓN 112
2.6.5. SERVICIOS DE COORDINACIÓN 112
2.7. ASPECTOS GENERALES 114
3. MANUALES, CATALOGOS Y FOLLETOS 115
4. PATENTES, MARCAS Y DERECHOS 115

5. MUESTRAS 115

6. PRUEBAS Y DESARROLLO A EFECTUAR A LAS MUESTRAS 115

7. LUGAR, PLAZO Y HORARIO DE LA PRESTACIÓN DEL SERVICIO 115

8. PLAZO PARA LA SUSPENSIÓN DEL SERVICIO 116

9. PAGO ..... Ciudad de México a 17 de mayo de 2022.

10. ENTREGABLES 116
10.1. ENTREGABLES INICIALES 116
10.2. ENTREGABLES MENSUALES 117
10.3. ENTREGABLES FINALES 118
10.3.1. Memoria técnica 118

11. NIVELES DE SERVICIO 118
11.1. Inicio de operaciones 118
11.2. PUESTA A PUNTO DEL SERVICIO INTEGRAL ADMINISTRADO 118
11.3. Cableado estructurado 119
11.4. Servicios bajo demanda 120
11.5. Incidentes por fallas 120
11.6. Cambios Estándar 121
11.7. Solicitud de Cambio (RFC#) 122

12. GARANTÍA DE CUMPLIMIENTO DEL CONTRATO 122

13. GARANTÍA DE RESPONSABILIDAD CIVIL 122

14. PENA CONVENCIONAL Y DEDUCTIVA 122
14.1. pena convencional 122
14.1.1. INICIO DE OPERACIONES 123
14.1.2. PUESTA A PUNTO DEL SERVICIO INTEGRAL ADMINISTRADO 123
14.1.3. SERCVICIO O EQUIPOS NO OTORGADOS 124
14.2. deductivas 125
Disponibilidad de servicios 125
Incidentes por fallas 126
Cambios Estándar 126

15. NORMAS APLICABLES 127

16. CONFIDENCIALIDAD 127

17. ADMINISTRADOR DEL CONTRATO 128
17.1. MODIFICACIONES QUE SE RESERVA EL ADMINISTRADOR DEL CONTRATO . 128

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

1. INFORMACION GENERAL

1.1. ANTECEDENTES

Actualmente el Instituto FONACOT dispone de un universo aproximado de 1,700 usuarios, de los cuales el 30% es personal de estructura, el 50 % operativo y el 20% externo. Este personal se encuentra distribuido en las Oficinas Centrales de Insurgentes, Edificio Plaza de la República, Direcciones Regionales, Estatales, Representaciones y/o Módulos ubicadas en distintas entidades federativas a nivel nacional, todos interconectados mediante una red VPN MPLS y en algunos casos mediante enlaces ADSL.
Asimismo, el Instituto FONACOT, cuenta con un centro de datos que soporta los servicios sustantivos, los cuales también se encuentran integrados a la red VPN MPLS.
Los elementos de infraestructura que conforman el prototipo de una localidad del Instituto FONACOT son los siguientes:

- Switch
- Access Points
- Equipo de energía ininterrumpible
- Cableado estructurado

1.2. OBJETIVO DEL SERVICIO

Gestionar, monitorear y en su caso suministrar los elementos necesarios de infraestructura de telecomunicaciones para la adecuada operación de las redes de área local, y los servicios informáticos del Instituto FONACOT, a fin de garantizar que las oficinas del Instituto FONACOT se encuentren intercomunicadas de manera óptima.

Los objetivos especificos a cubrir son los siguientes:

- Monitorear la disponibilidad y desempeño de la infraestructura tecnológica y servicios informáticos involucrados en el otorgamiento del servicio solicitado en este anexo técnico.
- Administrar y operar los servicios solicitados, basándose en estándares internacionales como ITIL, para atender de manera oportuna los incidentes de administración y soporte técnico.
- Atender cualquier eventualidad relacionada con los elementos de administración y seguridad propuesta, de acuerdo a los niveles de servicio.
- Operar el monitoreo, la administración de los servicios y redes en un esquema 7 x 24.
- Brindar el soporte técnico de manera remota preferentemente o en sitio, cumpliendo

con los niveles de servicio establecidos.

- Brindar asesoría proactiva en el tratamiento de incidentes que involucren la aparición y/o detección de nuevas vulnerabilidades sobre los componentes de seguridad involucrados en el servicio solicitado.

- Coordinar con el escritorio de servicio y con los diferentes grupos resolutores del Instituto FONACOT para dar respuesta a los incidentes relacionados con la administración del monitoreo de la infraestructura de red.
- Proporcionar los reportes de comprobación del cumplimiento de los niveles de servicio establecidos y de análisis de incidencias.

2. DESCRIPCIÓN DEL SERVICIO INTEGRAL ADMINISTRADO

2.1. ALCANCE DEL SERVICIO

En términos generales el servicio comprende los siguientes elementos, las características de cada uno de los servicios se expresa en el punto 2.4 ESPECIFICACIONES DEL SERVICIO

2.2. IMPLEMENTACIÓN DEL SERVICIO

2.2.1. CONTINUIDAD OPERATIVA

A fin de establecer las mejores condiciones para la prestación de los servicios, Tecnología en Seguridad y Comunicaciones S.A. de C.V., verificará y mantendrá los servicios para la correcta operación del Instituto.

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

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

A continuación, se enlistan los servicios requeridos por el Instituto FONACOT:

SERVICIO INTEGRAL ADMINISTRADO

SERVICIO DE MONITOREO DE INFRAESTRUCTURA
SERVICIO DE SWITCHING.

- Herramienta de Administración de la Red
- Esquema de Alta Disponibilidad en Switches CORE Tipo A.
- Esquema de Alta Disponibilidad en Switches CORE Tipo B
- Switches de acceso

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Switch de acceso Tipo1
- Switch de acceso Tipo2
- Switch de acceso Tipo 3
- Switch de acceso Tipo4
- Switch de acceso Tipo 5

RED INALÁMBRICA

- Servicio de red Inalambrica en edificio SEDE
- Servicio de red inalambrica en localidades

ARCHIVOS COMPARTIDOS EN RED

- FILESERVER
- FTP

GESTIÓN DE LA SEGURIDAD

- Servicio de Contención Perimetral
  - Firewall Tipo 1
  - Firewall Tipo 2

FILTRADO DE CONTENIDOS

- Filtrado de contenido Web

SERVICIO DE ADMINISTRACIÓN DE ENERGÍA REGULADA (UPS)

- UPS tipo 1, 3 KVA
- UPS tipo 2, 5 KVA
- UPS tipo 3, 8 KVA
- UPS tipo 4, 10 KVA
- UPS tipo 5, 16 KVA
- UPS tipo 6, 20 KVA
- UPS tipo 7, 30 KVA
- UPS tipo 8, 40 KVA
- UPS tipo 9, 100 KVA

CABLEADO ESTRUCTURADO

- Instalación de nodos nuevos
- Reubicación de nodos existentes
- Mantenimiento de nodos de red
- Instalación de Fibra Óptica
- Movimientos de Infraestructura.

SOPORTE TÉCNICO.

SERVICIOS BAJO DEMANDA

TRANSFERENCIA DEL CONOCIMIENTO

PLAN DE RETORNO

- Políticas

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

GESTIÓN DEL SERVICIO:

Escritorio de servicio.

- Administración de incidentes
- Administración de problemas
- Administración y cambios de la configuración

Servicios de coordinación.

ASPECTOS GENERALES

23. ESPECIFICACIONES DEL SERVICIO

A continuación, se describen las especificaciones que Tecnología en Seguridad y Comunicaciones S.A. de C.V., cumplirá para proveer el Servicio Integral Administrado:

23.1. Servicio de Monitoreo de Infraestructura

Tecnología en Seguridad y Comunicaciones S.A. de C.V., realizará el monitoreo de la disponibilidad, capacidad y rendimiento de la infraestructura de comunicaciones, servidores, bases de datos, aplicaciones y transacciones basadas en Java, a fin de que su utilización permita mantener la supervisión ininterrumpida de la infraestructura, aplicaciones que soportan los sistemas institucionales y servicios informáticos del Instituto FONACOT.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., realizará el monitoreo de toda la infraestructura utilizando herramientas especializadas que cumpla al menos con las siguientes características técnicas:

- Soportará SNMP versión 1, 2 y 3. Contendrá protocolos para monitoreo de anchode banda además de SNMP: WMI, Netflow, jFlow, sFlow, Packet Sniffing.
- Poseerá un acceso HTML puro y debe ser accesible vía http o SSL.
- Poseerá un acceso a través de una aplicación nativa de Windows y una aplicación para dispositivos móviles que puedan ser utilizadas simultáneamente.
- Será capaz de realizar el monitoreo sin agentes.
- La herramienta realizará monitoreo al menos de los siguientes aspectos: ancho de banda, aplicaciones, servidores virtuales, SLA, LAN, VPN, WAN y sitios distribuidos, monitoreo de QoS (para VoIP)
- Soportará IPv6
- Será capaz de enviar notificaciones vía correo electrónico, y los recipientes serán configurables por cada cuenta de usuario de la herramienta de forma independiente.
- Las notificaciones serán flexibles a modo de que la arquitectura sea tolerante a fallos (email, alertas en las aplicaciones móviles, Syslog, acciones HTTP o notificaciones en tecnologías externas a través de un EXE)

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 25 de mayo de 2022.

- La herramienta proveerá la opción de trabajar con un nodo Failover en cluster.
- Escalado de alertas que envíe una notificación extra cada cierto tiempo durante el periodo de caída del dispositivo.
- Existirá una característica jerárquica en las notificaciones adjuntas e integradas a la jerarquía entre dispositivos, de modo que, si un dispositivo principal falla y esta característica está activa, las alarmas de todos los dispositivos que están jerárquicamente bajo el fallido sean silenciadas.
- Interfaz única para el monitoreo de dispositivos y aplicaciones.
- Proveerá muestreo vía SNMP para dispositivos capa 2 y capa 3
- Al detectar alguna falla en algún dispositivo, suprimirá las alarmas dependientes demodo que solo la alarma de más alto nivel se reciba.
- Tendrá la capacidad de ejecutar comandos al recibir una alerta.
- Permitirá la configuración personalizada de umbrales para las alarmas.
- Permitirá la configuración de múltiples condiciones para desencadenar una alerta
- Será capaz de monitorear varias redes en diferentes localidades
- La interfaz del producto estará disponible en idioma español
- La documentación y manuales estarán disponibles al menos en idioma inglés
- Soporta distintos intervalos de muestreo dependiendo de la variable que se está interrogando.
- Será compatible con plataforma Windows Server 2008 o superior.
- Permitirá realizar búsquedas de los dispositivos por dirección IP, modelo, grupos, tecnologías.
- Será capaz de realizar un descubrimiento automático de la red
- Contará con módulos integrados para el monitoreo de bases de datos SQL medianteun agente SNMP

- Generará reportes en tiempo real enfocados a análisis de fallas, y acuerdos de calidad de servicio (SLA). Los reportes serán generados mediante la recolección automática de datos y eventos de los diferentes dispositivos. De igual manera los reportes serán generados bajo demanda o programados en esquema diario, semanal, mensual y enviados vía correo electrónico a la dirección o direcciones que el área técnicadel Instituto FONACOT defina.
- Tendrá la capacidad de generar tableros de control de acuerdo con lo siguiente:
    - Mapas y tableros de control. Proveerá tableros de control con información de rendimiento en tiempo real
    - Los tableros de control serán diseñables de forma interactiva, ofreciendo diversos objetos gráficos y la posibilidad de importar imágenes para ser mostradas dentro del dashboard.
    - Será capaz de generar tableros de control por proceso, de acuerdo con las métricas de los dispositivos involucrados en cada proceso.
- Reportes Detallados

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Entregar reportes en HTML o PDF
- Programar las tareas de los informes o hacerse ad-hoc
- Posibilidad de exportar datos históricos de monitoreo para análisis, en formatos XML, CSV o HTML
- Ofrecer gráficos con gran nivel de detalle, además de presentar los datos de forma tabular por métrica de los dispositivos
- Mostrar tiempo productivo e improductivo, en segundos y en porcentaje
- Mostrar un análisis top del uso de ancho de banda
- Mostrar análisis top del uso de CPU

- Recolectará métricas de desempeño de redes, aplicaciones, servidores y servicios en tiempo real.
- Detección y notificación de fallas en tiempo real de redes, aplicaciones, servidores y servicios.
- Asegura la disponibilidad del servicio soportada por la infraestructura tecnológica.
- Realizará monitoreo proactivo para evitar la afectación de los niveles de servicio, alertando posibles fallos de acuerdo con los umbrales personalizables
- Será capaz de realizar un análisis estadístico para detectar comportamientos inusuales de acuerdo con la información histórica del dispositivo
- Permitirá a los usuarios la consulta de reportes a través de un navegador Web.
- Soportará encripción SSL para el envío de información entre redes monitoreadas en múltiples sitios
- Soportará HTTPS para Web y Windows
- Soportará control de acceso de usuarios de acuerdo a los siguientes puntos:
  - Manejar perfiles de usuario.
  - Es capaz de limitar a qué dispositivos puede acceder el usuario.
  - Es capaz de limitar los derechos de lectura/escritura, para sólo lectura
  - Permite agendar mantenimientos de manera programada.
- Permitirá configurar el tiempo límite de respuesta de un dispositivo.
- Utilizará una base de datos.

- Toda la información histórica debe ser almacenada en una base de datos única, a prueba de ataques SQL injection
- Será auto administrable, de forma que no sea necesario la intervención humana para su administración.
- Será fácilmente configurable y contar una GUI visual
- Los reportes y la interfaz web serán personalizables para el del área técnica del Instituto FONACOT
- Será capaz de importar archivos MIB para monitorear dispositivos de múltiples fabricantes

- Contará con una API que permita crear, borrar y editar objetos de monitoreo

Ciudad de México a 17 de mayo de 2022.

Como parte del servicio, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado será responsable de proporcionar el licenciamiento necesario para que el personal autorizado del área técnica del Instituto FONACOT acceda a las consolas de monitoreo.

Como parte de este servicio, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado durante toda la vigencia del servicio se obliga a realizar sin costo adicional para la convocante, todas las modificaciones,adecuaciones y/o cambios en los tableros (dashboards), contenedores, vistas, topologías, y cualquier actividad que permita optimizar la visualización de la información colectada porlas diferentes herramientas de monitoreo consideradas en este rubro.

Es responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado mantendrá el licenciamiento vigente y efectuar las actualizaciones hacia las nuevas versiones disponibles e incorporando nuevas funcionalidades de las mismas durante toda la vigencia del contrato, sin costo adicional para la convocante.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado presentará la información de disponibilidad, capacidad y rendimiento de la infraestructura monitoreada a través de una pantalla que deberá ubicarse en las oficinas centrales del Instituto FONACOT.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado contemplará todos los accesorios necesarios para el montaje dela pantalla en el lugar que designe el área técnica del Instituto FONACOT, así como loscomponentes o elementos (cables e interfaces, etc.) que sean obligados para su operación.

El servicio de monitoreo operará en infraestructura de Tecnología en Seguridad y Comunicaciones S.A. de C.V., por lo quees responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., mantener la configuración, parametrización y puesta a punto de las herramientas de monitoreo involucradas en el servicio solicitado.

2.3.2. Servicio de Switching.

2.3.3.

2.3.3.1. Herramienta de Administración de la Red

Tecnología en Seguridad y Comunicaciones S.A. de C.V., llevará a cabo las actividades de administración de la infraestructurade switches propuestos, utilizando el software especializado Netsight Console, Policy Manager, Inventory Manager y NAC Manager propiedad del Instituto FONACOT. Este software cuenta con mantenimiento vigente hasta el 31 de mayo de 2022, por lo que es responsabilidad Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado mantenerlo vigente durante toda la vigencia del servicio, así como, realizar lo necesario para dar continuidad al uso de estas herramientas actualizándolas a las nuevas versiones disponibles e incorporando las nuevas funcionalidades cubriendo al menos los siguientes puntos:

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Permitirá la administración centralizada de parámetros de todos los switches que suministre Tecnología en Seguridad y Comunicaciones S.A. de C.V para otorgar el servicio de Switching.
- Permitirá la aplicación de reglas de clasificación de tráfico de capas 2, 3 y 4,a usuarios, con el fin de asegurar el acceso de los mismos a los recursos de red que les corresponden.
- Permitirá mediante una interfaz Web tener visibilidad completa y un cierto nivel de control sobre todos los switches que conforman este servicio a fin de proporcionar la siguiente información:
  - Dashboards, reportes, graficas, tablas y estadísticas interactivas que muestren los principales parámetros de la red, tales como: estado de los elementos de red, alarmas, eventos, desplegado de puertos, uso de CPU, SSIDs, así como de los usuarios conectados a la red, identificación de dispositivos de acuerdo al sistema operativo, tipo de autenticación y perfil.
  - Búsqueda de dispositivos por dirección IP, dirección MAC o nombre de usuario.
  - Diagramas de conexión lógica de los dispositivos y elementos de red.
  - Datos provenientes de la solución de Control de Acceso a la Red y gestión de funciones de dicha solución, tales como dar de baja usuarios y/o dispositivos, re autenticación de los mismos, movimiento de usuarios y/o dispositivos a diferentesgrupos de trabajo que proporcione la solución de Control de Acceso a la Red.
  - Generación de reportes.
  - Guardar un histórico de la información hasta por 6 meses.
- Contará con un visor de flujos basado en NetFlow para efectos de diagnóstico y soporte.
- Identificará diferentes tipos de equipos como PC's, Servidores, Impresoras, Cámaras IP, Teléfonos IP conectados a la red e identificar las vulnerabilidades asociadas a ellos.
- Interactuará con los equipos propuestos para localizar ubicación exacta de los eventos de seguridad que sean notificados vía SNMP v3 por el dispositivo de análisis de comportamiento de la red y detener el ataque en forma automática desde el puerto donde se genere la anomalía o en el punto de ingreso a la red, através de implementación dinámica de políticas de control de tráfico, que deshabiliten el puerto y/o bloqueen el flujo origen de la anomalía de seguridad sin intervención manual.
- Capacidad de administrar controladoras y Access Points del mismo fabricante.
- Capacidad de detectar alguna las siguientes amenazas:
  - AP intrusos (rogue)
  - Dispositivos en modo Ad-Hoc.
  - Ataques de Denial of Service (DoS)

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Fuentes de interferencia
- Intentos de password Cracking
  - Capacidad de habilitar la captura de información en tiempo real en un AccessPoint de la red
  - Capacidad de reportar fuentes de interferencia
  - Capacidad de desplegar información sobre cada controlador inalámbrico
- Listado de Access Point conectados por canal
- Clientes
- Uso de ancho de banda
  - Capacidad de listar los Access Point del sistema y desplegar información individual sobre:
- Controlador al que está conectado
- Ancho de banda
- Clientes conectados
- Alarmas
  - Capacidad de listar los clientes del sistema y desplegar información individualsobre:
- Horarios de inicio y fin de sesión
- Historial de roaming entre Access Point
- Cambios de dirección IP
- Cambios de estado de autenticación
  - Clientes conectados
  - Capacidad de listar las amenazas detectadas mediante WIDS/Wips

Tecnología en Seguridad y Comunicaciones S.A. de C.V., mantendrá la continuidad de los servicios que se encuentran implementados actualmente en la red del Instituto FONACOT, por lo que las configuraciones, reglas y políticas de acceso a usuarios, serán migradas de manera transparente a los equipos propuestos porTecnología en Seguridad y Comunicaciones S.A. de C.V.,

Durante toda la vigencia del contrato, la herramienta de administración se mantendrá a la última versión de software estable liberada por el fabricante.

Se considerará al menos 3 accesos concurrentes a la herramienta de administración para personal del area técnica del Instituto FONACOT independientes a los que Tecnología en Seguridad y Comunicaciones S.A. de C.V., requiera para la operación del servicio.

Este servicio deberá operar en la infraestructura de Tecnología en Seguridad y Comunicaciones S.A. de C.V.

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez. C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

1.3.1.1. Esquema de Alta Disponibilidad en Switches CORE Tipo A.

Ciudad de México a 17 de mayo de 2022.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., implementará un esquema de alta disponibilidad en las Oficinas Centrales del Instituto FONACOT (Sede Insurgentes), basado en dos Switches CORE deúltima generación con la finalidad de contar con redundancia a nivel backbone de fibraóptica. Es responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerar el dimensionamiento adecuado encuanto a hardware, licenciamiento, actualizaciones, componentes y cualquier otro elemento que se requiera para la adecuada operación de los equipos que conformen este esquema.

Es responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., garantizar que el esquema de alta disponibilidad implementado mantenga la configuracion, niveles de seguridad y control de tráfico porservicio y por usuario que actualmente tiene definidas el área técnica Instituto FONACOT. La implementación de los equipos CORE deberá integrarse nativamente con la herramienta de administración de la Red, propiedad del Instituto FONACOT.
A continuación, se muestra el esquema de alta disponibilidad de switches core en oficinas centrales (Sede Insurgentes) solicitado para el presente proyecto.

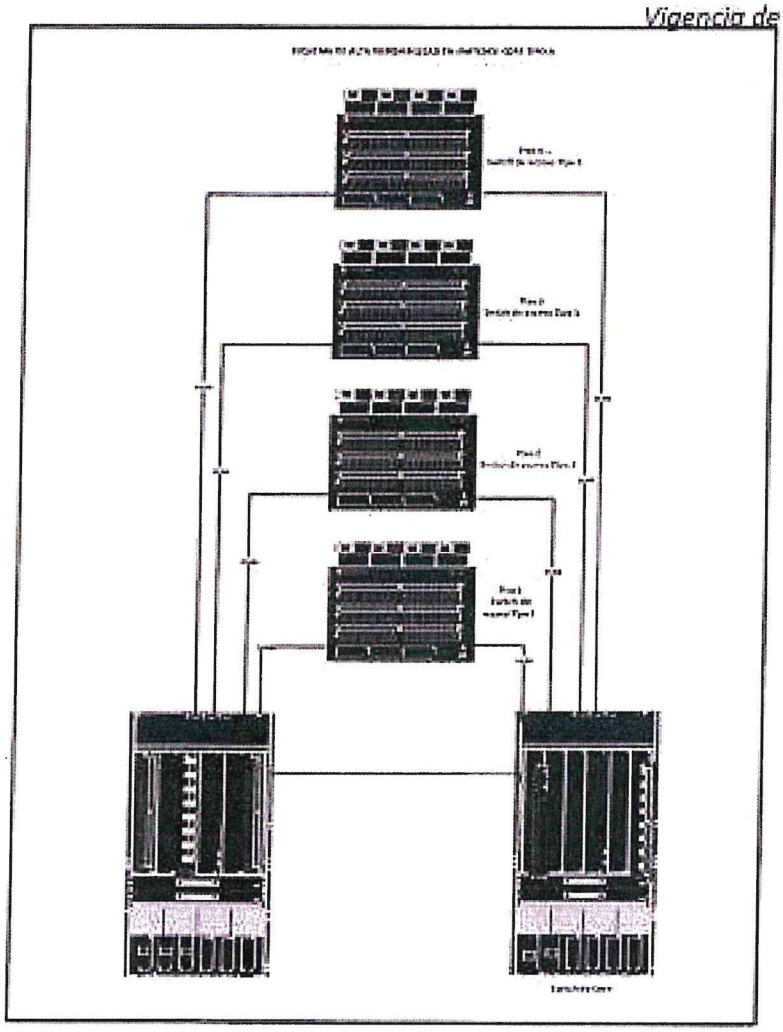
TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.



Los Switches CORE que conformen el esquema de alta disponibilidad en las Oficinas Centrales del Instituto FONACOT (Sede Insurgentes), cumplirán con al menos las siguientes características tecnicas:

- El equipo proveerá al menos 06 ranuras para la inserción de tarjetas y crecimientos en un futuro.
- El equipo será capaz de soportar las siguientes densidades de puertos:
  - 432 puertos 10/100/1000 Base-TX o 1000Base-X SFP
  - 168 puertos 10GBase-X SFP+
  - 36 puertos 40GBase-X QSFP+
    - Soportará voltaje de Alimentación 100-240 VCA, a una frecuencia de 50-60 Hz

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Incluirá Ventiladores y Fuentes de alimentación de tipo Hot-swappable
- Proveerá la facilidad de insertar, remover o reemplazar módulos, sin interrumpir laoperación del sistema.
- El equipo incluirá al menos 2 fuentes de poder internas en modo redundante, para garantizar la total operación de la unidad, aun cuando una fuente de poder haya fallado. Las fuentes de poder redundantes realizarán balanceo de carga.
- Soportará la funcionalidad de "Virtual Chassis", "Chassis Bonding", "Virtual Switching System" o similar. Con la finalidad de poder realizar configuraciones de alta disponibilidad a nivel de L2, sin que existan los problemas y tiempo de re- convergencia por los protocolos de Spanning Tree, permitiendo la Administraciónde dos switches como uno sólo.
- Acorde a la arquitectura del equipo, incluirá redundancia en tarjetas supervisoras (controladoras) o en su defecto un esquema de procesamiento distribuido
- Incluirá al menos para los 2 equipos de Oficinas Centrales:
  - 96 Puertos 10/100/1000Base-TX RJ45 PoE+
  - 10 puertos Ethernet 10GBase-X
    - Soportará auto-mdi/mdix, auto-sensing y auto-negotiation en todos los puertos10/100/1000 Base-TX
    - Contará con puerto serial USB y RJ45 para configuración del equipo y carga defirmware, así como de carga y descarga de archivos.
    - Soportará Power over Ethernet con estándares 802.3af/802.3at
    - La capacidad de conmutación o switching capacity del chasis será de al menos 96 Gbps
    - Un Throughput IPv4 por chasis de al menos 720 Mpps
    - Soportar un desempeño mínimo por cada tarjeta de servicio (tarjeta I/O) de 160Gbps
    - Contar con al menos 10 colas de prioridad (Queues) por puerto
    - Soportará al menos 65000 MAC Address
    - Soportará al menos 4000 VLANs
    - Soportará e incluir Netflow v9.
    - Contará con el soporte de Jumbo frames de 9,216 bytes
    - Soportará SNMP v1/v2c/v3
    - Soportará al menos 15 mirrors por chasis, los cuales pueden ser de:
      - Uno a uno
      - Uno a muchos
      - Muchos a uno
      - Mirror de Vlans
    - Soportará Remote Port Mirror

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de lo mismo

Ciudad de México a 17 de mayo de 2022.

- Soportará CDP v1/2
- Incluirá la funcionalidad Proxy ARP
- Incluirá la funcionalidad Bi-directional Forwarding Detection (BFD)
- Contará con la funcionalidad Q-in-Q
- Será capaz de implementar NTP (Network Time Protocol) ó SNTP (Simple NetworkTime Protocol).
- Incluirá la funcionalidad de NAT
- Con el sistema operativo base, proveerá la función de balanceo de servicios, de tal forma que se puedan generar gateways virtuales de servicios como WEB, SMTP o algún otro aplicativo, sin la necesidad de agregar módulos especiales y licenciamiento para este propósito.
- Soportará la funcionalidad DHCP Server / Relay
- Soportará la funcionalidad Unidirectional Link Detection
- Incluirá la funcionalidad de Supresión de Broadcast
- Soportará el estándar 802.1ak MVRP
- Incluirá la funcionalidad Generic VLAN Registration Protocol (GVRP)
- Soportará IGMP v1/v2/v3
- Soportará los siguientes Estándares:
  - 802.3u Fast Ethernet
  - 802.3ab Gigabit Ethernet
  - 802.3z Gigabit Ethernet
  - 802.3ae 10 Gigabit Ethernet
  - 802.3an 10Gase-T
- Soportará los siguientes Estándares:
  - 802.1Q VLANs
  - 802.1D MAC Bridges
  - 802.1w RSTP
  - 802.1s MST
  - 802.1t Path Cost
  - 802.3ad Link Aggregation
  - 802.3ae Gigabit Ethernet
  - 802.3x Flow Control
  - 802 1ab LLDP-MED
- Soportará el protocolo 802.3ad permitiendo la agrupación de hasta 190 LAG por chasis, y hasta 64 puertos por cada LAG.
- Soportará los siguientes Estándares:
  - 802.1Qaz ETS y DCBx
  - 802.1Qbb PFC
  - 802.1Qau Congestion Notification
  - Soportará Ruteo Estático
  - Soportará ACLs Estándar y Extendidas

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Incluirá Policy-Based Routing (PBR)
- Soportará VRF en IPv4/IPv6
- Soportará OSPF
- Soportará OSPF ECMP
  - Soportará RIP v2
  - Soportará BGPv4
  - Soportará L2VPN
  - Soportará L3VPN over native MPLS
  - Soportará PIM-DM
  - Soportará al menos 1,000,000 de entradas en la tabla de ruteo IPv4
  - Soportará al menos 50,000 de entradas en la tabla de ruteo IPv6
  - Soportará al menos 100 interfaces IPv6
  - Soportará al menos 10 IP helper address por interface
  - Incluirá las siguientes funcionalidades para IPv6:
- Ruteo estático
- DVMRPv3
- OSPFv3
- Ruteo basado en políticas IPv6 (PBR)
- PIM-SM v6
- PIM-SSM v6
- MLD v1/v2
- RIPng
- IPv6 ACLs
- DHCP relay
- Neighbor Discovery
- IPSec para OSPFv3
  - Soportará los siguientes estandares:
- RFC 1195 Use of OSI IS-IS for Routing in TCP/IP
- RFC 1265 BGP Protocol Analysis
- RFC 1266 Experience with the BGP Protocol
- RFC 1519 CIDR
- RFC 3101 OSPFv2 NSSA
- RFC 1657 Managed Objects for BGP-4 using SMIv2
- RFC 1771 A Border Gateway Protocol 4 (BGP-4)
- RFC 1772 Application of BGP in the Internet
- RFC 1773 Experience with the BGP-4 protocol
- RFC 1774 BGP-4 Protocol Analysis
- RFC 1812 General Routing/RIP Requirements
- RFC 1853 IP in IP Tunneling
- RFC 1886 DNS Extensions to support IP version 6
- RFC 1930 Guidelines for creation, selection, and registration of an

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

AutonomousSystem (AS)

- RFC 1966 BGP Route Reflection
- RFC 1981 Path MTU Discovery for IPv6
- RFC 1998 BGP Community Attribute in Multi-home Routing
- RFC 2003 IP Encapsulation within IP
- RFC 2082 RIP-II MD5 Authentication
- RFC 2260 Support for Multi-homed Multi-prov
- RFC 2270 Dedicated AS for Sites Homed to one Provider
- RFC 2373 Address notation compression
- RFC2374 IPv6 Aggregatable Global Unicast Address Format
- RFC2375 IPv6 Multicast Address Assignments
- RFC 2391 Load Sharing Using Network Address Translation(LSNAT)
- RFC2401 Security Architecture for the Internet Protocol
- RFC2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC2406 IP Encapsulating Security Payload (ESP)
- RFC2407 Internet IP Security Domain of Interpretation for ISAKMP
- RFC2408 Internet Security Association and Key Management Proto-col (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2450 Proposed TLA and NLA Assignment Rule
- RFC 2460 IPv6 Specification
- RFC 2462 IPv6 Stateless Address Auto-configuration
- RFC 2464 Transmission of IPv6 over Ethernet
- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2474 Definition of DS Field in the IPv4/v6 Headers
- RFC 2519 A Framework for Inter-Domain Route Aggregation
- RFC 2547 BGP/MPLS VPNs
- RFC 2553 BasICSocket Interface Extensions for IPv6
- RFC 2577 FTP Security Considerations
- RFC 2597 Assured Forwarding PHB Group
- RFC 2685 Virtual Private Networks Identifier
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2715 Interoperability Rules for Multicast Routing Protocols
- RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2784 Generic Routing Encapsulation
- RFC 2890 Key and Sequence Number Extensions to GRE
- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
- RFC 2894 Router Renumbering
- RFC 2918 Route Refresh Capability for BGP
- RFC 2966 Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- RFC 3065 Autonomous System Confederations for BGP
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3162 RADIUS and IPv6
- RFC 3345 BGP Persistent Route Oscillation
- RFC 3359 TLV Codepoints in IS-IS
- RFC 3373 Three-Way Handshake for IS-IS
- RFC 3567 IS-IS Cryptographic Authentication
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC3596 DNS Extensions to Support IP Version 6
- RFC 3768 VRRP
- RFC 3769 Requirements for IPv6 Prefix Delegation
- RFC 3810 MLDv2 for IPv6
- RFC 3879 Deprecating Site Local Addresses
- RFC 3956 Embedding the RP Address in IPv6 MCAST Address
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4023 Encapsulating MPLS in IP
- RFC 4109 Algorithms for IKEv1
- RFC 4191 Default Router Preferences and More-Specific Routes
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4213 Basic Transition Mechanisms for IPv6
- RFC 4222 Prioritized Treatment of OSPFv2 Packets
- RFC 4264 BGP Wedgies
- RFC 4265 Definition of Textual Conventions for (VPN) Management
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4272 BGP Security Vulnerabilities Analysis
- RFC 4273 Managed Objects for BGP-4 using SMIv2
- RFC 4274 BGP-4 Protocol Analysis
- RFC 4276 BGP-4 Implementation Report
- RFC 4277 Experience with the BGP-4 protocol
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4301 Security Architecture for IP
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4305 Crypto Algorithm Requirements for ESP and AH
- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in IKEv2
- RFC 4308 Cryptographic Suites for IPSec
- RFC 4360 BGP Extended Communities Attribute
- RFC 4364 BGP/MPLS IP VPNs
- RFC 4365 Applicability Statement for BGP/MPLS IP VPNs
- RFC 4384 BGP Communities for Data Collection

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- RFC 4443 ICMPv6 for IPv6
- RFC 4456 BGP Route Reflection
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4451 BGP MULTI_EXIT_DISC (MED) Considerations
- RFC 4541 MLD Snooping
- RFC 4552 Authentication/Confidentiality for OSPFv3
- RFC 4601 PIM-SM
- RFC 4604 IGMPv3 & MLDv2 & Source-Specific Multicast
- RFC 4607 Source-Specific Multicast for IP
- RFC 4608 PIM--SSM in 232/8
- RFC 4610 Anycast-RP Using PIM
- RFC 4611 MSDP Deployment Scenarios
- RFC 4632 Classless Inter-Domain Routing (CIDR)
- RFC 4659 BGP-MPLS (VPN) Extension for IPv6 VPN
- RFC 4724 Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4835 CryptoAlgorithm Requirements for ESP and AH
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 4884 Extended ICMP Multi-Part Messages
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 5059 Bootstrap Router (BSR) Mechanism for (PIM)
- RFC 5065 Autonomous System Confederations for BGP
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 5186 IGMPv3/MLDv2/MCAST Routing Protocol Interaction
- RFC 5187 OSPFv3 Graceful Restart
- RFC 5240 PIM Bootstrap Router MIB
- RFC 5250 The OSPF Opaque LSA Option
- RFC 5291 Outbound Route Filtering Capability for BGP-4
- RFC 5292 Address-Prefix-Outbound Route Filter for BGP-4
- RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 5302 Domain-wide Prefix Distribution with IS-IS
- RFC 5303 3Way Handshake for IS-IS P2P Adjacencies
- RFC 5304 IS-IS Cryptographic Authentication
- RFC 5306 Restart Signaling for IS-IScol for BGP L3 VPNs
- Soportar las siguientes MIB:
- RFC 2578 SNMPv2 SMI
- RFC 3418 SNMPv2 MIB
- RFC 2576 SNMP-Community MIB
- RFC 2863 IF MIB
- RFC 3621 Power Ethernet MIB
- RFC 4750 OSPFv2 MIB

- CISCO CDP MIB
- CISCO NETFLOW MIB
- Incluirá la funcionalidad de Redirección de peticiones

Web Funcionalidades de Administración y Monitoreo

- El equipo será Administrado por
  - Puerto de Consola
  - SNMP
  - Remotamente por Sesión VTY
    - Soportará SSHv2
    - Soportará Telnet como Servidor y Cliente
    - Soportará SNTP o NTP
    - Soportará Interface Web de Gestión
    - Poseerá una función de actualización de firmware y almacenamiento de imágenesde respaldo en caso de que el proceso falle o bien la imagen se encuentre dañadao corrupta.
    - Soportará Múltiples archivos de configuración
    - Soportará download de imágenes de Sistema Operativo o Firmware y archivos deconfiguración desde servidores:
  - FTP
  - TFTP
  - SCP
    - Incluirá una funcionalidad para realizar upgrades de Sistema Operativo o Firmwarede forma gradual por tarjeta y por Grupo de Tarjetas, de forma que no se reinicieel equipo completo para aplicar actualizaciones de Sistema Operativo.
    - Incluirá funcionalidad de IP SLA para la medición de jitter y delay
    - Soportará VLAN de Administración

    - Capacidad de envío de logs de acuerdo a su grado de severidad al menos hacia 8servidores Syslog, de ser requerido.
    - Soportará la Autenticación y Encripción por algoritmos aprobados FIPS
    - Soportará la funcionalidad de especificar por usuario administrador la hora de inicioy termino de acceso al equipo.
    - Soportará la funcionalidad de especificar la cantidad máxima de sesiones simultáneas por usuario administrador en el switch.
    - Soportará la funcionalidad de especificar la cantidad máxima de días de inactividad por usuario administrador, antes de que la cuenta sea deshabilitada en el switch
    - Soportará la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

de cada uno de este tipo de caracteres:

- Letra mayúscula
- Letra minúscula
- Numero
- Caracteres especiales
  - Soportará 802.3 2008 Clause 57 Ethernet OAM – Link Layer OAM

Funciones de Control y Seguridad

- Soportará rate-limiting desde 8 Kbps
- Soportará rate-limiting de entrada y salida
- Soportará IP ToS/DSCP Marking/Remarking
- Soportará los siguientes Controles de Flood-Limiting por Puerto:
  - Broadcast
  - Multicast
  - Unknown Unicast
- Detectará dispositivos de telefonía IP o video de al menos 2 distintos fabricantes, una vez detectados aplicara configuración de forma dinámica en el puerto.
- Detectará dispositivos de telefonía IP de terceros para aplicar configuración de forma dinámica en el puerto, los dispositivos de teléfonia podrán emplear los protocolos:
  - H.323
  - SIP
- Realizará Clasificacion y QoS de paquetes multicapa basado en usuario y así dar un tratamiento especifico por Grupos de Usuario y Usuario
- Soportará al menos tres distintos mecanismos de gestión de colas (queuing)
- Soportará de múltiples usuarios/dispositivos (como teléfonos IP, computadoras, impresoras, fotocopiadoras, cámaras de seguridad, lectores de tarjeta, servidores virtuales, etc.) y múltiples métodos de autenticación (por 802.1x, WEP y MAC o lacombinación de estos) en un puerto o en todos los puertos, soportando por lo menos 1000 usuarios/dispositivos autenticados por módulo.
- Soportará 802.1D
- Soportará 802.1p

- Poseerá la funcionalidad de poder detectar eventos de intermitencias o flaps en lospuertos y llevará a cabo acciones como inhabilitar el(los) puerto(s) involucrados y generar una entrada de log y/o envío de traps.
- Protección automática para conexión de dispositivos de comunicación no permitidos, los cuales activen el protocolo de STP y generen alguna

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

reconvergencia en la red.

- Soportará autentificación de usuarios administradores de equipos mediante TACACS+.
- Soportará al menos 9 grupos de RMON
- Será capaz de clasificar tráfico en base a los siguientes criterios:

- MAC source address
- MAC destination addres
- Source IPX address
- Destination IPX address
- Source IPX socket
- Destination IPX socket
- Transmission control IPX
- IPX packet type
- IPv6 source address
- IPv6 destination address
- IPv6 flow label
- Source IP address.
- Destination IP address.
- IP fragmentation value.
- UDP source port
- UDP destination port
- TCP source port
- TCP destination port
- ICMP packet type
- Time-To-Live (TTL)
- Type of Service
- ICMPv6 packet type
- VLAN tag
- Port-string
- Incluirá la funcionalidad de limitar el acceso de una MAC Address dada a un puertoespecifico, la cual puede aprender el equipo de forma estática o dinámica

- Incluir mecanismos de mitigación ante los siguientes ataques DoS:

- Bad SIP
- Christmas Tree
- Fragmented ICMP
- ICMP Flood
- Large ICMP
- LANd
- Smurf
- Fraggle Attack

- SYN Flood
  - Contar con al menos 3 distintos mecanismos anti-spoofing
  - Soportará RADIUS accounting / snooping
  - Soportará RFC 3580
  - Soportará prevención de ARP storm
  - El equipo soportará e incluirá una funcionalidad capaz de distinguir la identidad de un usuario/dispositivo que es autenticado en otro switch conectadoa este mismo, pudiendo asignar alguna política de L2, L3 y L4, permitiendo, negando, etiquetando, redireccionando, asignando una prioridad y un rate limiting.
  - Soportará funciones de mitigación de ataques de tipo DoS de tal forma que se pueden configurar umbrales permitidos de cantidad de tráfico, los cuales puedan desencadenar acciones como descartar tráfico excedente, envío de SNMP o logs e inclusive hasta desactivar una o más interfaces.

2.3.1.2 *Esquema de Alta Disponibilidad en Switches CORE Tipo B*

Tecnología en Seguridad y Comunicaciones S.A. de C.V., implementará un esquema de alta disponibilidad en la sede de Plaza de la Republica del Instituto FONACOT, basado en dos Switches CORE de últimageneración con la finalidad de contar con redundancia a nivel backbone de fibra óptica.Es responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerar el dimensionamiento adecuado en cuantoa hardware, licenciamiento, actualizaciones, componentes y cualquier otro elemento que se requiera para la adecuada operación de los equipos que conformen este esquema.

Es responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., garantizar que el esquema de alta disponibilidad implementado mantenga las configuraciones, niveles de seguridad y control de tráficopor servicio y por usuario que actualmente tiene definidas el área técnica Instituto FONACOT. Los equipos CORE propuestos para este esquema, deberán integrarse nativamente con la herramienta de administración de la Red, propiedad del Instituto FONACOT.

A continuación, se muestra el esquema de alta disponibilidad de switches core tipo 2 solicitado en **Plaza de la Republica** para el presente proyecto

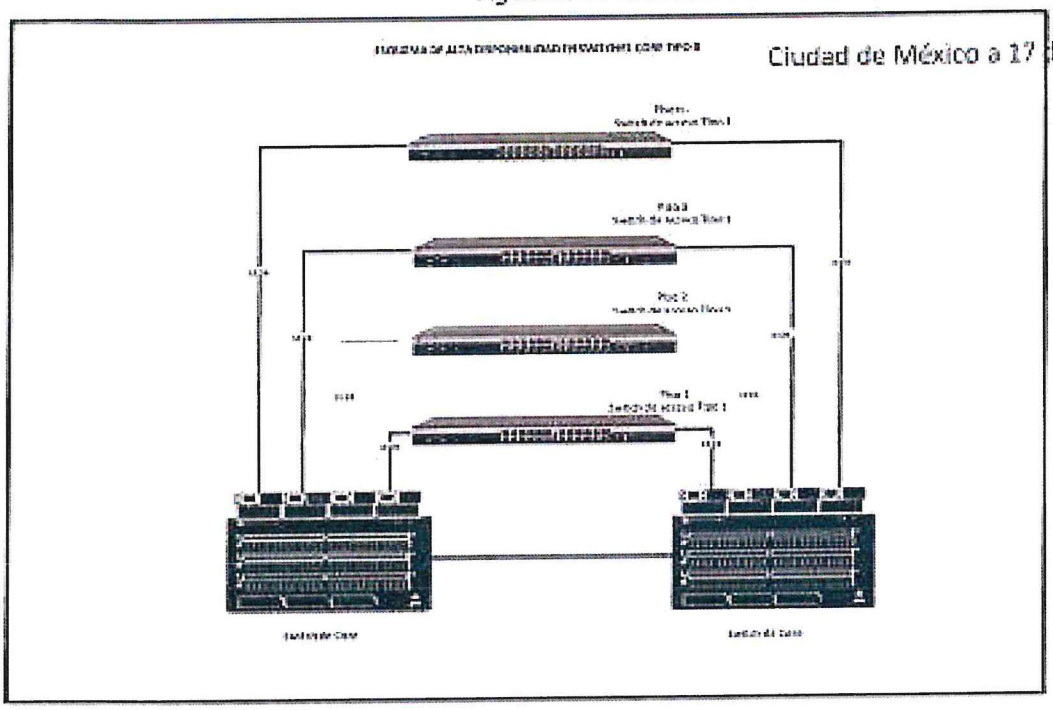
TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.



Los Switches CORE que conformen el esquema de alta disponibilidad en Plaza de la Republica del Instituto FONACOT, deberán cumplir con al menos las siguientes características tecnicas:

- El equipo proveerá al menos 03 ranuras para la inserción de tarjetas y crecimientos en un futuro.
- El equipo será capaz de soportar las siguientes densidades de puertos
  - 216 puertos 10/100/1000 Base-TX o 1000Base-X SFP
  - 96 puertos 10GBase-X SFP+
- Soportará voltaje de Alimentación 100-240 VCA, a una frecuencia de 50-60 Hz
- Incluirá Ventiladores y Fuentes de alimentación de tipo Hot-swappable
- Proveerá la facilidad de insertar, remover o reemplazar módulos, sin interrumpir laoperación del sistema.
- El equipo incluirá al menos 2 fuentes de poder internas en modo redundante, para garantizar la total operación de la unidad, aun cuando una fuente de poder haya fallado. Las fuentes de poder redundantes deberán de realizar balanceo de carga.
- Sportará la funcionalidad de "Virtual Chassis", "Chassis Bonding", "Virtual Switching System" o similar. Con la finalidad de poder realizar configuraciones de alta disponibilidad a nivel de L2, sin que existan los problemas y tiempo de re-convergencia por los protocolos de Spanning Tree, permitiendo la Administración

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

de dos switches como uno sólo.

- Acorde a la arquitectura del equipo, incluirá redundancia en tarjetas supervisoras (controladoras) o en su defecto un esquema de procesamiento distribuido
- Incluirá al menos para los 2 equipos de Plaza de la Republica:
  - 48 Puertos 10/100/1000Base-TX RJ45 PoE+
  - 12puertos Ethernet 10GBase X
- Soportará auto-mdi/mdix, auto-sensing y auto-negotiation en todos los puertos10/100/1000 Base-TX
- Contará con puerto serial USB y RJ45 para configuración del equipo y carga defirmware, así como de carga y descarga de archivos.
- Soportará Power over Ethernet con estándares 802.3af/802.3at
- La capacidad de conmutación o switching capacity del chasis será de al menos 360 Gbps
- Un Throughput IPv4 por chasis de al menos 90 Mpps
- Soportará un desempeño mínimo por cada tarjeta de servicio (tarjeta I/O) de 160Gbps
- Contará con al menos 10 colas de prioridad (Queues) por puerto
- Soportará al menos 128000 MAC Address
- Soportará al menos 4000 VLANs
- Soportará e incluirá Netflow v9, v9 para el monitoreo de al menos 20 interfases del equipo, y soportará al menos configuración de 4 colectores posibles,sin la necesidad de un licenciamiento adicional, cambio o modificación del hardware para el empleo de dicho protocolo, y cuyo empleo no impacte en el desempeño del equipo tanto en funcionalidades de switching como de routing
- Contará con el soporte de Jumbo frames de 9216bytes
- Soportará SNMP v1/v2c/v3
- Soportará al menos 15 mirrors por chasis, los cuales pueden ser de:
  - Uno a uno
  - Uno a muchos
  - Muchos a uno
  - Mirror de Vlans
- Soportará Remote Port Mirror
- Soportará CDP v1/2
- Incluirá la funcionalidad Proxy ARP
- Incluirá la funcionalidad Bi-directional Forwarding Detection (BFD)
- Contará con la funcionalidad Q-in-Q
- Será capaz de implementar NTP (Network Time Protocol) ó SNTP (Simple NetworkTime Protocol).
- Incluirá la funcionalidad de NAT

Con el sistema operativo base, proveerá la función de balanceo de servicios,de tal

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 10 de mayo de 2022.

- forma que se puedan generar gateways virtuales de servicios, SWG o algún otro aplicativo, sin la necesidad de agregar módulos especiales y licenciamiento para este propósito.
- Soportará la funcionalidad DHCP Server / Relay
- Soportará la funcionalidad Unidirectional Link Detection

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Incluirá la funcionalidad de Supresión de Broadcast
- Soportará el estándar 802.1ak MVRP
- Incluirá la funcionalidad Generic VLAN Registration Protocol (GVRP)
- Soportará IGMP v1/v2/v3
- Soportará los siguientes Estándares:
  - 802.3u Fast Ethernet
  - 802.3ab Gigabit Ethernet
  - 802.3z Gigabit Ethernet
  - 802.3ae 10 Gigabit Ethernet
  - 802.3an 10Gase-T
- Soportará los siguientes Estándares:
  - 802.1Q VLANs
  - 802.1D MAC Bridges
  - 802.1w RSTP
  - 802.1s MST
  - 802.1t Path Cost
  - 802.3ad Link Aggregation
  - 802.3ae Gigabit Ethernet
  - 802.3x Flow Control
  - 802 1ab LLDP-MED
- Soportará el protocolo 802.3ad permitiendo la agrupación de hasta 190 LAG porchasis, y hasta 64 puertos por cada LAG.
- Soportará los siguientes Estándares
  - 802.1Qaz ETS y DCBx
  - 802.1Qbb PFC
  - 802.1Qau Congestion Notification
  - Soportará Ruteo Estático
  - Soportará ACLs Estándar y Extendidas
  - Incluirá Policy-Based Routing (PBR)
  - Soportará VRF en IPv4/IPv6
  - Soportará OSPF
  - Soportará OSPF ECMP
- Soportará RIP v2
- Soportará BGPv4
- Soportará L2VPN
- Soportará L3VPN over native MPLS
- Soportará PIM-DM
- Soportará al menos 1,000,000 de entradas en la tabla de ruteo IPv4
- Soportará al menos 50,000 de entradas en la tabla de ruteo IPv6
- Soportará al menos 100 interfaces IPv6
- Soportará al menos 10 IP helper address por interface

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Incluirá las siguientes funcionalidades para IPv6:
  - Ruteo estático
  - DVMRPv3
  - OSPFv3
  - Ruteo basado en políticas IPv6 (PBR)
  - PIM-SM v6
  - PIM-SSM v6
  - MLD v1/v2
  - RIPng
  - IPv6 ACLs
  - DHCP relay
  - Neighbor Discovery
  - IPSec para OSPFv3
- Soportará los siguientes estandares:
  - RFC 1195 Use of OSI IS-IS for Routing in TCP/IP
  - RFC 1265 BGP Protocol Analysis
  - RFC 1266 Experience with the BGP Protocol
  - RFC 1519 CIDR
  - RFC 3101 OSPFv2 NSSA
  - RFC 1657 Managed Objects for BGP-4 using SMIv2
  - RFC 1771 A Border Gateway Protocol 4 (BGP-4)
  - RFC 1772 Application of BGP in the Internet
  - RFC 1773 Experience with the BGP-4 protocol
  - RFC 1774 BGP-4 Protocol Analysis
  - RFC 1812 General Routing/RIP Requirements
  - RFC 1853 IP in IP Tunneling
  - RFC 1886 DNS Extensions to support IP version 6
  - RFC 1930 Guidelines for creation, selection, and registration of an Autonomous System (AS)
  - RFC 1966 BGP Route Reflection
  - RFC 1981 Path MTU Discovery for IPv6
  - RFC 1998 BGP Community Attribute in Multi-home Routing
  - RFC 2003 IP Encapsulation within IP
  - RFC 2082 RIP-II MD5 Authentication
  - RFC 2260 Support for Multi-homed Multi-prov
  - RFC 2270 Dedicated AS for Sites Homed to one Provider
  - RFC 2373 Address notation compression
  - RFC2374 IPv6 Aggregatable Global Unicast Address Format
  - RFC2375 IPv6 Multicast Address Assignments
  - RFC 2391 Load Sharing Using Network Address Translation(LSNAT)
  - RFC2401 Security Architecture for the Internet Protocol
  - RFC2404 The Use of HMAC-SHA-1-96 within ESP and AH

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

- RFC2406 IP Encapsulating Security Payload (ESP)
- RFC2407 Internet IP Security Domain of Interpretation for ISAKMP
- RFC2408 Internet Security Association and Key Management Proto-col (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2450 Proposed TLA and NLA Assignment Rule
- RFC 2460 IPv6 Specification
- RFC 2462 IPv6 Stateless Address Auto-configuration
- RFC 2464 Transmission of IPv6 over Ethernet
- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2474 Definition of DS Field in the IPv4/v6 Headers
- RFC 2519 A Framework for Inter-Domain Route Aggregation
- RFC 2547 BGP/MPLS VPNs
- RFC 2553 BasicSocket Interface Extensions for IPv6
- RFC 2577 FTP Security Considerations
- RFC 2597 Assured Forwarding PHB Group
- RFC 2685 Virtual Private Networks Identifier
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2715 Interoperability Rules for Multicast Routing Protocols
- RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2784 Generic Routing Encapsulation
- RFC 2890 Key and Sequence Number Extensions to GRE
- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
- RFC 2894 Router Renumbering
- RFC 2918 Route Refresh Capability for BGP
- RFC 2966 Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3065 Autonomous System Confederations for BGP
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3162 RADIUS and IPv6
- RFC 3345 BGP Persistent Route Oscillation
- RFC 3359 TLV Codepoints in IS-IS
- RFC 3373 Three-Way Handshake for IS-IS
- RFC 3567 IS-IS Cryptographic Authentication
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC3596 DNS Extensions to Support IP Version 6
- RFC 3768 VRRP
- RFC 3769 Requirements for IPv6 Prefix Delegation
- RFC 3810 MLDv2 for IPv6

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- RFC 3879 Deprecating Site Local Addresses
- RFC 3956 Embedding the RP Address in IPv6 Multicast Address
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4023 Encapsulating MPLS in IP
- RFC 4109 Algorithms for IKEv1
- RFC 4191 Default Router Preferences and More-Specific Routes
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4213 Basic Transition Mechanisms for IPv6
- RFC 4222 Prioritized Treatment of OSPFv2 Packets
- RFC 4264 BGP Wedgies
- RFC 4265 Definition of Textual Conventions for (VPN) Management
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4272 BGP Security Vulnerabilities Analysis
- RFC 4273 Managed Objects for BGP-4 using SMIv2
- RFC 4274 BGP-4 Protocol Analysis
- RFC 4276 BGP-4 Implementation Report
- RFC 4277 Experience with the BGP-4 protocol
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4301 Security Architecture for IP
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4305 Crypto Algorithm Requirements for ESP and AH
- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in IKEv2
- RFC 4308 Cryptographic Suites for IPSec
- RFC 4360 BGP Extended Communities Attribute
- RFC 4364 BGP/MPLS IP VPNs
- RFC 4365 Applicability Statement for BGP/MPLS IP VPNs
- RFC 4384 BGP Communities for Data Collection
- RFC 4443 ICMPv6 for IPv6
- RFC 4456 BGP Route Reflection
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4451 BGP MULTI_EXIT_DISC (MED) Considerations
- RFC 4541 MLD Snooping
- RFC 4552 Authentication/Confidentiality for OSPFv3
- RFC 4601 PIM-SM
- RFC 4604 IGMPv3 & MLDv2 & Source-Specific Multicast
- RFC 4607 Source-Specific Multicast for IP
- RFC 4608 PIM--SSM in 232/8
- RFC 4610 Anycast-RP Using PIM
- RFC 4611 MSDP Deployment Scenarios
- RFC 4632 Classless Inter-Domain Routing (CIDR)

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

- RFC 4659 BGP-MPLS (VPN) Extension for IPv6 VPN
- RFC 4724 Graceful Restart Mechanism for BGP Ciudad de México a 17 de mayo de 2022.
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4835 CryptoAlgorithm Requirements for ESP and AH
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 4884 Extended ICMP Multi-Part Messages
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 5059 Bootstrap Router (BSR) Mechanism for (PIM)
- RFC 5065 Autonomous System Confederations for BGP
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 5186 IGMPv3/MLDv2/MCAST Routing Protocol Interaction
- RFC 5187 OSPFv3 Graceful Restart
- RFC 5240 PIM Bootstrap Router MIB
- RFC 5250 The OSPF Opaque LSA Option
- RFC 5291 Outbound Route Filtering Capability for BGP-4
- RFC 5292 Address-Prefix-Outbound Route Filter for BGP-4
- RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 5302 Domain-wide Prefix Distribution with IS-IS
- RFC 5303 3Way Handshake for IS-IS P2P Adjacencies
- RFC 5304 IS-IS Cryptographic Authentication
- RFC 5306 Restart Signaling for IS-IScol for BGP L3 VPNs

- Soportará las siguientes MIB:
  - RFC 2578 SNMPv2 SMI
  - RFC 3418 SNMPv2 MIB
  - RFC 2576 SNMP-Community MIB
  - RFC 2863 IF MIB
  - RFC 3621 Power Ethernet MIB
  - RFC 4750 OSPFv2 MIB
- CISCO CDP MIB
- CISCO NETFLOW MIB
- Incluirá la funcionalidad de Redirección de peticiones

WebFuncionalidades de Administración y Monitoreo

- El equipo será Administrado por:
  - Puerto de Consola
  - SNMP
  - Remotamente por Sesión VTY
- Soportará SSHv2
- Soportará Telnet como Servidor y Cliente
- Soportará SNTP o NTP
- Soportará Interface Web de Gestión
- Poseerá una función de actualización de firmware y almacenamiento de imágenes

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

de respaldo en caso de que el proceso falle o bien la imagen se encuentre dañada o corrupta.

- Soportará Múltiples archivos de configuración
- Soportará download de imágenes de Sistema Operativo o Firmware y archivos de configuración desde servidores:
  - FTP
  - TFTP
  - SCP
- Incluirá una funcionalidad para realizar upgrades de Sistema Operativo o Firmware de forma gradual por tarjeta y por Grupo de Tarjetas, de forma que no se reinicie el equipo completo para aplicar actualizaciones de Sistema Operativo.
- Incluirá funcionalidad de IP SLA para la medición de jitter y delay
- Soportará VLAN de Administración
- Capacidad de envío de logs de acuerdo a su grado de severidad al menos hacia 8 servidores Syslog, de ser requerido.
- Soportará la Autenticación y Encripción por algoritmos aprobados FIPS
- Soportará la funcionalidad de especificar por usuario administrador la hora de inicio y termino de acceso al equipo.
- Soportará la funcionalidad de especificar la cantidad máxima de sesiones simultáneas por usuario administrador en el switch.
- Soportará la funcionalidad de especificar la cantidad máxima de días de inactividad por usuario administrador, antes de que la cuenta sea deshabilitada en el switch
- Soportará la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula
  - Letra minúscula
  - Numero
  - Caracteres especiales
- Contará con un packet buffering de 6 GB
- Soportará 802.3 2008 Clause 57 Ethernet OAM – Link Layer

OAMFunciones de Control y Seguridad

- Soportará rate-limiting desde 8 Kbps
- Soportará rate-limiting de entrada y salida
- Soportará IP ToS/DSCP Marking/Remarking
- Soportará los siguientes Controles de Flood-Limiting por Puerto:
  - Broadcast
  - Multicast
  - Unknown Unicast
- Detectará dispositivos de telefonía IP o video de al menos 2 distintos fabricantes,

una vez detectados aplicará configuración de forma dinámica en el puerto.

- Detectará dispositivos de telefonía IP de terceros para aplicar configuración de forma dinámica en el puerto, los dispositivos de teléfonía podrán emplear los protocolos:
  - H.323
  - SIP
  - Realizará Clasificacion y QoS de paquetes multicapa basado en usuario yasi dar un tratamiento especifico por Grupos de Usuario y Usuario
- Soportará al menos tres distintos mecanismos de gestión de colas (queuing)
- Soporte de múltiples usuarios/dispositivos (como teléfonos IP, computadoras, impresoras, fotocopiadoras, cámaras de seguridad, lectores de tarjeta, servidores virtuales, etc.) y múltiples métodos de autenticación (por 802.1x, WEP y MAC o la combinación de estos) en un puerto o en todos los puertos, soportando por lo menos 1000 usuarios/dispositivos autenticados por módulo.
- Soportará 802.1D
- Soportará 802.1p
- Poseerá la funcionalidad de poder detectar eventos de intermitencias o flaps en los puertos y llevar a cabo acciones como inhabilitar el(los) puerto(s) involucrados y generar una entrada de log y/o envio de traps.
- Protección automática para conexión de dispositivos de comunicación no permitidos, los cuales activen el protocolo de STP y generen alguna reconvergencia en la red.

- Soportará autentificación de usuarios administradores de equipos mediante TACACS+.
- Soportará al menos 9 grupos de RMON
- Será capaz de clasificar tráfico en base a los siguientes criterios:
  - MAC source address
  - MAC destination addres
  - Source IPX address
  - Destination IPX address
  - Source IPX socket
  - Destination IPX socket
  - Transmission control IPX
  - IPX packet type
  - IPv6 source address
  - IPv6 destination address
  - IPv6 flow label
  - Source IP address.
  - Destination IP address.
  - IP fragmentation value.

- UDP source port
- UDP destination port
- TCP source port
- TCP destination port
- ICMP packet type
- Time-To-Live (TTL)
- Type of Service
- ICMPv6 packet type
- VLAN tag
- Port-string
- Incluirá la funcionalidad de limitar el acceso de una MAC Address dada a un puerto especifico, la cual puede aprender el equipo de forma estática o dinámica

- Incluirá mecanismos de mitigación ante los siguientes ataques DoS:
  - Bad SIP
  - Christmas Tree
  - Fragmented ICMP
  - ICMP Flood
  - Large ICMP
  - LANd
  - Smurf
  - Fraggle Attack
  - SYN Flood
- Soportará RADIUS accounting / snooping
- Contará con al menos 3 mecanismos anti spoofing
- Soportará RFC 3580
- Soportará prevención de ARP storm

- El equipo soportará e incluirá una funcionalidad capaz de distinguir laidentidad de un usuario/dispositivo que es autenticado en otro switch conectadoa este mismo, pudiendo asignar alguna política de L2, L3 y L4, permitiendo, negando, etiquetando, redireccionando, asignando una prioridad y un rate limiting.
- Soportará funciones de mitigación de ataques de tipo DoS de tal forma que se pueden configurar umbrales permitidos de cantidad de tráfico, los cuales puedan desencadenar acciones como descartar tráfico excedente, envío de SNMP o logs e inclusive hasta desactivar una o más interfaces.

2.3.2. Switches de acceso

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Tecnologia en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado mantendrá la operación en todas las sucursales del Tostituto FONACOT incluyendo Oficinas Centrales y Plaza de la Republica. Para el casoparticular de estos dos últimos sitios, Tecnología en Seguridad y Comunicaciones S.A. de C.V., implementará un esquema de alta disponibilidad en conjunto con los switches de CORE propuestos, para lo cual Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerará el dimensionamiento adecuado en cuanto a hardware, licenciamiento, actualizaciones, componentes y cualquier otro elemento que se requiera para la adecuada operación de este esquema.

Los switches de acceso propuestos por Tecnología en Seguridad y Comunicaciones S.A. de C.V., para este servicio, cumplirán con al menos las siguientes caracteristicas técnicas

23.2.1. Switch de acceso Tipo1

- El equipo proveerá al menos 03 ranuras para la inserción de tarjetas y crecimientos en un futuro.
- El equipo será capaz de soportar las siguientes densidades de puertos:
  - 216 puertos 10/100/1000 Base-TX o 1000Base-X SFP
  - 96 puertos 10GBase-X SFP

  Soportará voltaje de Alimentación 100-240 VCA, a una frecuencia de 50-60 Hz
- Incluirá Ventiladores y Fuentes de alimentación de tipo Hot-swappable
- Proveerá la facilidad de insertar, remover o reemplazar módulos, sin interrumpir la operación del sistema.
- El equipo incluirá al menos 2 fuentes de poder internas en modo redundante, para garantizar la total operación de la unidad, aun cuando una fuente de poder haya fallado. Las fuentes de poder redundantes deberán de realizar balanceo de carga.
- Soportar la funcionalidad de "Virtual Chassis", "Chassis Bonding", "Virtual Switching System" o similar. Con la finalidad de poder realizar configuraciones de alta disponibilidad a nivel de L2, sin que existan los problemas y tiempo de re-convergencia por los protocolos de Spanning Tree, permitiendo la Administración de dos switches como uno sólo.
- Acorde a la arquitectura del equipo, incluirá redundancia en tarjetas supervisoras (controladoras) o en su defecto un esquema de procesamiento distribuido
- Incluirá al menos:
  - 144 Puertos 10/100/1000Base-TX RJ45 PoE+

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México, 17 de mayo de 2022.

- Se incluirán al menos 2 conectores opticos 10G SR SFP+
- Soportará auto-mdi/mdix, auto-sensing y auto-negotiation en todos los puertos 10/100/1000 Base-TX
- Contar con puerto serial USB y RJ45 para configuración del equipo y carga de firmware, así como de carga y descarga de archivos.
- Soportará Power over Ethernet con estándares 802.3af/802.3at
- La capacidad de conmutación o switching capacity del chasis será de al menos 360 Gbps
- Un Throughput IPv4 por chasis de al menos 360 Mpps
- Soportará un desempeño mínimo por cada tarjeta de servicio (tarjeta I/O)de 120 Gbps
- Contará con al menos 10 colas de prioridad (Queues) por puerto
- Soportará al menos 65,000 MAC Address
- Soportará al menos 4000 VLANs
- Soportará e incluir Netflow
- Contará con el soporte de Jumbo frames.
- Soportará SNMP v1/v2c/v3
- Soportará al menos 15 mirrors por chasis, los cuales pueden ser de:
  - Uno a uno
  - Uno a muchos
  - Muchos a uno
  - Mirror de VLANs.
- Soportará Remote Port Mirror
- Soportará CDP v1/2
- Incluirá la funcionalidad Proxy ARP
- Incluirá la funcionalidad Bi-directional Forwarding Detection (BFD)
- Contará con la funcionalidad Q-in-Q
- Será capaz de implementar NTP (Network Time Protocol) ó SNTP (SimpleNetwork Time Protocol).
- Incluirá la funcionalidad de NAT

Con el sistema operativo base, proveerá la función de balanceo deservicios, de tal forma que se puedan generar gateways virtuales de

- servicios como WEB, SMTP o algún otro aplicativo, sin la necesidad de agregar módulos especiales y licenciamiento para este propósito.
- Soportará la funcionalidad DHCP Server / Relay
- Soportará la funcionalidad Unidirectional Link Detection
- Incluirá la funcionalidad de Supresión de Broadcast
- Soportará el estándar 802.1ak MVRP
- Incluirá la funcionalidad Generic VLAN Registration Protocol (GVRP)

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Soportará IGMP v1/v2/v3
- Soportará los siguientes Estándares:
  - 802.3u Fast Ethernet
  - 802.3ab Gigabit Ethernet
  - 802.3z Gigabit Ethernet
  - 802.3ae 10 Gigabit Ethernet
  - 802.3an 10Gase-T
- Soportará los siguientes Estándares:
  - 802.1Q VLANs
  - 802.1D MAC Bridges
  - 802.1w RSTP
  - 802.1s MST
  - 802.1t Path Cost
  - 802.3ad Link Aggregation
  - 802.3ae Gigabit Ethernet
  - 802.3x Flow Control
  - 802.1ab LLDP-MED
- Soportará el protocolo 802.3ad permitiendo la agrupación de hasta 190 LAGpor chasis, y hasta 64 puertos por cada LAG.
- Soportará los siguientes Estándares:
  - 802.1Qaz ETS y DCBx
  - 802.1Qbb PFC
  - 802.1Qau Congestion Notification
  - Soportará Ruteo Estático
  - Soportará ACLs Estándar y Extendidas
  - Incluirá Policy-Based Routing (PBR)
  - Soportará VRF en IPv4/IPv6
  - Soportará OSPF
  - Soportará OSPF ECMP
- Soportará RIP v2
- Soportará BGPv4
- Soportará L2VPN
- Soportará L3VPN over native MPLS
- Soportará PIM-DM
- Soportará al menos 1,000,000 de entradas en la tabla de ruteo IPv4
- Soportará al menos 50,000 de entradas en la tabla de ruteo IPv6
- Soportará al menos 100 interfaces IPv6
- Soportará al menos 10 IP helper address por interface
- Incluirá las siguientes funcionalidades para IPv6:
  - Ruteo estático
  - DVMRPv3

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- OSPFv3
- Ruteo basado en políticas IPv6 (PBR)
- PIM-SM v6
- PIM-SSM v6
- MLD v1/v2
- RIPng
- IPv6 ACLs
- DHCP relay
- Neighbor Discovery
- IPSec para OSPFv3

* Soportará los siguientes estandares:
  - RFC 1195 Use of OSI IS-IS for Routing in TCP/IP
  - RFC 1265 BGP Protocol Analysis
  - RFC 1266 Experience with the BGP Protocol
  - RFC 1519 CIDR
  - RFC 3101 OSPFv2 NSSA
  - RFC 1657 Managed Objects for BGP-4 using SMIv2
  - RFC 1771 A Border Gateway Protocol 4 (BGP-4)
  - RFC 1772 Application of BGP in the Internet
  - RFC 1773 Experience with the BGP-4 protocol
  - RFC 1774 BGP-4 Protocol Analysis
  - RFC 1812 General Routing/RIP Requirements
  - RFC 1853 IP in IP Tunneling
  - RFC 1886 DNS Extensions to support IP version 6
  - RFC 1930 Guidelines for creation, selection, and registration of an Autonomous System (AS)
  - RFC 1966 BGP Route Reflection
  - RFC 1981 Path MTU Discovery for IPv6
  - RFC 1998 BGP Community Attribute in Multi-home Routing
  - RFC 2003 IP Encapsulation within IP
  - RFC 2082 RIP-II MD5 Authentication
  - RFC 2260 Support for Multi-homed Multi-prov
  - RFC 2270 Dedicated AS for Sites Homed to one Provider
  - RFC 2373 Address notation compression
  - RFC2374 IPv6 Aggregatable Global Unicast Address Format
  - RFC2375 IPv6 Multicast Address Assignments
  - RFC 2391 Load Sharing Using Network Address Translation(LSNAT)
  - RFC2401 Security Architecture for the Internet Protocol
  - RFC2404 The Use of HMAC-SHA-1-96 within ESP and AH
  - RFC2406 IP Encapsulating Security Payload (ESP)
  - RFC2407 Internet IP Security Domain of Interpretation for ISAKMP

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- RFC2408 Internet Security Association and Key Management Proto-col (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2450 Proposed TLA and NLA Assignment Rule
- RFC 2460 IPv6 Specification
- RFC 2462 IPv6 Stateless Address Auto-configuration
- RFC 2464 Transmission of IPv6 over Ethernet
- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2474 Definition of DS Field in the IPv4/v6 Headers
- RFC 2519 A Framework for Inter-Domain Route Aggregation
- RFC 2547 BGP/MPLS VPNs
- RFC 2553 BasicSocket Interface Extensions for IPv6
- RFC 2577 FTP Security Considerations
- RFC 2597 Assured Forwarding PHB Group
- RFC 2685 Virtual Private Networks Identifier
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2715 Interoperability Rules for Multicast Routing Protocols
- RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2784 Generic Routing Encapsulation
- RFC 2890 Key and Sequence Number Extensions to GRE
- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
- RFC 2894 Router Renumbering
- RFC 2918 Route Refresh Capability for BGP
- RFC 2966 Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3065 Autonomous System Confederations for BGP
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3162 RADIUS and IPv6
- RFC 3345 BGP Persistent Route Oscillation
- RFC 3359 TLV Codepoints in IS-IS
- RFC 3373 Three-Way Handshake for IS-IS
- RFC 3567 IS-IS Cryptographic Authentication
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC3596 DNS Extensions to Support IP Version 6
- RFC 3768 VRRP
- RFC 3769 Requirements for IPv6 Prefix Delegation
- RFC 3810 MLDv2 for IPv6
- RFC 3879 Deprecating Site Local Addresses
- RFC 3956 Embedding the RP Address in IPv6 MCAST Address

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez. C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4023 Encapsulating MPLS in IP
- RFC 4109 Algorithms for IKEv1
- RFC 4191 Default Router Preferences and More-Specific Routes
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4213 Basic Transition Mechanisms for IPv6
- RFC 4222 Prioritized Treatment of OSPFv2 Packets
- RFC 4264 BGP Wedgies
- RFC 4265 Definition of Textual Conventions for (VPN) Management
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4272 BGP Security Vulnerabilities Analysis

- RFC 4273 Managed Objects for BGP-4 using SMIv2
- RFC 4274 BGP-4 Protocol Analysis
- RFC 4276 BGP-4 Implementation Report
- RFC 4277 Experience with the BGP-4 protocol
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4301 Security Architecture for IP
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4305 Crypto Algorithm Requirements for ESP and AH
- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in IKEv2
- RFC 4308 Cryptographic Suites for IPSec
- RFC 4360 BGP Extended Communities Attribute
- RFC 4364 BGP/MPLS IP VPNs
- RFC 4365 Applicability Statement for BGP/MPLS IP VPNs
- RFC 4384 BGP Communities for Data Collection
- RFC 4443 ICMPv6 for IPv6
- RFC 4456 BGP Route Reflection
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4451 BGP MULTI_EXIT_DISC (MED) Considerations
- RFC 4541 MLD Snooping
- RFC 4552 Authentication/Confidentiality for OSPFv3
- RFC 4601 PIM-SM
- RFC 4604 IGMPv3 & MLDv2 & Source-Specific Multicast
- RFC 4607 Source-Specific Multicast for IP
- RFC 4608 PIM--SSM in 232/8
- RFC 4610 Anycast-RP Using PIM
- RFC 4611 MSDP Deployment Scenarios
- RFC 4632 Classless Inter-Domain Routing (CIDR)
- RFC 4659 BGP-MPLS (VPN) Extension for IPv6 VPN

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- RFC 4724 Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4835 CryptoAlgorithm Requirements for ESP and AH
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 4884 Extended ICMP Multi-Part Messages
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 5059 Bootstrap Router (BSR) Mechanism for (PIM)
- RFC 5065 Autonomous System Confederations for BGP
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 5186 IGMPv3/MLDv2/MCAST Routing Protocol Interaction
- RFC 5187 OSPFv3 Graceful Restart

- RFC 5240 PIM Bootstrap Router MIB
- RFC 5250 The OSPF Opaque LSA Option
- RFC 5291 Outbound Route Filtering Capability for BGP-4
- RFC 5292 Address-Prefix-Outbound Route Filter for BGP-4

- RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 5302 Domain-wide Prefix Distribution with IS-IS
- RFC 5303 3Way Handshake for IS-IS P2P Adjacencies
- RFC 5304 IS-IS Cryptographic Authentication
- RFC 5306 Restart Signaling for IS-IScol for BGP L3 VPNs
- Soportar las siguientes MIB:
- RFC 2578 SNMPv2 SMI
- RFC 3418 SNMPv2 MIB
- RFC 2576 SNMP-Community MIB
- RFC 2863 IF MIB
- RFC 3621 Power Ethernet MIB
- RFC 4750 OSPFv2 MIB

- CISCO CDP MIB
- CISCO NETFLOW MIB
- Incluirá la funcionalidad de Redirección de peticiones

WebFuncionalidades de Administración y Monitoreo

- El equipo será Administrado por:
  - Puerto de Consola
  - SNMP
  - Remotamente por Sesión VTY
- Soportará SSHv2
- Soportará Telnet como Servidor y Cliente
- Soportará SNTP o NTP
- Soportará Interface Web de Gestión

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

- Poseerá una función de actualización de firmware y almacenamiento de imágenes de respaldo en caso de que el proceso falle o bien la imagen se encuentre dañada o corrupta.
- Soportará Múltiples archivos de configuración
- Soportará download de Imágenes de Sistema Operativo o Firmware y archivos de configuración desde servidores:
  - FTP
  - TFTP
  - SCP
- Incluirá una funcionalidad para realizar upgrades de Sistema Operativo oFirmware de forma gradual por tarjeta y por Grupo de Tarjetas, de forma que no se reinicie el equipo completo para aplicar actualizaciones de Sistema Operativo.
- Incluirá funcionalidad de IP SLA para la medición de jitter y delay
- Soportará VLAN de Administración

Capacidad de envío de logs de acuerdo a su grado de severidad al menos

- hacia 8 servidores Syslog, de ser requerido.
- Soportará la Autenticación y Encripción por algoritmos aprobados FIPS
- Soportará la funcionalidad de especificar por usuario administrador la hora de inicio y termino de acceso al equipo.

- Soportará la funcionalidad de especificar la cantidad máxima de sesiones simultáneas por usuario administrador en el switch.
- Soportará la funcionalidad de especificar la cantidad máxima de días de inactividad por usuario administrador, antes de que la cuenta sea deshabilitada en el switch
- Soportará la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula
  - Letra minúscula
  - Numero
  - Caracteres especiales
  - Contar con un packet buffering.
- Soportará 802.3 2008 Clause 57 Ethernet OAM – Link Layer

OAMFunciones de Control y Seguridad

- Soportará rate-limiting desde 8 Kbps
- Soportará rate-limiting de entrada y salida
- Soportará IP ToS/DSCP Marking/Remarking
- Soportará los siguientes Controles de Flood-Limiting por Puerto:

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Broadcast
- Multicast
- Unknown Unicast

- Detectará dispositivos de telefonía IP o video de al menos 2 distintos fabricantes, una vez detectados aplicara configuración de forma dinámica en el puerto.
- Detectará dispositivos de telefonía IP de terceros para aplicar configuración de forma dinámica en el puerto, los dispositivos de teléfonia podrán emplear los protocolos:
  - H.323
  - SIP
- Realizará Clasificacion y QoS de paquetes multicapa basado en usuario y así dar un tratamiento específico por Grupos de Usuario y Usuario
- Soporte de múltiples usuarios/dispositivos (como teléfonos IP, computadoras, impresoras, fotocopiadoras, cámaras de seguridad, lectores de tarjeta, servidores virtuales, etc.) y múltiples métodos de autenticación (por 802.1x, WEP y MAC o la combinación de estos) en un puerto o en todos los puertos, soportando por lo menos 1000 usuarios/dispositivos autenticados por módulo.
- Soportará 802.1D
- Soportará 802.1p
- Poseerá la funcionalidad de poder detectar eventos de intermitencias o flaps en los puertos y llevará a cabo acciones como inhabilitar el(los) puerto(s) involucrados y generar una entrada de log y/o envío de traps.

- Protección automática para conexión de dispositivos de comunicación no permitidos, los cuales activen el protocolo de STP y generen alguna reconvergencia en la red.
- Soportará autentificación de usuarios administradores de equipos mediante TACACS+.
- Soportará al menos 9 grupos de RMON
- Será capaz de clasificar tráfico en base a los siguientes criterios:
  - MAC source address
  - MAC destination addres
  - Source IPX address
  - Destination IPX address
  - Source IPX socket
  - Destination IPX socket
  - Transmission control IPX
  - IPX packet type

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- IPv6 source address
- IPv6 destination address
- IPv6 flow label
- Source IP address.
- Destination IP address.
- IP fragmentation value.
- UDP source port
- UDP destination port
- TCP source port
- TCP destination port
- ICMP packet type
- Time-To-Live (TTL)
- Type of Service
- ICMPv6 packet type
- VLAN tag
- Port-string

- Incluirá la funcionalidad de limitar el acceso de una MAC Address dada aun puerto especifico, la cual puede aprender el equipo de forma estática o dinámica
- Incluirá mecanismos de mitigación ante los siguientes ataques DoS:
  - Bad SIP
  - Fragmented ICMP
  - ICMP Flood
  - Large ICMP
  - LANd
  - Smurf
  - Fraggle Attack
  - SYN Flood
- Contará con al menos 3 distintos mecanismos anti-spoofing
- Soportará RADIUS accounting / snooping

- Soportará RFC 3580
- Soportará prevención de ARP storm
- El equipo soportará e incluirá una funcionalidad capaz de distinguir la identidad de un usuario/dispositivo que es autenticado en otro switch conectado a este mismo, pudiendo asignar alguna politica de L2, L3 y L4, permitiendo, negando, etiquetando, redireccionando, asignando una prioridad y un rate limiting.
- Soportará funciones de mitigación de ataques de tipo DoS de tal forma que se pueden configurar umbrales permitidos de cantidad de tráfico, los cuales puedan desencadenar acciones como descartar tráfico excedente,

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

envio de SNMP o logs e inclusive hasta desactivar una o más interfases

Ciudad de México a 17 de mayo de 2022.

2.1.2.1. Switch de acceso Tipo2

- Switch apilable con desempeño mínimo de 260 Gbps y 193 Mpps con arquitectura no bloqueable, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad.
- El equipo contará con al menos la siguiente densidad de puertos:
  - 48 puertos 10/100/1000 BASE-T
  - 4 puertos 10GBase-X (SFP+) se deberán incluir al menos 2 conectores opticos 10G SR SFP+
  - 2 Puertos de apilamiento dedicado
  - 1 puerto serial
  - 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda
  - 1 puerto USB para almacenamiento externo
- El equipo soportará el siguiente tipo de interfaces:
  - Gigabit Ethernet: SX, LX, ZX, BX-D, BX-U, 100FX/1000LX, 10/100/1000BASE-T en formato SFP
  - 10 Gigabit Ethernet: SR, LR, ER, LRM y CR en formato SFP+
- Contará con un procesador de 64-bits a 1GHz y al menos 1GB enRAM
- Soporte de los siguientes estándares:
  - IEEE 802.3af / at
  - IEEE 802.3az
- El equipo contará con un sistema de ventilación Front-to-Back.
- El equipo soportará fuentes redundantes internas.
- El equipo estará diseñado para una altura no mayor a una unidadde rack (1 RU)
- El equipo tendrá una latencia menor a 5 micro segundos
- Soportará al menos 50,000 MAC Address
- Soportará al menos 4094 VLANs
- Soporta de Jumbo Frames 9216 Bytes

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- El equipo serrá capaz de soportar apilamiento con un ancho de bandade al menos 80 Gbps
- Soporte de apilamiento de hasta 8 unidades
- Tendrá la capacidad de apilarse con switches de la misma familia de productos, aunque sea otro modelo de menor o mayor capacidad.
- Funcionalidades de Capa 2, Switching
- El equipo soportará al menos las siguientes funcionalidades y especificaciones:
- Soporte de IEEE 802.1D STP
- Soporte de IEEE 802.1w RSTP
- Soporte de IEEE 802.1s MSTP
- Soporte de PVST+, Per VLAN STP
- Soporte de IEEE 802.3ad LACP, con la capacidad de al menos 120 grupos de agregación cuyo máximo sea de al menos 30 puertos por cada cada grupo.
- Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
- Soporte de LLDP-MED
- Soporte de Cisco Discovery Protocol (CDP) v1 y v2
- Soporte de IEEE 802.1ag Connectivity Fault Management
- Soporte del estándar Y.1731 Frame Delay
- Soporte de ITU G.8032 Ethernet Ring Protection Switching
- Soporte de PIM Snooping
- Soporte de Multicast VLAN Registration (MVR)
- Soporte de IEEE 802.1Q VLAN Tagging
- Soporte de IEEE 802.1v
- Soporte de VLANs basadas por Puerto, MAC y Protocolo
- Contará con la capacidad de trasladar los tags 802.1Q de varias VLANs al tagde una sola VLAN.
- Soporte de IEEE 802.1AK MVRP
- IEEE 802.1 Audio Video Bridging (AVB), este protocolo no es imprescindible incluirlo en la propuesta, sin embargo, el equipo ofertado estará capacitado para soportarlo sin la necesidad de hardware adicional.
- Soportará un mecanismo de redundancia a nivel de capa 2, que permita un tiempo de recuperación en caso de caída o restauración de la red en menos de 1 segundo, garantizando disponibilidad y confiabilidad ala red para aplicaciones como voz y video. Este mecanismo trabajará al menos en topologías de anillo.
- Contará con un mecanismo correctivo de detección de Loops que

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

permita tomar medidas de manera inmediata ante una falla en la red, diferente a Spanning Tree Protocol.

- Contará con una funcionalidad que permita conjuntar o agregar puertos en al menos 2 switches de tal forma que dicho arreglo proporcione una sóla conexión lógica hacia otro dispositivo, en donde dicho dispositivo puede ser un servidor o algún otro dispositivo de red que puede ser configurado por medio de algún protocolo como LAG o similar.
- Soporta de Port Mirroring tanto local como remoto
- Soportará al menos 120 filtros por puerto espejo, permitiendo una mayorgranularidad en el tipo de información que se necesita monitorear
- Funcionalidades de Clasificación de Tráfico y Calidad de Servicio
- Contará con al menos 8 colas (queues) por puerto y soportar los siguientes algoritmos de encolamiento: Weigthed Fair Queuing, Round Robin Priority y Strict Priority Queuing
- Calidad de servicio aplicable a tráfico por clasificación de acuerdo a los siguientes criterios: VLAN ID, dirección MAC, dirección IP, puerto TCP/UDP, 802.1p, DiffServ
- Soportará un rate-limiting con una granularidad de 8 kbps tanto de ingreso como de egreso
- Soporte de rate shaping
- Funcionalidades de Capa 3
- Soporte IGMP v1/v2/v3
- Ruteo estático unicast y multicast para IPv4
- Soportará al menos 15,000 entradas de IPv4
- Soporte de IP Route Compression
- Soporte de CIDR
- Soporte de ECMP
- Soporte de VRRPv2
- Soporte de BOOTP/DHCP relay agent y DHCP server
- Soporte de RIPv1 y RIPV2
- Soporte de OSPFv2
- Soporte de Autenticación MD5 para OSPF
- Soporte de PIM-SM, PIM-SSM
- Soporte de Policy Based Routing para IPv4 e IPv6
- Soportará al menos 8,000 entradas en IPv6
- Soporte de Virtual Routers, al menos 48
- Soporte de VRFs
- Soporte de ruteo estático unicast para IPv6
- Soporte de RIPng

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Soporte de MLDv1/v2
- Soporte de ICMP sobre IPv6
- Soporte de Traceroute sobre IPv6
- Soporte de Telnet sobre IPv6
- Soporte de SSHv2 sobre IPv6

- Soporte de las siguientes especificaciones para IPv6:
  - RFC 2460 - Internet Protocol,Version 6 (IPv6) Specification
  - RFC 4861 - Neighbor Discovery for IP Version 6
  - RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks
  - RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture
  - RFC 5722 - Handling of Overlapping IPv6
  - RFC 2462 - IPv6 Stateless Address Auto Configuration – Router Requirements
  - RFC 2740 OSPF v3 for IPv6 Seguridad
- El equipo contará con protección para contra ataques DoS y man-in-the-middle
- El sistema operativo del equipo soportará CLI Scripting, que permita automatizar configuraciones, tales como QoS, ACLs, etc.
- El equipo soportará múltiples suplicantes por puerto, y múltiples métodos de autenticación: 802.1x, MAC y Web
- El equipo será capaz de permitir el acceso a la red de los usuarios, através de autenticación y Kerberos snooping.
- Contará con la funcionalidad de aplicar políticas de seguridad (perfiles), con base al rol que tenga el usuario de la red en la organización,y contará con las siguientes caracteristicas:
- La creación de roles o perfiles deberá ajustarse a las necesidades del negocio, de tal modo que cada uno cuente con los privilegios especificos para el acceso de los recursos de red y de aplicativos.
- El rol o perfil será asignado por usuario y este prevalecerá inclusosi se mueve de puerto.
- El rol o perfil puede ser asignado de forma dinámica por medio de mecanismos de autenticación RADIUS con base en lo siguiente:
  - Por atributos que la propia arquitectura defina tales como campos Filter-ID o VSA.
  - Soporte del estándar RFC 3580 por medio de atributos VLAN Tunnels,
  - Soportará un modo mixto o hibrido, de acuerdo a los dos esquemasantes solicitados.

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- La funcionalidad de políticas o perfiles de seguridad contarán con al menos las siguientes capacidades:
  - 60 Perfiles o Roles por Switch
  - 800 Reglas por cada perfil o rol por Switch
  - 128 usuarios autenticados por Puerto
  - 512 usuarios por Switch
- La funcionalidad de políticas o perfiles de seguridad será capaz de clasificar o identificar el tráfico por los siguientes criterios de capa 2/3/4:
  - Por identificación del campo Type de tramas Ethernet II
  - Dirección MAC origen/destino
  - Dirección IP origen/destino
  - Dirección IPX origen/destino
  - Socket IPX origen/destino
  - Por el campo de tipo de servicio (Type of Service) en los paquetes IP
  - Puerto UDP y TCP origen/destino
  - Puerto UDP y TCP origen/destino
  - Por tipo de ICMP
  - Por tipo de Protocolo IP
  - Por identificador del puerto físico del equipo
  - Por el TAG de la VLAN
- La funcionalidad de políticas o perfiles de seguridad contarán con al menos las siguientes acciones a ejecutar:
  - Asignación de VLAN
  - Filtrado de tráfico (Permitir/Negar)
  - Asignación de Rate-Limiting
  - Rate Shaping
  - Priorización del tráfico
  - Manipulación y reescritura del campo TCI
- Contará con un mecanismo de seguridad que permita detectar amenazas y reaccionar ante la intrusión de la red. Esto basado en modelo de alertas basadas en el traspaso de umbrales definidos por el administrador de la red.
- Contará con herramientas que permitan rastrear a los usuarios dela red y proporcionará información tal como: el switch al que se conecta el usuario, el puerto físico de conexión, la MAC address, la VLAN de trabajo e identidad del usuario.
- El equipo soportará aprovisionamiento automático a través deperfiles, basados en eventos como el logging o logoff de un usuario, horadel día por medio del uso de scripts o LLDP, permitiendo configurar los parámetros necesarios de manera automática en el puerto para soluciones de telefonía IP, videoconferencia, video vigilancia,

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

autenticación de usuarios.

- Contará con un mecanismo que permita la detección de máquinas virtuales, configuración de su puerto e inventario de manera automática, el equipo será capaz de identificar la máquina virtual a través de su dirección MAC y autenticar la conexión a la red, aplicar la configuración al puerto autenticado y remover la configuración del puerto en donde la máquina virtual ha sido removida, así como de las políticas que se le hayan aplicado a la misma, sin necesidad de reconfigurar los equipos de la red.
- Contará con un mecanismo de notificaciones de eventos a través de XML, como un cambio en la configuración, cambio de estado, o cualquier evento deseado que quiera ser reportado, a través de un servidor Web externo, esto con la finalidad de alinear la estrategia de las mejores prácticas de TI y contar con una bitácora precisa de los cambios y eventos ocurridos en la red.
- Soporte de las siguientes especificaciones:
  - RFC 1492 TACACS+
  - RFC 1866 HTML
  - RFC 3580 IEEE 802.1x RADIUS
  - RFC 3579 RADIUS EAP
  - RFC 2866 RADIUS Accounting
  - RFC 2865 RADIUS Authentication
  - RFC 4668 RADIUS Authentication Client MIB for IPv6
  - RFC 4670 RADIUS Accounting Client MIB for Ipv6
  - Soporte de Listas de Control de Acceso (ACLs) en capas 2/3/4 y Wire-Speed
- Soportará al menos 4,000 listas de control de acceso para garantizar la seguridad de la red.
- Manejo de Guest VLAN para 802.1x
- Soporte de SSL/TLS
- Soporte de mecanismos para la limitar el número de direcciones MAC determinadas por puerto.
- Soporte de mecanismo para prevenir que dispositivos no autorizados tengan acceso a la red basados en su dirección MAC, garantizando sólo aquellos que estén debidamente registrados o asociados a los puertos.
- Soporte de DHCP Snooping o Trusted DHCP Server
- Soporte de Dynamic ARP Inspection o ARP Validation
- Soporte de MD5 para protocolos de enrutamiento/stración
- Contará un esquema de protección de memoria para cada aplicación, para que se manejen como procesos separados; el sistema operativo será

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

modular y contar con funciones de monitoreo y reinicio de procesos sin la necesidad de reiniciar el equipo completamente.

- Contará con APIs XML para integración con terceros.
- Contará con la capacidad de soportar scripts CLI a través de lenguajes deprogramación como Python.
- Soporte de Telnet en modalidad cliente y servidor
- Soporte de SSH2 en modalidad cliente y servidor
- Soporte de SCP en modalidad cliente y servidor
- Soporte de SFTP en modalidad servidor
- Soporte de TFTP
- Soporte de Syslog para envío de al menos para 4 servidores
- Soporte de las siguientes especificaciones:
  - RFC 1650 Ethernet-Like MIB
  - RFC 1901 – 1908 SNMPv2c, SMIv2 and Revised MIB-II
  - RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management Framework
  - RFC 1155 Structure of Management Information (SMIv1)
  - RFC 5905 1 – Network Time Protocol v4
  - RFC 2030 - SNTP, Simple Network Time Protocol v4
  - RFC 2613 SMON MIB
  - RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- Soporte de SNMPv1/v2/v3
- Soporte de gestión vía HTTP y HTTPS
- 4 Grupos de RMON
- Soportará la funcionalidad de muestreo mediante el protocolo sFlow v5 oIPFIX
- Soporte de DDMI
- Manejo de múltiples archivos de configuración
- Manejo de múltiples imágenes de firmware o Sistema operativo
- Soportará la funcionalidad de especificar un periodo de inactividad en las cuentas de administrador local después de haber sido bloqueada por intentos fallidos de la misma y tener la capacidad de habilitarse automáticamente al haber transcurrido el periodo especificado.
- Soportará la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula
  - Letra minúscula

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

- Numero
- Caracteres especiales

Ciudad de México a 17 de mayo de 2022.

- Soportará la funcionalidad de prevenir que un usuario administrador local pueda emplear un password que anteriormente empleó y ya ha caducado.
- Soportará SDN OpenStack, con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Funcionalidad para configurar un modelo de Redes Definidas por Software (SDN) mediante la especificación de estándar abierto OpenFlow 1.0, con el cual desde un Sistema Controlador se manipulen los flujos de datos usando protocolos estándares para que de forma dinámica se configuren las tablas de flujos, esto con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Contará con la capacidad de manejar comunicación FCoE, iSCIvia Data Center Bridging IEEE P802.1Qaz
- Soportará la especificación IEEE VEPA – Direct Attach
- Especificaciones a cumplir y Condiciones de Operación
- Rango de Temperatura de Operación: 0°C - 48°C
- Humedad en condiciones operativas: 10 - 95 % Humedad relativa no condensada
- Altura en condiciones operativas: 0 - 4500 m
- UL 60950-1
- FCC 21CFR 1040.10 (U.S. Laser Safety)
- EN 60825-1+A2:2001 (Lasers Safety)
- FCC CFR 47 part 15 Class A (USA)
- EN 55022:2006+A1:2007 Class A
- EN 61000-3-2 (Harmonics)
- EN 61000-3-3 2008 (Flicker)
- CISPR 22: 2006 (International Emissions)
- CISPR 24:A2:2003 Class A (International Immunity)
- IEC 61000-4-5:2005
- EN 61000-4-5:2006
- IEC/EN 61000-4-11:2004
- ETSI EN 300 386:2001
- VCCI Class A
- ETSI EN 300 019

2.1.2.3. **Switch de acceso Tipo 3**

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Características Generales

- Switch apilable con desempeño mínimo de 212 Gbps y 157 Mpps con arquitectura no bloqueable, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad.
- El equipo contará con al menos la siguiente densidad de puertos:
  - 24 puertos 10/100/1000 BASE-T
  - 4 puertos 10GBase-X (SFP+) se incluirá al menos 2conectores ópticos 10G SR SFP+
  - 2 Puertos de apilamiento dedicado.
  - 1 puerto serial
  - 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda
  - 1 puerto USB para almacenamiento externo
- El equipo soportará el siguiente tipo de interfaces:
  - Gigabit Ethernet: SX, LX, ZX, BX-D, BX-U, 100FX/1000LX, 10/100/1000BASE-T en formato SFP
  - 10 Gigabit Ethernet: SR, LR, ER, LRM y CR en formato SFP+
- Contará con un procesador de 64-bits a 1GHz y al menos 1GB enRAM
- Soporte de los siguientes estándares:
  - IEEE 802.3af / at
  - IEEE 802.3az
- El equipo contará con un sistema de ventilación Front-to-Back.
- El equipo soportará fuentes redundantes internas.
- El equipo estará diseñado para una altura no mayor a una unidadde rack (1 RU)
- El equipo tendrá una latencia menor a 5 micro segundos
- Soportará al menos 50,000 MAC Address
- Soportará al menos 4094 VLANs
- Soporte de Jumbo Frames 9216 Bytes
- El equipo será capaz de soportar apilamiento con un ancho de bandade al menos 80 Gbps
- Soporte de apilamiento de hasta 8 unidades
- Tendrá la capacidad de apilarse con switches de la misma familia de productos aunque sea otro modelo de menor o mayor capacidades de Capa 2, Switching

- El equipo soportará al menos las siguientes funcionalidades y especificaciones:
  - Soporte de IEEE 802.1D STP
  - Soporte de IEEE 802.1w RSTP

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Soporte de IEEE 802.1s MSTP
- Soporte de PVST+, Per VLAN STP
- Soporte de IEEE 802.3ad LACP, con la capacidad de al menos 120 grupos de agregación cuyo máximo sea de al menos 30 puertos por cada cada grupo.
- Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
- Soporte de LLDP-MED
- Soporte de Cisco Discovery Protocol (CDP) v1 y v2
- Soporte de IEEE 802.1ag Connectivity Fault Management
- Soporte del estándar Y.1731 Frame Delay
- Soporte de ITU G.8032 Ethernet Ring Protection Switching
- Soporte de PIM Snooping
- Soporte de Multicast VLAN Registration (MVR)
- Soporte de IEEE 802.1Q VLAN Tagging
- Soporte de IEEE 802.1v
- Soporte de VLANs basadas por Puerto, MAC y Protocolo
- Contará con la capacidad de trasladar los tags 802.1Q de varias VLANs al tag de una sola VLAN.

- Soportará un mecanismo de redundancia a nivel de capa 2, quepermita un tiempo de recuperación en caso de caída o restauración de lared en menos de 1 segundo, garantizando disponibilidad y confiabilidad ala red para aplicaciones como voz y video. Este mecanismo trabajará al menos en topologías de anillo.
- Contará con un mecanismo correctivo de detección de Loops que permita tomar medidas de manera inmediata ante una falla en la red, diferente a Spanning Tree Protocol
- Contará con una funcionalidad que permita conjuntar o agregar puertos en al menos 2 switches de tal forma que dicho arreglo proporcione una sóla conexión lógica hacia otro dispositivo, en donde dicho dispositivo puede ser un servidor o algún otro dispositivo de red que puede ser configurado por medio de algún protocolo como LAG o similar.
- Soporte de Port Mirroring tanto local como remoto
- Soportará al menos 120 filtros por puerto espejo, permitiendo una mayor granularidad en el tipo de información que se necesita monitoreardad de Servicio
- Contará con al menos 8 colas (queues) por puerto y soportar los siguientes algoritmos de encolamiento: Weigthed Fair Queuing, Round Robin Priority y Strict Priority Queuing
- Calidad de servicio aplicable a tráfico por clasificación de acuerdo a los siguientes criterios: VLAN ID, dirección MAC, dirección IP, puerto TCP/UDP, 802.1p, DiffServ

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Soportará un rate-limiting con una granularidad de 8 kbps tanto de ingreso como de egreso
- Soporte de rate shapingnalidades de Capa 3
- Soporte IGMP v1/v2/v3
- Ruteo estático unicast y multicast para IPv4
- Soportará al menos 15,000 entradas de IPv4
- Soporte de IP Route Compression
- Soporte de CIDR
- Soporte de ECMP
- Soporte de VRRPv2
- Soporte de BOOTP/DHCP relay agent y DHCP server
- Soporte de RIPv1 y RIPV2
- Soporte de OSPFv2
- Soporte de Autenticación MD5 para OSPF
- Soporte de PIM-SM, PIM-SSM
- Soporte de Policy Based Routing para IPv4 e IPv6
- Soportará al menos 8,000 entradas en IPv6
- Soporte de Virtual Routers, al menos 48
- Soporte de VRFs
- Soporte de ruteo estático unicast para IPv6
- Soporte de RIPng
- Soporte de MLDv1/v2
- Soporte de ICMP sobre IPv6
- Soporte de Traceroute sobre IPv6
- Soporte de Telnet sobre IPv6
- Soporte de SSHv2 sobre IPv6
- Soporte de las siguientes especificaciones para IPv6
  - RFC 2460 - Internet Protocol,Version 6 (IPv6) Specification
  - RFC 4861 - Neighbor Discovery for IP Version 6
  - RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks
  - RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture
  - RFC 5722 - Handling of Overlapping IPv6
  - RFC 2462 - IPv6 Stateless Address Auto Configuration – Router Requirements
  - RFC 2740 OSPF v3 for IPv6
- El equipo contará con protección para contra ataques DoS y man-in-the-middle
- El sistema operativo del equipo soportará CLI Scripting, que permita

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

automatizar configuraciones, tales como QoS, ACLs, etc.

- El equipo soportará múltiples suplicantes por puerto, múltiples métodos de autenticación: 802.1x, MAC y Web
- El equipo será capaz de permitir el acceso a la red de los usuarios, a través de autenticación y Kerberos snooping.

- Contará con la funcionalidad de aplicar políticas de seguridad (perfiles), con base al rol que tenga el usuario de la red en la organización,y contará con las siguientes características:
- La creación de roles o perfiles se ajustarán a las necesidades del negocio, de tal modo que cada uno cuente con los privilegios específicos para el acceso de los recursos de red y de aplicativos.
- El rol o perfil será asignado por usuario y este debe prevalecer inclusosi se mueve de puerto.
- El rol o perfil puede ser asignado de forma dinámica por medio de mecanismos de autenticación RADIUS con base en lo siguiente:
- Por atributos que la propia arquitectura defina tales como campos Filter-ID o VSA.
- Soporte del estándar RFC 3580 por medio de atributos VLAN Tunnels,
- Soportará un modo mixto o híbrido, de acuerdo a los dos esquemas antessolicitados.
- La funcionalidad de políticas o perfiles de seguridad contará con al menos las siguientes capacidades:
  - 60 Perfiles o Roles por Switch
  - 800 Reglas por cada perfil o rol por Switch
  - 128 usuarios autenticados por Puerto
  - 512 usuarios por Switch
- La funcionalidad de políticas o perfiles de seguridad será capaz de clasificar o identificar el tráfico por los siguientes criterios de capa 2/3/4:
  - Por identificación del campo Type de tramas Ethernet II
  - Dirección MAC origen/destino
  - Dirección IP origen/destino
  - Dirección IPX origen/destino
  - Socket IPX origen/destino
  - Por el campo de tipo de servicio (Type of Service) en los paquetes IP
  - Puerto UDP y TCP origen/destino
  - Puerto UDP y TCP origen/destino
  - Por tipo de ICMP
  - Por tipo de Protocolo IP
  - Por identificador del puerto físico del equipo

- Por el TAG de la VLAN
- La funcionalidad de políticas o perfiles de seguridad contarán con al menos las siguientes acciones a ejecutar:
  - Asignación de VLAN
  - Filtrado de tráfico (Permitir/Negar)
  - Asignación de Rate-Limiting
  - Rate Shaping
  - Priorización del tráfico
  - Manipulación y reescritura del campo TCI
- Contará con un mecanismo de seguridad que permita detectar amenazas y reaccionar ante la intrusión de la red. Esto basado en modelo de alertas basadas en el traspaso de umbrales definidos por el administrador de la red.
- Contará con herramientas que permitan rastrear a los usuarios dela red y proporcionar información tal como: el switch al que se conecta el usuario, el puerto físico de conexión, la MAC address, la VLAN de trabajo e identidad del usuario.
- El equipo soportará aprovisionamiento automático a través deperfiles, basados en eventos como el logging o logoff de un usuario, horadel día por medio del uso de scripts o LLDP, permitiendo configurar los parámetros necesarios de manera automática en el puerto para soluciones de telefonía IP, videoconferencia, video vigilancia, autenticación de usuarios.
- Contará con un mecanismo que permita soportar la migración de máquinas virtuales, configuración de su puerto e inventario de manera automática, el equipo será capaz de identificar la máquina virtuala través de su dirección MAC y autenticar la conexión a la red, aplicar la configuración al puerto autenticado y remover la configuración del puerto en donde la máquina virtual ha sido removida, así como de las políticas que se le hayan aplicado a la misma, sin necesidad de reconfigurar los equipos de la red.
- Contará con un mecanismo de notificaciones de eventos a travésde XML, como un cambio en la configuración, cambio de estado, o cualquier evento deseado que quiera ser reportado, a través de un servidor Web externo, esto con la finalidad de alinear la estrategia de las mejores prácticas de TI y contar con una bitácora precisa de los cambios yeventos ocurridos en la red.
- Soporte de las siguientes especificaciones:
  - RFC 1492 TACACS+

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- RFC 1866 HTML
- RFC 3580 IEEE 802.1x RADIUS
- RFC 3579 RADIUS EAP
- RFC 2866 RADIUS Accounting
- RFC 2865 RADIUS Authentication
- RFC 4668 RADIUS Authentication Client MIB for IPv6
- RFC 4670 RADIUS Accounting Client MIB for Ipv6

- Soporte de Listas de Control de Acceso (ACLs) en capas 2/3/4 y Wire-Speed
- Soportará al menos 4,000 listas de control de acceso paragarantizar la seguridad de la red.
- Manejo de Guest VLAN para 802.1x
- Soporte de SSL/TLS
- Soporte de mecanismos para la limitar el número de direcciones MAC determinadas por puerto.
- Soporte de mecanismo para prevenir que dispositivos no autorizados tengan acceso a la red basados en su dirección MAC, garantizando sólo aquellos que estén debidamente registrados o asociados a los puertos.

- Soporte de DHCP Snooping o Trusted DHCP Server
- Soporte de Dynamic ARP Inspection o ARP Validation
- Soporte de MD5 para protocolos de enrutamiento
- Funcionalidades de Administración
- Contará un esquema de protección de memoria para cada aplicación, para que se manejen como procesos separados: el sistema operativo será modular y contar con funciones de monitoreo y reinicio de procesos sin la necesidad de reiniciar el equipo completamente.
- Contará con APIs XML para integración con terceros.
- Contará con la capacidad de soportar scripts CLI a través de lenguajes deprogramación como Python.
- Soporte de Telnet en modalidad cliente y servidor
- Soporte de SSH2 en modalidad cliente y servidor
- Soporte de SCP en modalidad cliente y servidor
- Soporte de SFTP en modalidad servidor
- Soporte de TFTP
- Soporte de Syslog para envío de al menos para 4 servidores
- Soporte de las siguientes especificaciones
  - RFC 1650 Ethernet-Like MIB
  - RFC 1901 – 1908 SNMPv2c, SMIv2 and Revised MIB-II
  - RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Framework
- RFC 1155 Structure of Management Information (SMIv1)
- RFC 1157 SNMPv1
- RFC 5905 1 – Network Time Protocol v4
- RFC 2030 - SNTP, Simple Network Time Protocol v4
- RFC 2613 SMON MIB
- RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model

- Soporte de SNMPv1/v2/v3
- Soporte de gestión vía HTTP y HTTPS
- 4 Grupos de RMON
- Soportará la funcionalidad de muestreo mediante el protocolo sFlow v5 oIPFIX
- Soporte de DDMI
- Maneja de múltiples archivos de configuración
- Maneja de múltiples imágenes de firmware o Sistema operativo
- Soportará la funcionalidad de especificar un periodo de inactividad en las cuentas de administrador local después de haber sido bloqueada por intentos fallidos de la misma y tener la capacidad de habilitarse automáticamente al haber transcurrido el periodo especificado.
- Soportará la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula
  - Letra minúscula
  - Numero
  - Caracteres especiales
  - Soportará la funcionalidad de prevenir que un usuario administrador local pueda emplear un password que anteriormente empleó y ya ha caducado.
  - Funcionalidades Especiales
- Soportará SDN OpenStack, con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Funcionalidad para configurar un modelo de Redes Definidas por Software (SDN) mediante la especificación de estándar abierto OpenFlow, con el cual desde un Sistema Controlador se manipulen los flujos de datos usando protocolos estándares para que de forma dinámica se configuren las tablas de flujos, esto con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Contará con la capacidad de manejar comunicación FCoE, iSCIvia Data Center Bridging IEEE P802.1Qaz

Ciudad de México a 17 de mayo de 2022.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Soportará la especificación IEEE VEPA – Direct Attach
- Especificaciones a cumplir y Condiciones de Operación
- Rango de Temperatura de Operación: 0°C - 48°C
- Humedad en condiciones operativas: 10 - 95 % Humedad relativa no condensada
- Altura en condiciones operativas: 0 - 4500 m
- UL 60950-1
- FCC 21CFR 1040.10 (U.S. Laser Safety)
- EN 60825-1+A2:2001 (Lasers Safety)
- FCC CFR 47 part 15 Class A (USA)
- EN 55022:2006+A1:2007 Class A
- EN 61000-3-2 (Harmonics)
- EN 61000-3-3 2008 (Flicker)
- CISPR 22: 2006 (International Emissions)
- CISPR 24:A2:2003 Class A (International Immunity)
- IEC 61000-4-5:2005
- EN 61000-4-5:2006
- IEC/EN 61000-4-11:2004
- ETSI EN 300 386:2001
- VCCI Class A
- ETSI EN 300 019

2.3.1.4. Switch de acceso Tipo4

- Switch apilable con desempeño mínimo de 260 Gbps y 193 Mpps con arquitectura no bloqueable, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad.
- El equipo contará con al menos la siguiente densidad de puertos:
  - 48 puertos 10/100/1000 BASE-T
  - 1 puerto serial
  - 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda
  - 1 puerto USB para almacenamiento externo
- El equipo soportará el siguiente tipo de interfaces:
  - Gigabit Ethernet: SX, LX, ZX, BX-D, BX-U, 100FX/1000LX, 10/100/1000BASE-T en formato SFP
  - 10 Gigabit Ethernet: SR, LR, ER, LRM y CR en formato SFP+
- Soporte de los siguientes estándares:
  - IEEE 802.3af / at
  - IEEE 802.3az

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- El equipo soportará fuentes redundantes.
- El equipo tendrá una latencia menor a 5 microsegundos
- Soportará al menos 32,000 MAC Address
- Soportará al menos 4094 VLANs
- Soporte de Jumbo Frames.
- Funcionalidades de Capa 2, Switching
- El equipo soporta al menos las siguientes funcionalidades y especificaciones:
- Soporte de IEEE 802.1D STP
- Soporte de IEEE 802.1w RSTP
- Soporte de IEEE 802.1s MSTP
- Soporte de PVST+, Per VLAN STP
- Soporte de IEEE 802.3ad LACP.
- Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
- Soporte de LLDP-MED
- Soporte de Cisco Discovery Protocol (CDP) v1 y v2
- Soporte de IEEE 802.1ag Connectivity Fault Management
- Soporte del estándar Y.1731 Frame Delay
- Soporte de ITU G.8032 Ethernet Ring Protection Switching
- Soporte de PIM Snooping
- Soporte de Multicast VLAN Registration (MVR)
- Soporte de IEEE 802.1Q VLAN Tagging
- Soporte de IEEE 802.1v
- Soporte de VLANs basadas por Puerto, MAC y Protocolo
- Contará con la capacidad de trasladar los tags 802.1Q de varias VLANs al tagde una sola VLAN.
- Soporte de IEEE 802.1AK MVRP
- IEEE 802.1 Audio Video Bridging (AVB), este protocolo no es imprescindible incluirlo en la propuesta, sin embargo, el equipo ofertado estará capacitado para soportarlo sin la necesidad de hardware adicional.
- Soportará un mecanismo de redundancia a nivel de capa 2, quepermita un tiempo de recuperación en caso de caída o restauración de lared en menos de 1 segundo, garantizando disponibilidad y confiabilidad ala red para aplicaciones como voz y video. Este mecanismo trabajará al menos en topologías de anillo.
- Contará con un mecanismo correctivo de detección de Loops que permita tomar medidas de manera inmediata ante una falla en la red,

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

diferente a Spanning Tree Protocol.

- Contará con una funcionalidad que permita configurar un arreglo de [illegible] de 2022. en al menos 2 switches de tal forma que dicho arreglo proporcione una sóla conexión lógica hacia otro dispositivo, en donde dicho dispositivo puede ser un servidor o algún otro dispositivo de red que puede ser configurado por medio de algún protocolo como LAG o similar.
- Soporte de Port Mirroring tanto local como remoto
- Funcionalidades de Clasificación de Tráfico y Calidad de Servicio
- Contará con al menos 8 colas (queues) por puerto y soportar los siguientes algoritmos de encolamiento: Weigthed Fair Queuing, Round Robin Priority y Strict Priority Queuing
- Calidad de servicio aplicable a tráfico por clasificación de acuerdo a los siguientes criterios: VLAN ID, dirección MAC, dirección IP, puerto TCP/UDP, 802.1p, DiffServ
- Soportará un rate-limiting con una granularidad de 8 kbps tanto de ingreso como de egreso
- Soporte de rate shaping
- Funcionalidades de Capa 3
- Soporte IGMP v1/v2/v3
- Ruteo estático unicast y multicast para IPv4
- Soportará al menos 15,000 entradas de IPv4
- Soporte de CIDR
- Soporte de ECMP
- Soporte de VRRPv2
- Soporte de BOOTP/DHCP relay agent y DHCP server
- Soporte de RIPv1 y RIPV2
- Soporte de OSPFv2
- Soporte de Autenticación MD5 para OSPF
- Soporte de PIM-SM, PIM-SSM
- Soporte de Policy Based Routing para IPv4 e IPv6
- Soporte de Virtual Routers, al menos 48
- Soporte de VRFs
- Soporte de ruteo estático unicast para IPv6
- Soporte de RIPng
- Soporte de MLDv1/v2
- Soporte de ICMP sobre IPv6

- Soporte de Traceroute sobre IPv6
- Soporte de Telnet sobre IPv6

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Soporte de SSHv2 sobre IPv6
- Soporte de las siguientes especificaciones para IPv6
  - RFC 2460 - Internet Protocol,Version 6 (IPv6) Specification
  - RFC 4861 - Neighbor Discovery for IP Version 6
  - RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks
  - RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture
  - RFC 5722 - Handling of Overlapping IPv6
  - RFC 2462 - IPv6 Stateless Address Auto Configuration - Router Requirements
  - RFC 2740 OSPF v3 for IPv6 Seguridad
- El equipo contará con protección para contra ataques DoS y man-in-the-middle
- El sistema operativo del equipo soportará CLI Scripting, que permita automatizar configuraciones, tales como QoS, ACLs, etc.
- El equipo soportará múltiples suplicantes por puerto, y múltiples métodos de autenticación: 802.1x, MAC y Web
- El equipo será capaz de permitir el acceso a la red de los usuarios, através de autenticación y Kerberos snooping.
- Contará con la funcionalidad de aplicar políticas de seguridad (perfiles), con base al rol que tenga el usuario de la red en la organización, y contará con las siguientes características:
- La creación de roles o perfiles se ajustarán a las necesidades del negocio, de tal modo que cada uno cuente con los privilegios específicos para el acceso de los recursos de red y de aplicativos.
- El rol o perfil será asignado por usuario y este prevalecerá inclusosi se mueve de puerto.
- El rol o perfil será asignado de forma dinámica por medio de mecanismos de autenticación RADIUS con base en lo siguiente:
  - Por atributos que la propia arquitectura defina tales como campos Filter-ID o VSA.
  - Soporte del estándar RFC 3580 por medio de atributos VLAN Tunnels,
  - Soportará un modo mixto o hibrido, de acuerdo a los dos esquemasantes solicitados.
- La funcionalidad de políticas o perfiles de seguridad contará con al menos las siguientes capacidades:
  - 60 Perfiles o Roles por Switch
  - 800 Reglas por cada perfil o rol por Switch
  - 128 usuarios autenticados por Puerto
  - 512 usuarios por Switch

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 19 de mayo de 2022.

- La funcionalidad de políticas o perfiles de seguridad será capaz de clasificar o identificar el tráfico por los siguientes criterios (al menos):
  - Por identificación del campo Type de tramas Ethernet II
  - Dirección MAC origen/destino
  - Dirección IP origen/destino
  - Dirección IPX origen/destino
  - Socket IPX origen/destino
  - Por el campo de tipo de servicio (Type of Service) en los paquetes IP
  - Puerto UDP y TCP origen/destino
  - Puerto UDP y TCP origen/destino
  - Por tipo de ICMP
  - Por tipo de Protocolo IP
  - Por identificador del puerto físico del equipo
  - Por el TAG de la VLAN
- La funcionalidad de políticas o perfiles de seguridad contará con almenos las siguientes acciones a ejecutar:
  - Asignación de VLAN
  - Filtrado de tráfico (Permitir/Negar)
  - Asignación de Rate-Limiting
  - Rate Shaping
  - Priorización del tráfico
  - Manipulación y reescritura del campo TCI
- Contará con un mecanismo de seguridad que permita detectar amenazas y reaccionar ante la intrusión de la red. Esto basado en modelo de alertas basadas en el traspaso de umbrales definidos por el administrador de la red.
- Contará con herramientas que permitan rastrear a los usuarios dela red y proporcionar información tal como: el switch al que se conecta el usuario, el puerto físico de conexión, la MAC address, la VLAN de trabajo e identidad del usuario.
- El equipo soportará aprovisionamiento automático a través deperfiles, basados en eventos como el logging o logoff de un usuario, horadel día por medio del uso de scripts o LLDP, permitiendo configurar los parámetros necesarios de manera automática en el puerto para soluciones de telefonía IP, videoconferencia, video vigilancia, autenticación de usuarios.
- Contará con un mecanismo que permita soportar la migración de máquinas virtuales, configuración de su puerto e inventario de manera automática, el equipo será capaz de identificar la máquina virtuala través de su dirección MAC y autenticar la conexión a la red, aplicar la configuración al puerto autenticado y remover la configuración del puerto

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

en donde la máquina virtual ha sido removida, así como de las políticas que se le hayan aplicado a la misma, sin necesidad de reconfigurar los equipos de la red.

- Contará con un mecanismo de notificaciones de eventos a través de XML, como un cambio en la configuración, cambio de estado, o cualquier evento deseado que quiera ser reportado, a través de un servidor Web externo, esto con la finalidad de alinear la estrategia de las mejores prácticas de TI y contar con una bitácora precisa de los cambios y eventos ocurridos en la red.
- Soporte de las siguientes especificaciones
  - RFC 1492 TACACS+
  - RFC 1866 HTML
  - RFC 3580 IEEE 802.1x RADIUS
  - RFC 3579 RADIUS EAP
  - RFC 2866 RADIUS Accounting
  - RFC 2865 RADIUS Authentication
  - RFC 4668 RADIUS Authentication Client MIB for IPv6
  - RFC 4670 RADIUS Accounting Client MIB for Ipv6
- Soporte de Listas de Control de Acceso (ACLs) en capas 2/3/4 y Wire-Speed
- Manejo de Guest VLAN para 802.1x
- Soporte de SSL/TLS
- Soporte de mecanismos para la limitar el número de direcciones MAC determinadas por puerto.
- Soporte de mecanismo para prevenir que dispositivos no autorizados tengan acceso a la red basados en su dirección MAC, garantizando sólo aquellos que estén debidamente registrados o asociados a los puertos.
- Soporte de DHCP Snooping o Trusted DHCP Server
- Soporte de Dynamic ARP Inspection o ARP Validation
- Soporte de MD5 para protocolos de enrutamientoistración
- Contará un esquema de protección de memoria para cada aplicación, para que se manejen como procesos separados; el sistema operativo será modular y contar con funciones de monitoreo y reinicio de procesos sin la necesidad de reiniciar el equipo completamente.
- Contar con APIs XML para integración con terceros.
- Contar con la capacidad de soportar scripts CLI a través de lenguajes de programación como Python.
- Soporte de Telnet en modalidad cliente y servidor
- Soporte de SSH2 en modalidad cliente y servidor
- Soporte de SCP en modalidad cliente y servidor
- Soporte de SFTP en modalidad servidor

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

- Soporte de TFTP
- Soporte de Syslog para envío de al menos [illegible] a 17 de mayo de 2022.
- Soporte de las siguientes especificaciones:
  - RFC 1650 Ethernet-Like MIB
  - RFC 1901 – 1908 SNMPv2c, SMIv2 and Revised MIB-II
  - RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management Framework
  - RFC 1155 Structure of Management Information (SMIv1)
  - RFC 5905 1 – Network Time Protocol v4
  - RFC 2030 - SNTP, Simple Network Time Protocol v4
  - RFC 2613 SMON MIB
  - RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- Soporte de SNMPv1/v2/v3
- Soporte de gestión vía HTTP y HTTPS
- 4 Grupos de RMON
- Soportará la funcionalidad de muestreo mediante el protocolo sFlow v5 oIPFIX
- Soporte de DDMI
- Manejo de múltiples archivos de configuración
- Manejo de múltiples imágenes de firmware o Sistema operativo
- Soportará la funcionalidad de especificar un periodo de inactividad en las cuentas de administrador local después de haber sido bloqueada por intentos fallidos de la misma y tener la capacidad de habilitarse automáticamente al haber transcurrido el periodo especificado.
- Soportará la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula
  - Letra minúscula
  - Numero
  - Caracteres especiales
- Soportará la funcionalidad de prevenir que un usuario administrador local pueda emplear un password que anteriormente empleó y ya ha caducado.
- Funcionalidad para configurar un modelo de Redes Definidas por Software (SDN) mediante la especificación de estándar abierto OpenFlow 1.0, con el cual desde un Sistema Controlador se manipulen los flujos de

datos usando protocolos estándares para que de forma dinámica se configuren las tablas de flujos, esto con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.

- Contará con la capacidad de manejar comunicación FCoE, iSCIvia Data Center Bridging IEEE P802.1Qaz
- Soportará la especificación IEEE VEPA – Direct Attach
- Especificaciones a cumplir y Condiciones de Operación
- Rango de Temperatura de Operación: 0°C - 48°C
- Humedad en condiciones operativas: 10 - 95 % Humedad relativa no condensada
- Altura en condiciones operativas: 0 - 4500 m
- UL 60950-1
- FCC 21CFR 1040.10 (U.S. Laser Safety)
- EN 60825-1+A2:2001 (Lasers Safety)
- FCC CFR 47 part 15 Class A (USA)
- EN 55022:2006+A1:2007 Class A
- EN 61000-3-2 (Harmonics)

- EN 61000-3-3 2008 (Flicker)
- CISPR 22: 2006 (International Emissions)
- CISPR 24:A2:2003 Class A (International Immunity)
- IEC 61000-4-5:2005
- EN 61000-4-5:2006
- IEC/EN 61000-4-11:2004
- ETSI EN 300 386:2001
- VCCI Class A
- ETSI EN 300 019

1.3.1.5. Switch de acceso Tipo 5

Características Generales

- Switch apilable con desempeño mínimo de 212 Gbps y 157 Mpps con arquitectura no bloqueable, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad.
- El equipo contará con al menos la siguiente densidad de puertos:
  - 24 puertos 10/100/1000 BASE-T
  - 2 Puertos de apilamiento dedicado.
  - 1 puerto serial
  - 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- 1 puerto USB para almacenamiento externo

- El equipo soportará el siguiente tipo de interfaces:
  - Gigabit Ethernet: SX, LX, ZX, BX-D, BX-U, 100FX/1000LX, 10/100/1000BASE-T en formato SFP
  - 10 Gigabit Ethernet: SR, LR, ER, LRM y CR en formato SFP+
- Contará con un procesador de 64-bits a 1GHz y al menos 1GB enRAM
- Soporte de los siguientes estándares:
  - IEEE 802.3af / at
  - IEEE 802.3az
- El equipo soportará fuentes redundantes.
- El equipo estará diseñado para una altura no mayor a una unidadde rack (1 RU)
- El equipo tendrá una latencia menor a 5 micro segundos
- Soportará al menos 32,000 MAC Address
- Soportará al menos 4094 VLANs
- Soporte de Jumbo Frames
- El equipo serrá capaz de soportar apilamiento con un ancho de bandade al menos 80 Gbps
- Soporte de apilamiento de hasta 8 unidades
- Tendrá la capacidad de apilarse con switches de la misma familia de productos aunque sea otro modelo de menor o mayor capacidades de Capa 2, Switching

- El equipo soportará al menos las siguientes funcionalidades y especificaciones:
  - Soporte de IEEE 802.1D STP
  - Soporte de IEEE 802.1w RSTP
  - Soporte de IEEE 802.1s MSTP
  - Soporte de PVST+, Per VLAN STP
  - Soporte de IEEE 802.3ad LACP, con la capacidad de al menos 120 grupos de agregación cuyo máximo sea de al menos 30 puertos por cada cada grupo.
  - Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
  - Soporte de LLDP-MED
  - Soporte de Cisco Discovery Protocol (CDP) v1 y v2
  - Soporte de IEEE 802.1ag Connectivity Fault Management
  - Soporte del estándar Y.1731 Frame Delay
  - Soporte de ITU G.8032 Ethernet Ring Protection Switching
  - Soporte de PIM Snooping
  - Soporte de Multicast VLAN Registration (MVR)

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Soporte de IEEE 802.1Q VLAN Tagging
- Soporte de IEEE 802.1v
- Soporte de VLANs basadas por Puerto, MAC y Protocolo
- Contará con la capacidad de trasladar los tags 802.1Q de varias VLANsal tag de una sola VLAN.
- Soporte de IEEE 802.1AK MVRP

- Soportará un mecanismo de redundancia a nivel de capa 2, que permita un tiempo de recuperación en caso de caída o restauración de lared en menos de 1 segundo, garantizando disponibilidad y confiabilidad a la red para aplicaciones como voz y video. Este mecanismo trabajará al menos en topologías de anillo.
- Contará con un mecanismo correctivo de detección de Loops que permita tomar medidas de manera inmediata ante una falla en la red, diferente a Spanning Tree Protocol.
- Contará con una funcionalidad que permita conjuntar o agregar puertos en al menos 2 switches de tal forma que dicho arreglo proporcione una sóla conexión lógica hacia otro dispositivo, en donde dicho dispositivo puede ser un servidor o algún otro dispositivo de red que puede ser configurado por medio de algún protocolo como LAG o similar.
- Soporte de Port Mirroring tanto local como remoto
- Soportará al menos 120 filtros por puerto espejo, permitiendo una mayor granularidad en el tipo de información que se necesite monitorear.
- Contará con al menos 8 colas (queues) por puerto y soportar los siguientes algoritmos de encolamiento: Weigthed Fair Queuing, Round Robin Priority y Strict Priority Queuing
- Calidad de servicio aplicable a tráfico por clasificación de acuerdo a los siguientes criterios: VLAN ID, dirección MAC, dirección IP, puerto TCP/UDP, 802.1p, DiffServ

- Soportará un rate-limiting con una granularidad de 8 kbps tanto de ingreso como de egreso
- Soporte de rate shapingnalidades de Capa 3
- Soporte IGMP v1/v2/v3
- Ruteo estático unicast y multicast para IPv4
- Soportará al menos 15,000 entradas de IPv4
- Soporte de IP Route Compression
- Soporte de CIDR
- Soporte de ECMP
- Soporte de VRRPv2
- Soporte de BOOTP/DHCP relay agent y DHCP server

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Soporte de RIPv1 y RIPV2
- Soporte de OSPFv2
- Soporte de Autenticación MD5 para OSPF
- Soporte de PIM-SM, PIM-SSM
- Soporte de Policy Based Routing para IPv4 e IPv6
- Soportar al menos 8,000 entradas en IPv6
- Soporte de Virtual Routers, al menos 48
- Soporte de VRFs
- Soporte de ruteo estático unicast para IPv6
- Soporte de RIPng
- Soporte de MLDv1/v2
- Soporte de ICMP sobre IPv6
- Soporte de Traceroute sobre IPv6
- Soporte de Telnet sobre IPv6
- Soporte de SSHv2 sobre IPv6
- Soporte de las siguientes especificaciones para IPv6:
  - RFC 2460 - Internet Protocol,Version 6 (IPv6) Specification
  - RFC 4861 - Neighbor Discovery for IP Version 6
  - RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks
  - RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture
  - RFC 5722 - Handling of Overlapping IPv6
  - RFC 2462 - IPv6 Stateless Address Auto Configuration – Router Requirements
  - RFC 2740 OSPF v3 for IPv6
- El equipo contará con protección para contra ataques DoS y man-in-the-middle
- El sistema operativo del equipo soportará CLI Scripting, que permita automatizar configuraciones, tales como QoS, ACLs, etc.
- El equipo soportará múltiples suplicantes por puerto, y múltiples métodos de autenticación: 802.1x, MAC y Web
- El equipo será capaz de permitir el acceso a la red de los usuarios, a través de autenticación y Kerberos snooping.

- Contará con la funcionalidad de aplicar políticas de seguridad (perfiles), con base al rol que tenga el usuario de la red en la organización,y contará con las siguientes características:
- La creación de roles o perfiles se ajustarán a las necesidades del negocio, de tal modo que cada uno cuente con los privilegios específicos para el acceso de los recursos de red y de aplicativos.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- El rol o perfil será asignado por usuario y este prevalecerá inclusosi se mueve de puerto.
- El rol o perfil puede ser asignado de forma dinámica por medio de mecanismos de autenticación RADIUS con base en lo siguiente:
- Por atributos que la propia arquitectura defina tales como campos Filter-ID o VSA.
- Soporte del estándar RFC 3580 por medio de atributos VLAN Tunnels,
- Soportar un modo mixto o híbrido, de acuerdo a los dos esquemas antes solicitados.
- La funcionalidad de políticas o perfiles de seguridad contará con al menos las siguientes capacidades:
  - 60 Periles o Roles por Switch
  - 800 Reglas por cada perfil o rol por Switch
  - 128 usuarios autenticados por Puerto
  - 512 usuarios por Switch
- La funcionalidad de políticas o perfiles de seguridad será capaz de clasificar o identificar el tráfico por los siguientes criterios de capa 2/3/4:
  - Por identificación del campo Type de tramas Ethernet II
  - Dirección MAC origen/destino
  - Dirección IP origen/destino
  - Dirección IPX origen/destino
  - Socket IPX origen/destino
  - Por el campo de tipo de servicio (Type of Service) en los paquetes IP
  - Puerto UDP y TCP origen/destino
  - Puerto UDP y TCP origen/destino
  - Por tipo de ICMP
  - Por tipo de Protocolo IP
  - Por identificador del puerto físico del equipo
  - Por el TAG de la VLAN
- La funcionalidad de políticas o perfiles de seguridad contará con almenos las siguientes acciones a ejecutar:
  - Asignación de VLAN
  - Filtrado de tráfico (Permitir/Negar)
  - Asignación de Rate-Limiting
  - Rate Shaping
  - Priorización del tráfico
  - Manipulación y reescritura del campo TCI
- Contará con un mecanismo de seguridad que permita detectar amenazas y reaccionar ante la intrusión de la red. Esto basado en modelo

de alertas basadas en el traspaso de umbrales definidos por el

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de enero de 2022.

administrador de la red.

- Contará con herramientas que permitan rastrear a los usuarios de la red y proporcionar información tal como: el switch al que se conecta el usuario, el puerto físico de conexión, la MAC address, la VLAN de trabajo e identidad del usuario.
- El equipo soportará aprovisionamiento automático a través deperfiles, basados en eventos como el logging o logoff de un usuario, horadel día por medio del uso de scripts o LLDP, permitiendo configurar los parámetros necesarios de manera automática en el puerto para soluciones de telefonía IP, videoconferencia, video vigilancia, autenticación de usuarios.
- Contará con un mecanismo que permita soportar la migración de máquinas virtuales, configuración de su puerto e inventario de manera automática, el equipo será capaz de identificar la máquina virtual a través de su dirección MAC y autenticar la conexión a la red, aplicar la configuración al puerto autenticado y remover la configuración del puerto en donde la máquina virtual ha sido removida, así como de las políticas que se le hayan aplicado a la misma, sin necesidad de reconfigurar los equipos de la red.
- Contará con un mecanismo de notificaciones de eventos a travésde XML, como un cambio en la configuración, cambio de estado, o cualquier evento deseado que quiera ser reportado, a través de un servidor Web externo, esto con la finalidad de alinear la estrategia de las mejores prácticas de TI y contar con una bitácora precisa de los cambios yeventos ocurridos en la red.
- Soporte de las siguientes especificaciones:
  - RFC 1492 TACACS+
  - RFC 1866 HTML
  - RFC 3580 IEEE 802.1x RADIUS
  - RFC 3579 RADIUS EAP
  - RFC 2866 RADIUS Accounting
  - RFC 2865 RADIUS Authentication
  - RFC 4668 RADIUS Authentication Client MIB for IPv6
  - RFC 4670 RADIUS Accounting Client MIB for Ipv6
- Soporte de Listas de Control de Acceso (ACLs) en capas 2/3/4 y Wire-Speed
- Soportará al menos 4,000 listas de control de acceso paragarantizar la seguridad de la red.
- Manejo de Guest VLAN para 802.1x
- Soporte de SSL/TLS

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022

- Soporte de mecanismos para la limitar el número de direcciones MAC determinadas por puerto.
- Soporte de mecanismo para prevenir que dispositivos no autorizados tengan acceso a la red basados en su dirección MAC, garantizando sólo aquellos que estén debidamente registrados o asociados a los puertos.
- Soporte de DHCP Snooping o Trusted DHCP Server
- Soporte de Dynamic ARP Inspection o ARP Validation
- Soporte de MD5 para protocolos de enrutamiento
- Funcionalidades de Administración
- Contará un esquema de protección de memoria para cada aplicación, para que se manejen como procesos separados; el sistema operativo será modular y contará con funciones de monitoreo y reinicio de procesos sin la necesidad de reiniciar el equipo completamente.
- Contará con APIs XML para integración con terceros.
- Contará con la capacidad de soportar scripts CLI a través de lenguajes deprogramación como Python.
- Soporte de Telnet en modalidad cliente y servidor
- Soporte de SSH2 en modalidad cliente y servidor
- Soporte de SCP en modalidad cliente y servidor
- Soporte de SFTP en modalidad servidor
- Soporte de TFTP
- Soporte de Syslog para envio de al menos para 4 servidores
- Soporte de las siguientes especificaciones:
  - RFC 1650 Ethernet-Like MIB
  - RFC 1901 – 1908 SNMPv2c, SMIv2 and Revised MIB-II
  - RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management Framework
  - RFC 1155 Structure of Management Information (SMIv1)
  - RFC 5905 1 – Network Time Protocol v4
  - RFC 2030 - SNTP, Simple Network Time Protocol v4
  - RFC 2613 SMON MIB
  - RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- Soporte de SNMPv1/v2/v3
- Soporte de gestión vía HTTP y HTTPS
- 4 Grupos de RMON
- Soportará la funcionalidad de muestreo mediante el protocolo sFlow v5 oIPFIX
- Soporte de DDMI

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Manejo de múltiples archivos de configuración
- Manejo de múltiples imágenes de firmware o Sistema operativo
- Soportará la funcionalidad de especificar un periodo de inactividad en las cuentas de administrador local después de haber sido bloqueada por intentos fallidos de la misma y tener la capacidad de habilitarse automáticamente al haber transcurrido el periodo especificado.
- Soportará la funcionalidad de establecer la cantidad mínima de caracteres para formar un password de usuario administrador, especificando el mínimo de cada uno de este tipo de caracteres:
  - Letra mayúscula
  - Letra minúscula
  - Numero
  - Caracteres especiales
  - Soportará la funcionalidad de prevenir que un usuario administrador local pueda emplear un password que anteriormente empleó y ya ha caducado.
  - Funcionalidades Especiales
- Soportará SDN OpenStack, con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Funcionalidad para configurar un modelo de Redes Definidas por Software (SDN) mediante la especificación de estándar abierto OpenFlow, con el cual desde un Sistema Controlador se manipulen los flujos de datos usando protocolos estándares para que de forma dinámica se configuren las tablas de flujos, esto con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Contará con la capacidad de manejar comunicación FCoE, iSCIvia Data Center Bridging IEEE P802.1Qaz
- Soportará la especificación IEEE VEPA – Direct Attach
- Especificaciones a cumplir y Condiciones de Operación
- Rango de Temperatura de Operación: 0°C - 48°C
- Humedad en condiciones operativas: 10 - 95 % Humedad relativa no condensada
- Altura en condiciones operativas: 0 - 4500 m
- UL 60950-1
- FCC 21CFR 1040.10 (U.S. Laser Safety)
- EN 60825-1+A2:2001 (Lasers Safety)
- FCC CFR 47 part 15 Class A (USA)
- EN 55022:2006+AL:2007 Class A
- EN 61000-3-2 (Harmonics)
- EN 61000-3-3 2008 (Flicker)

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- CISPR 22: 2006 (International Emissions)
- CISPR 24:A2:2003 Class A (International Immunity)
- IEC 61000-4-5:2005
- EN 61000-4-5:2006
- IEC/EN 61000-4-11:2004
- ETSI EN 300 386:2001
- VCCI Class A
- ETSI EN 300 019

Los switches de acceso se distribuirán conforme a la siguiente tabla,mismas que podrán variar según las necesidades del Instituto.

Sede	Ubicación	Switch de Acceso	Cantidad
Oficinas centrales (Insurgentes)	Piso 1	Tipo 1	1
	Piso 2	Tipo 1	1
	Piso 3	Tipo 1	1
	Piso 4	Tipo 1	1
	Piso 5	Tipo 1	1
	Centro de Datos 1	Tipo 1	1
	Centro de Datos 2	Tipo 1	1
	DMZ	Tipo 5	1
	Monitores	Tipo 5	1
Plaza de la Republica	Mezzanine	Tipo 2	2
		Tipo 4	1
	Piso 1	Tipo 2	1
	Piso 2	Tipo 2	1
	Piso 3	Tipo 2	1
	Piso 5	Tipo 2	1
		Tipo 3	1
	Piso 6	Tipo 2	1
	Piso 7	Tipo 2	1
		Tipo 3	1
	Piso 8	Tipo 2	1
		Tipo 3	1
		Tipo 2	1

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

	Piso 9	Tipo 3	1
Acapulco	Ubicación Única	Tipo 5	1
Aguascallentes	Ubicación Única	Tipo 4	1
Almacen Mar Adriatico	Ubicación Única	Tipo 5	1
Campeche	Ubicación Única	Tipo 4	1
Cancun	Ubicación Única	Tipo 4	1
Cd Acuña	Ubicación Única	Tipo 5	1
Cd del Carmen	Ubicación Única	Tipo 5	1
Cd juarez	Ubicación Única	Tipo 4	1
Cd Obregon	Ubicación Única	Tipo 4	1
Cd Valles	Ubicación Única	Tipo 5	1
Cd Victoria	Ubicación Única	Tipo 5	1
Celaya	Ubicación Única	Tipo 5	1
Chetumal	Ubicación Única	Tipo 5	1
Chihuahua	Ubicación Única	Tipo 4	1
		Tipo 4	1
Chilpancingo	Ubicación Única	Tipo 5	1
Coatzacoalcos	Ubicación Única	Tipo 5	1
Colima	Ubicación Única	Tipo 4	1
Congreso del Trabajo	Ubicación Única	No Requerido	0
Cordoba	Ubicación Única	Tipo 5	1
Cozumel	Ubicación Única	Tipo 5	1
Cuautitlan	Ubicación Única	Tipo 5	1
Cuautla	Ubicación Única	Tipo 5	1
Cuernavaca	Ubicación Única	Tipo 4	1
Culiacan	Ubicación Única	Tipo 4	1
Delicias	Ubicación Única	Tipo 5	1
Durango	Ubicación Única	Tipo 4	1
Ecatepec	Ubicación Única	Tipo 5	1
Empalme	Ubicación Única	Tipo 5	1
Ensenada	Ubicación Única	Tipo 5	1
Fresnillo	Ubicación Única	Tipo 5	1

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez. C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Guadalajara Abastos	Ubicación Única	Tipo 4	1
Guadalajara Federalismo	Ubicación Única	No Requerido	0
Hermosillo	Ubicación Única	No Requerido	0
Irapuato	Ubicación Única	Tipo 4	1
La Paz	Ubicación Única	Tipo 4	1
Lazaro Cardenas	Ubicación Única	Tipo 5	1
Leon	Ubicación Única	Tipo 4	1
Los Mochis	Ubicación Única	Tipo 5	1
Manzanillo	Ubicación Única	Tipo 5	1
Matamoros	Ubicación Única	Tipo 5	1
Mazatlan	Ubicación Única	Tipo 4	1
Merida	Ubicación Única	Tipo 4	1
Metro 6	Ubicación Única	Tipo 4	1
Mexicali	Ubicación Única	Tipo 4	1
Monclova	Ubicación Única	Tipo 5	1
Monterrey	Ubicación Única	No Requerido	0
Monterrey 2	Ubicación Única	Tipo 5	1
Morelia	Ubicación Única	Tipo 4	1
Nogales	Ubicación Única	No Requerido	0
Oaxaca	Ubicación Única	Tipo 4	1
Pachuca	Ubicación Única	Tipo 4	1
Piedras Negras	Ubicación Única	Tipo 5	1
Playa del Carmen	Ubicación Única	Tipo 5	1
Portales	Ubicación Única	Tipo 5	1
		Tipo 4	1
Puebla	Ubicación Única	Tipo 4	1
Puerto Vallarta	Ubicación Única	Tipo 4	1
Queretaro	Ubicación Única	Tipo 4	1
Reynosa	Ubicación Única	Tipo 5	1
Saltillo	Ubicación Única	Tipo 4	1
San Jose del Cabo	Ubicación Única	Tipo 5	1
San Juan del Rio	Ubicación Única	Tipo 5	1

Sinelf	Ubicación Única	Tipo 5	1
San Luis Potosi	Ubicación Única	Tipo 4	1
Molinos	Ubicación Única	No Requerido	0
Tampico	Ubicación Única	Tipo 4	1
Tapachula	Ubicación Única	Tipo 5	1
Tehuacan	Ubicación Única	Tipo 5	1
Tepic	Ubicación Única	Tipo 4	1
Texcoco	Ubicación Única	Tipo 5	1
Tijuana	Ubicación Única	Tipo 4	1
Tlalnepantla	Ubicación Única	Tipo 4	1
		No Requerido	0
Tlaxcala	Ubicación Única	Tipo 4	1
Toluca	Ubicación Única	Tipo 4	1
Torreon	Ubicación Única	Tipo 4	1
Tuxtepec	Ubicación Única	Tipo 5	1
Tuxtla	Ubicación Única	Tipo 4	1
Uruapan	Ubicación Única	Tipo 5	1
Vallejo	Ubicación Única	No Requerido	0
Veracruz	Ubicación Única	Tipo 4	1
Villahermosa	Ubicación Única	Tipo 4	1
Xalapa	Ubicación Única	No Requerido	0
Zacatecas	Ubicación Única	Tipo 4	1
Zamora	Ubicación Única	Tipo 5	1
Zaragoza	Ubicación Única	Tipo 4	1
		No Requerido	0
Lerma	Ubicación Única	Tipo 5	1

2.3.3. Red Inalámbrica

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado realizará la implementacion, operación, administración y puesta a punto del servicio de red inalámbrica en las oficinas del Instituto FONACOT, basado en puntos de acceso administrados mediante una controladora.

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

2.1.3.1. Servicio de red inalámbrica en Edificios Sede.

El servicio consiste en implementar un esquema de red inalámbrica que provea cobertura al 100% de las áreas operativas en los edificios sede del instituto Fonacot Oficinas Centrales (Sede Insurgentes) y Plaza de la Republica.
La infraestructura que conforme el servicio de red inalámbrica en edificios sede propuesto por Tecnología en Seguridad y Comunicaciones S.A. de C.V., cumplirá con al menos las siguientes características técnicas:

- Soportará el tratamiento del tráfico en los siguientes esquemas:
  - Centralizado en la Controladora
  - Procesado en cada Punto de Acceso
  - Combinación entre Centralizado en la Controladora y en el Punto de Acceso
- Soportará el protocolo CAPWAP
- Soportará el estándar IEEE 802.1D
- Soportará el estándar IEEE 802.1Q
- Soportará la funcionalidad Proxy ARP
- Soportará e incluir un esquema de ruteo dinámico OSPF sin que esto implique eluso de una licencia adicional.
- Soportará las siguientes acciones para QoS:
  - Rate limit de entrada / salida
  - Prioridad 802.1p
  - Asignará cola de transmisión (queue)
  - Remarcado de paquetes en ToS/DSCP
- Proporcionará un servicio local de DHCP con los siguientes parámetros configurables:
  - Dominio
  - Lease
  - Next Hop o Gateway
  - DNS server
  - WINS server
  - DLS DHCP
- Tendrá la capacidad para detectar e identificar la interferencia proveniente de otros dispositivos RF de tipo: microondas, bluetooth, bridges de video, etc. para que de forma automática se puedan redirigir las conexiones de clientes a canales más limpios o libres de interferencia.
- Empleará los métodos Packet fairness y Airtime fairness para proporcionar QoS.
- Soportará la funcionalidad denominada como Wireless Distribution System (WDS) y cumplir con los siguientes mecanismos:
- Tendrá la capacidad de formar un entrelazamiento inalámbrico entre Puntos de Acceso para formar una malla con trayectorias redundantes, con la finalidad de extender la cobertura en sitios en donde los Puntos de Acceso no puedan ser

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

cableados.

- Poseerá la funcionalidad de unir segmentos de redes alámbricas.
- Capacidad para que los Puntos de Acceso que funcionen como extensión o repetidores puedan también propagar al mismo tiempo el(los) SSID(s) requerido(s).
- Soportará un esquema de Alta Disponibilidad donde las Controladoras operen en modo Activo-Activo, sin necesidad de adquirir licencias o software adicionales para lograr dicha función.
- Contendrá tráfico de Bonjour y multicast, para evitar la introducción de tráfico no requerido y optimizar la operación de red
- Distribución de cargas entre varios Puntos de Acceso adyacentes para prevenir sobre carga de usuarios.
- Soportará la funcionalidad de Location-based Services e integrarse con herramientas como Aeroscout y Ekahau.
- Poseerá la funcionalidad de sincronizarse por medio del protocolo NTP, así como emplear el reloj propio de sistema
- Poddrá integrar Puntos de Acceso de otras marcas, para brindar servicio y seguridad mediante autenticación de usuarios.
- Para esquemas de alta disponibilidad del servicio, contará con la funcionalidad de permitir nuevas sesiones 802.1x aun cuando la comunicación entre la controladora y el Punto de Acceso este interrumpida.

Funciones de Seguridad

- Permitir el filtrado de direcciones MAC para negar o permitir el acceso a los servicios, las direcciones MAC podrán darse de alta de forma individual e importando un archivo.
- Disociación de clientes en forma manual.
- Soportará los siguientes estándares de cifrado o encripcion:
  - WEP
  - TKIP
  - WPA
  - WPA2
  - WPA-PSK
  - WPA2-PSK
  - AES (CCMP)
  - RC4-40, 104, 128-bit
- Interactuará con servidores de RADIUS con el objetivo de definir perfiles deacceso, basados en atributos como Filter-ID
- Soportará los siguientes métodos de autenticación:
- MAC

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Web o Captive Portal
- IEEE 802.1x
- Soportará RFC 3580
- Soportará la funcionalidad de portal cautivo para autenticación con las siguientes características:
- Autenticación 802.1X
- Uso de Portal cautivo interno
- Uso Portal cautivo externo
- Portal de Invitados con acceso temporal
- Personalización tanto para el portal interno como para el de invitados, de acuerdo a los patrones gráficos y logos requeridos por el Instituto FONACOT.
- El portal Cautivo Interno será configurado para desplegarse en HTTPo HTTPS
- El portal Cautivo Interno tendrá la capacidad para presentar diferentes atributos tales como el Número de serie del Punto de Acceso, SSID y MAC Address.
- Soportará los siguientes métodos de autenticación 802.1x:
  - EAP-TLS
  - EAP-MD5
  - EAP-FAST
  - EAP-SIM
  - EAP-TTLS
  - PEAP
- Capacidad para ocultar los SSID's configurados.
- Bloquear tráfico entre dispositivos asociados al mismo SSID
- Permitirá una distinción de privilegios por el tipo de usuario dentro del mismo SSID, dichos privilegios deberán abarcar desde el filtrado de tráfico de capa 2, capa 3 y capa 4, de acuerdo a los siguientes criterios:
  - Source MAC address
  - Destination MAC address
  - IPv4 Source IP address
  - IPv4 Destination IP address
  - Source layer 4 port
  - Destination layer 4 port
  - IPv4 Source socket
  - IPv4 Destination socket
  - IP type
  - ICMP packet type and code
  - ToS/DSCP marking
  - 802.1p priority

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Ethertype

- Limitará ancho de banda tanto a nivel de usuario como por tipo de tráfico, así como manejo de prioridades aplicando calidad de servicio a los mismos a nivel de capa 2 y capa 3.

- Permitirá filtrado de tráfico desde la Controladora y en los Puntos de Acceso de tal forma que este filtrado pueda radicar en los Puntos de Acceso, ya que en caso de un evento en el cual este pierda comunicación con la Controladora, el Punto de Acceso sea capaz de seguir soportando dicha aplicación de reglas.
- El filtrado de tráfico también será soportado para tráfico de Multicast
- Soportará la funcionalidad de actuar como WIDS/WIPS en base a los siguientes requerimientos:
- Detección y clasificación de Puntos de Acceso bajo diferentes categorías como Puntos de Accesos Vecinos o Externos, Autorizados, Ilegítimos o Prohibidos.
- Dicha detección informará datos de los Puntos de Acceso, tales como Dirección MAC, SSID y el Fabricante o Marca del equipo en cuestión.
- Proveerá la funcionalidad de clasificar Puntos de Acceso no categorizados como Puntos de Acceso Vecinos o Externos en forma manual de ser requerido, o en su caso ser clasificados como Puntos de Acceso Ilegítimos.
- Capacidad para llevar a cabo la mitigación de amenazas basada en countermeasures que puedan trabajar por limitación de inundación de tramas, por envío de tramas que eviten a los dispositivos adjuntarse a dispositivos no permitidos y por agregación de dispositivos no permitidos a una lista negra.
- Capacidad para elegir los siguientes tipos de mitigación de amenazas o countermeasures:
  - Prevenir a dispositivos permitidos para hacer roaming sobre Puntos de Acceso no permitidos tales como Vecinos o Externos, Ilegítimos o Prohibidos.
  - Prevenir a los dispositivos en participar en redes de tipo Ad-Hoc.
  - Remover dispositivos que estén generando algún tipo de ataque de DoS.
  - Eliminará tramas responsables que generen un ataque de inundación de tráfico.
- Reconocimiento de las siguientes amenazas:
  - Conexiones Ad-Hoc
  - Cracking de llaves WPA-WEP
  - Aplicaciones de tipo surveillance como Netstumbler

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Ataques de DoS
- Puntos de Acceso tipo Honeypot
- Detección de fuentes de interferencia como por ejemplo hornos de microondas o algún otro dispositivo que opere en la banda de los 2.4 GHz.
- Puntos de Acceso tipo spoofing

- La funcionalidad WIDS/WIPS proveerá reportes con el siguiente tipo de información:
- Fecha y hora en de detección de amenaza
- MAC Address del dispositivo fuente
- Tipo de amenza y categoria
- Intensidad de señal de la fuente de amenza (dBm)
- Access Point que realiza medida de contención
- Tipo de medida aplicada
- Clientes enviados a Lista Negra
- Detección de Rogue APs por método closed loop alámbrico / inalámbrico para reducción de falsos positivos

Funcionalidades de Administración y Monitoreo

- Contará con un Dashboard que presente los principales eventos en forma textual, gráfica y estadística de la red inalámbrica:
- Estatus de Access Point
- Clientes
- Sesiones activas de administradores
- Access Point por canal
- Licenciamiento
- WLANs inseguras
- Access Point sin categorizar
- Amenazas activas
- Eventos
- Soportará la función para gestionar usuarios que administren el sistema con privilegios de lectura/escritura y solo lectura, ya sea por autenticación local o remota, así como un tipo de usuario administrador adicional que solo pueda tener los privilegios para gestionar las cuentas de invitados y esta sea la única función a la que tenga acceso.
- Soportará SNMP v2c/v3
- La controladora soportará los siguientes esquemas de administración:
  - GUI o Web
  - CLI

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Consola
- Soportará el backup y restore de Imagen de Controladora, por los siguientes medios
  - FTP
  - Local
  - Flash
- La actualización del firmware de la Controladora podrá realizarse a través de GUI (Web) y por CLI
- Poseerá una función de actualización de firmware y almacenamiento de imágenes de respaldo (snapshot), para recuperar la controladora en caso de que el proceso falle o bien la imagen se encuentre dañada o corrupta
- Tendrá la función de realizar respaldos de la configuración en forma manual o calendarizada y que estos puedan ser enviados en forma automática a

  un servidor de almacenamiento por medio de un protocolo como FTP o SCP.
- Capacidad de envío de logs de acuerdo a su grado de severidad a un servidor Syslog, correspondientes a eventos de los Puntos de Acceso, Controladora, cambios de configuración y de los principales servicios proporcionados por la Controladora.
- Mostrará la siguiente información:
  - Puntos de Acceso Activos
  - Estadísticas WDS
  - Estadísticas de Balanceo de Cargas
  - Estadísticas de Alta Disponibilidad
  - Inventario de los Puntos de Acceso
- Mostrará la siguiente información con respecto a ruteo:
  - Forwarding Table
  - OSPF Linkstate
  - OSPF Neighbor
- Realizará un Inventario de los Puntos de Acceso que incluya:
  - Dirección IP/Máscara de Red/Gateway
  - Dirección MAC del Puerto Ethernet.
  - Versión de hardware y software
  - Antenas empleadas
  - Telnet or SSH (estado activo/inactivo)
  - DTIM period
  - Beacon Period
  - RTS Threshold
  - Canal(es) de Transmisión
  - Potencia de Transmisión (dB)

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de lo mismo

Ciudad de México a 17 de mayo de 2022.

- Rx Diversity
- Tx Diversity
- Preambulo (long, short)
- 11n Channel Width
- 11n Guard Interval
- 11n Channel Bonding

- Herramientas de troubleshooting tales como PING, Traceroute, captura de paquetes en tiempo real.
- Proporcionará un histórico de sesiones de usuarios, conocido como CallDetail Records (CDR).

Como parte del servicio de Red Inalambrica, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado realizará las siguientes actividades:

- Proveer todo lo necesario relacionado con hardware y software para la instalación y puesta a punto del esquema de alta disponibilidad de las controladoras con las que se administraran todos los Access Points que conformen el servicio de Red Inalámbrica.

- Mantener a la última versión disponible la controladora y los Access Points (firmware) durante toda la vigencia del servicio.
- Realizar los cambios, ajustes y configuraciones necesarias, en los Access Points y en controladora.
- Administrar altas, bajas y cambios en los equipos y controladoras.
- Proveer cualquier accesorio, componente y/o material misceláneo necesario para la instalación y el funcionamiento de los Access Points y controladoras.
- Mantener operando correctamente el servicio de Red Inalámbrica durante toda la vigencia del servicio.
- Entregar reportes mensuales ó a solicitud del area técnica del Instituto FONACOT, relaiconados con el servicio de Red Inalámbrica, como, por ejemplo velocidad promedio de usuarios, fallas, etc.
- A solicitud expresa del area tecnica, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado realizará estudios de cobertura de red inalámbrica de cualquier sucursal del Instituto FONACOT. Los resultados de dicho estudio permitirán definir la infraestructura necesaria para implementar servicios de red inalámbrica adicionales, en estos casos, la infraestructura requerida se solicitará expresamente por el administrador del contrato bajo el concepto de Servicios Bajo Demanda.

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

2.3.3.3. **Servicio de red inalámbrica en Localidades.** Ciudad de México a 17 de mayo de 2022.

El servicio consiste en implementar un esquema de red inalámbrica que provea cobertura a las áreas operativas en las localidades del Instituto Fonacot a nivel nacional. La infraestructura que conforme el servicio de red inalámbrica propuesto por Tecnología en Seguridad y Comunicaciones S.A. de C.V., cumplirá con al menos las siguientes características técnicas:

- Soportará el tratamiento del tráfico en los siguientes esquemas:
  - Centralizado en la Controladora
  - Procesado en cada Punto de Acceso
  - Combinación entre Centralizado en la Controladora y en el Punto de Acceso
- Soportará el protocolo CAPWAP
- Soportará el estándar IEEE 802.1D
- Soportará el estándar IEEE 802.1Q
- Soportará la funcionalidad Proxy ARP
- Soportará e incluirá un esquema de ruteo dinámico OSPF sin que esto implique eluso de una licencia adicional.
- Soportará las siguientes acciones para QoS:
  - Rate limit de entrada / salida
  - Prioridad 802.1p
  - Asignará cola de transmisión (queue)
  - Remarcado de paquetes en ToS/DSCP
- Proporcionará un servicio local de DHCP con los siguientes parámetros configurables:
  - Dominio
  - Lease
  - Next Hop o Gateway
  - DNS server
  - WINS server
  - DLS DHCP
- Tendrá la capacidad para detectar e identificar la interferencia proveniente de otros dispositivos RF de tipo: microondas, bluetooth, bridges de video, etc. para que de forma automática se puedan redirigir las conexiones de clientes a canales más limpios o libres de interferencia.
- Empleará los métodos Packet fairness y Airtime fairness para proporcionar QoS.
- Soportará la funcionalidad denominada como Wireless Distribution System (WDS) y cumplirá con los siguientes mecanismos:
- Tendrá la capacidad de formar un entrelazamiento inalámbrico entre Puntos de

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Acceso para formar una malla con trayectorias redundantes, con la finalidad de extender la cobertura en sitios en donde los Puntos de Acceso no puedan ser cableados.

- Poseerá la funcionalidad de unir segmentos de redes alámbricas.
- Capacidad para que los Puntos de Acceso que funcionen como extensión o repetidores puedan también propagar al mismo tiempo el(los) SSID(s) requerido(s).
- Soportará un esquema de Alta Disponibilidad donde las Controladoras operen en modo Activo-Activo, sin necesidad de adquirir licencias o software adicionales para lograr dicha función.
- Contendrá tráfico de Bonjour y multicast, para evitar la introducción de tráfico no requerido y optimizar la operación de red
- Distribución de cargas entre varios Puntos de Acceso adyacentes para prevenir sobre carga de usuarios.
- Soportará la funcionalidad de Location-based Services e integrarse con herramientas como Aeroscout y Ekahau.
- Poseerá la funcionalidad de sincronizarse por medio del protocolo NTP, así como emplear el reloj propio de sistema
- Podrá integrar Puntos de Acceso de otras marcas, para brindar servicio y seguridad mediante autenticación de usuarios.
- Para esquemas de alta disponibilidad del servicio, contará con la funcionalidad de permitir nuevas sesiones 802.1x aun cuando la comunicación entre la controladora y el Punto de Acceso este interrumpida.

Funciones de Seguridad

- Permitirá el filtrado de direcciones MAC para negar o permitir el acceso alos servicios, las direcciones MAC podrán darse de alta de forma individual e importando un archivo.
- Disociación de clientes en forma manual.
- Soportar los siguientes estándares de cifrado o encripcion:
  - WEP
  - TKIP
  - WPA
  - WPA2
  - WPA-PSK
  - WPA2-PSK
  - AES (CCMP)
  - RC4-40, 104, 128-bit
- Interactuará con servidores de RADIUS con el objetivo de definir perfiles

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

deacceso, basados en atributos como Filter-ID

- Soportará los siguientes métodos de autenticación:
- MAC
- Web o Captive Portal
- IEEE 802.1x
- Soportará RFC 3580
- Soportará la funcionalidad de portal cautivo para autenticación con las siguientes características:
- Autenticación 802.1X
- Uso de Portal cautivo interno
- Uso Portal cautivo externo
- Portal de Invitados con acceso temporal
- Personalización tanto para el portal interno como para el de invitados, de acuerdo a los patrones gráficos y logos requeridos por el Instituto FONACOT.
- El portal Cautivo Interno será configurado para desplegarse en HTTPo HTTPS
- El portal Cautivo Interno tendrá la capacidad para presentar diferentes atributos tales como el Número de serie del Punto de Acceso,SSID y MAC Address.
- Soportará los siguientes métodos de autenticación 802.1x:
  - EAP-TLS
  - EAP-MD5
  - EAP-FAST
  - EAP-SIM
  - EAP-TTLS
  - PEAP
- Capacidad para ocultar los SSID's configurados.
- Bloquear tráfico entre dispositivos asociados al mismo SSID
- Permitirá una distinción de privilegios por el tipo de usuario dentro del mismo SSID, dichos privilegios deberán abarcar desde el filtrado de tráfico de capa 2, capa 3 y capa 4, de acuerdo a los siguientes criterios:
  - Source MAC address
  - Destination MAC address
  - IPv4 Source IP address
  - IPv4 Destination IP address
  - Source layer 4 port
  - Destination layer 4 port
  - IPv4 Source socket

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- IPv4 Destination socket
- IP type
- ICMP packet type and code
- ToS/DSCP marking
- 802.1p priority
- Ethertype

- Limitará ancho de banda tanto a nivel de usuario como por tipo de tráfico, así como manejo de prioridades aplicando calidad de servicio a los mismos a nivel de capa 2 y capa 3.
- Permitirá filtrado de tráfico desde la Controladora y en los Puntos de Acceso de tal forma que este filtrado pueda radicar en los Puntos de Acceso, ya que en caso de un evento en el cual este pierda comunicación con la Controladora, el Punto de Acceso sea capaz de seguir soportando dicha aplicación de reglas.
- El filtrado de tráfico también será soportado para tráfico de Multicast
- Soportar la funcionalidad de actuar como WIDS/WIPS en base a los siguientes requerimientos:
- Detección y clasificación de Puntos de Acceso bajo diferentes categorías como Puntos de Accesos Vecinos o Externos, Autorizados, Ilegítimos o Prohibidos
- Dicha detección informará datos de los Puntos de Acceso, talescomo Dirección MAC, SSID y el Fabricante o Marca del equipo en cuestión.
- Proveerá la funcionalidad de clasificar Puntos de Acceso no categorizados como Puntos de Acceso Vecinos o Externos en forma manual de ser requerido, o en su caso ser clasificados como Puntos de Acceso Ilegítimos.
- Capacidad para llevar a cabo la mitigación de amenazas basada en countermeasures que puedan trabajar por limitación de inundación de tramas, por envío de tramas que eviten a los dispositivos adjuntarse a dispositivos no permitidos y por agregación de dispositivos no permitidos a una lista negra.
- Capacidad para elegir los siguientes tipos de mitigación de amenazas o countermeasures:
  - Puede prevenir a dispositivos permitidos para hacer roaming sobre Puntosde Acceso no permitidos tales como Vecinos o Externos, Ilegítimoso Prohibidos.
  - Puede prevenir a los dispositivos en participar en redes de tipo Ad-Hoc.
  - Puede remover dispositivos que estén generando algún tipo de ataque deDoS.
  - Puede eliminar tramas responsables que generen un ataque de inundación de tráfico.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Reconocimiento de las siguientes amenazas:
  - Conexiones Ad-Hoc
  - Cracking de llaves WPA-WEP
  - Ataques de DoS
  - Puntos de Acceso tipo Honeypot
  - Detección de fuentes de interferencia como por ejemplo hornos de microondas o algún otro dispositivo que opere en la banda de los 2.4 GHz.
  - Puntos de Acceso tipo spoofing
- La funcionalidad WIDS/WIPS proveerá reportes con el siguientetipo de información:
- Fecha y hora en de detección de amenaza
- MAC Address del dispositivo fuente
- Tipo de amenza y categoria
- Intensidad de señal de la fuente de amenza (dBm)
- Access Point que realiza medida de contención
- Tipo de medida aplicada
- Clientes enviados a Lista Negra
- Detección de Rogue APs por método closed loop alámbrico / inalámbrico para reducción de falsos positivos

Funcionalidades de Administración y Monitoreo

- Contará con un Dashboard que presente los principales eventos en forma textual, gráfica y estadistica de la red inalámbrica:
- Estatus de Access Point
- Clientes
- Sesiones activas de administradores
- Access Point por canal
- Licenciamiento
- WLANs inseguras
- Access Point sin categorizar
- Amenazas activas
- Eventos
- Soportará la función para gestionar usuarios que administren el sistema con privilegios de lectura/escritura y solo lectura, ya sea por autenticación local o remota, así como un tipo de usuario administrador adicional que solo pueda tener los privilegios para gestionar las cuentas de invitados y esta sea la única función a la que tenga acceso.
- Soportará SNMP v2c/v3

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- La controladora soportará los siguientes esquemas de administración:
  - GUI o Web
  - CLI
  - Consola
- Soportará el backup y restore de Imagen de Controladora, por los siguientes medios
  - FTP
  - Aplicaciones de tipo surveillance como Netstumbler
  - Local
  - Flash
- La actualización del firmware de la Controladora podrá realizarse a través de GUI (Web) y por CLI
- Poseerá una función de actualización de firmware y almacenamiento de imágenes de respaldo (snapshot), para recuperar la controladora en caso de que el proceso falle o bien la imagen se encuentre dañada o corrupta
- Tendrá la función de realizar respaldos de la configuración en forma manual o calendarizada y que estos puedan ser enviados en forma automática aun servidor de almacenamiento por medio de un protocolo como FTP oSCP.
- Capacidad de envío de logs de acuerdo a su grado de severidad a un servidor Syslog, correspondientes a eventos de los Puntos de Acceso, Controladora, cambios de configuración y de los principales servicios proporcionados por la Controladora.
- Mostrará la siguiente información:
  - Puntos de Acceso Activos
  - Estadísticas WDS
  - Estadísticas de Balanceo de Cargas
  - Estadísticas de Alta Disponibilidad
  - Inventario de los Puntos de Acceso
- Mostrará la siguiente información con respecto a ruteo:
  - Forwarding Table
  - OSPF Linkstate
  - OSPF Neighbor
- Realizará un Inventario de los Puntos de Acceso que incluya:
  - Dirección IP/Máscara de Red/Gateway
  - Dirección MAC del Puerto Ethernet.
  - Versión de hardware y software
  - Antenas empleadas
  - Telnet or SSH (estado activo/inactivo)

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- DTIM period
- Beacon Period
- RTS Threshold
- Canal(es) de Transmisión
- Potencia de Transmisión (dB)
- Rx Diversity
- Tx Diversity
- Preambulo (long, short)
- 11n Channel Width
- 11n Guard Interval
- 11n Channel Bonding

- Herramientas de troubleshooting tales como PING, Traceroute, captura de paquetes en tiempo real.

- Proporcionará un histórico de sesiones de usuarios, conocido como Call Detail Records (CDR).

Como parte del servicio de Red Inalambrica, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado realizará las siguientes actividades:

- Proveer todo lo necesario relacionado con hardware y software para la instalación y puesta a punto del esquema de alta disponibilidad de las controladoras con las que se administraran todos los Access Points que conformen el servicio de Red Inalámbrica.
- Mantener a la última versión disponible la controladora y los Access Points (firmware) durante toda la vigencia del servicio.
- Realizar los cambios, ajustes y configuraciones necesarias, en los Access Points y en controladora.
- Administrar altas, bajas y cambios en los equipos y controladoras.
- Proveer cualquier accesorio, componente y/o material misceláneo necesario para la instalación y el funcionamiento de los Access Points y controladoras.
- Mantener operando correctamente el servicio de Red Inalámbrica durante toda la vigencia del servicio.
- Entregar reportes mensuales ó a solicitud del area técnica del Instituto FONACOT, relacionados con el servicio de Red Inalámbrica, como, por ejemplo: velocidad promedio de usuarios, fallas, etc.
- A solicitud expresa del area tecnica, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado realizará estudios de cobertura de red inalámbrica de cualquier sucursal del Instituto FONACOT. Los resultados de dicho estudio permitirán definir

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

la infraestructura necesaria para implementar servicios de red inalámbrica adicionales, en estos casos, la infraestructura requerida se solicitará expresamente por el administrador del contrato bajo el concepto de Servicios Bajo Demanda.

Los sitios donde se requiere el servicio de Red Inalambrica son los siguientes, mismos que podrán variar según las necesidades del Instituto.

Item	Localidad
1	ACAPULCO
2	AGUASCALIENTES
3	Lerma
4	CAMPECHE
5	CANCÚN
6	CD. DEL CARMEN
7	CD. JUÁREZ
8	CD. OBREGÓN
9	CELAYA
10	CHIHUAHUA
11	CHILPANCINGO
12	METRO 6
13	COATZACOALCOS
14	COLIMA
15	CONGRESO
16	CUERNAVACA
17	CULIACÁN
18	DELICIAS
19	DURANGO
20	GUADALAJARA ABASTOS
21	GUADALAJARA FEDERALISMO
22	HERMOSILLO
23	LA PAZ
24	LÁZARO CÁRDENAS
25	LEÓN
26	LOS MOCHIS

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

27	MANZANILLO
28	MAZATLÁN
29	MÉRIDA
30	MEXICALI
31	MIXCOAC
32	MONCLOVA
33	MONTERREY
34	MONTERREY II
35	MORELIA
36	NOGALES
37	OAXACA
38	PACHUCA
39	PORTALES
40	PUEBLA
41	PUERTO VALLARTA
42	QUERÉTARO
43	REYNOSA
44	SALTILLO
45	SAN LUIS POTOSÍ
46	TAMPICO
47	TEPIC
48	TIJUANA
49	TLALNEPANTLA
50	TLAXCALA
51	TOLUCA
52	TORREÓN
53	TUXTLA GUTIÉRREZ
54	URUAPAN
55	VALLEJO
56	VERACRUZ
57	VILLAHERMOSA
58	XALAPA
59	ZACATECAS
60	ZARAGOZA
61	Almacen Mar Adriatico

2.3.4. Archivos Compartidos en Red.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., realizará las actividades para la administración de los servicios de FileServer y FTP. Actualmente estos servicios se encuentran operando en Oficinas Centrales del Instituto FONACOT bajo la plataforma del Sistema Operativo de MS Windows Server 2016 .
El servicio operará en infraestructura de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar ganador migrando bajo las siguientes particularidades:

2.3.4.1. FILESERVER.

- Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar ganador configurará el servicio para operar utilizandoReplicación DFS (Distributed File System) lo cual permita la replicación como estrategia de recuperación ante desastres
- El servicio operará basado en 1 nodo virtual en OC (sedeInsurgentes)
- • Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar ganador realizará la administración de los recursos configurando las particiones para alojar los datos del File Server en formato NTFS, así como la utilización de certificados SSL y estableciendo Quotas para limitar almacenamiento; estos límites de almacenamiento y los usuarios con acceso al éste servicio serán establecidos conforme a las necesidades del Instituto FONACOT.
- El servicio permitirá el uso de WorkFolders con acceso desde dispositivos Android, iOS y equipos de cómputo con versiones de sistema operativo Windows 7 o superiores, debiéndose poder filtrar y no permitir subir archivos de música, imágenes y video.
- El servicio de WorkFolders contará con una capacidad de almacenamiento de mínimo de 2GB por usuario
- El servicio de File Server contará con la opción de recuperación de archivos borrados en la red, por parte del usuario, contando con al menos

una versión diaria de la información. Así como permitir obtener información de la tendencia del uso del servicio

- Las versiones para recuperación estarán disponibles dentro de un límite de 1 TB y podrá ser modificado conforme a las necesidades del Instituto FONACOT.
- El servicio contemplará la creación de Checkpoints para las máquinas virtuales, permitiendo su utilización en caso de falla en los equipos virtualizados. Estas copias se realizarán cuando menos una vez al mes o cuando se realicen cambios en la configuraciones delservicio.
- Todas las actividades necesarias relacionadas con la migración, instalación, puesta a punto, operación y administración de estos servicios para los sitios que corresponda son responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar ganador
- En función de la migración del servicio de FileServer este se mantendrá operando en las Oficinas Centrales del Instituto FONACOT (Sede Insurgentes).
- La infraestructura que Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar ganador disponga para otorgar el servicio de FileServer mantendrá rangos menores al 80% diario,en lo que respecta al uso del procesador, memoria física y espacio de almacenamiento de todas las unidades de disco que componen el servicioporcada servidor instalado.
- Esto implica que el servicio de monitoreo configurará alertas con un umbral 80% en CPU, memoria y discos.

2.3.4.2. **FTP**

- El servicio se autentificará a los usuarios para su acceso a la información por medio credenciales de dominio y cuentas locales, no permitiéndose los accesos anónimos. Para realizar lo anterior, el Instituto FONACOT proporcionara todas las facilidades a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar ganador para integrarse con el servicio de Active Directory Institucional
- Para alojar los datos del FTP Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar ganador configurará lasparticiones de almacenamiento en formato NTFS
- Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar ganador garantizará la integridad, confidencialidad y disponibilidad de la información contenida en las carpetas durante y

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

posteriormente a la migración del servicio.

- Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar ganador realizará el respaldo de la información cuando menos de forma semanal manteniendo los dos inmediatos anteriores respaldos.

El servicio contemplará la creación de Checkpoints para las máquinas virtuales, permitiendo su utilización en caso de falla en los equipos virtualizados. Estas copias se realizarán cuando menos una vez al mes o cuando se realicen cambios en las configuraciones del servicio.

- En función de la migración del servicio de FTP, este operará en las oficinas centrales del Instituto FONACOT (Sede Insurgentes)
- La infraestructura que Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar ganador disponga para otorgar elservicio de FTP mantendrá rangos menores al 80% diario, en loque respecta al uso del procesador, memoria física y espacio dealmacenamiento de todas las unidades de disco que componen el servicio por cada servidor instalado.
- Esto implica que el servicio de monitoreo debe configurar alertas con un umbral 80% en CPU, memoria y discos.

Todo el licenciamiento necesario de la plataforma de Microsoft será proporcionado por el área técnica del Instituto FONACOT para la implementación de los servicios

GESTIÓN DE LA SEGURIDAD.

El Instituto FONACOT requiere el servicio de gestión de la Seguridad alineado a estándares, mejores prácticas internacionales y disposiciones establecidas por la administración pública federal en materia de seguridad informática, con el objeto de que la implantación, operación, monitoreo de la seguridad se proporcione con altos niveles de servicio. Tecnología en Seguridad y Comunicaciones S.A. de C.V., aplicará la proactividad (prevención) necesaria para reducir el riesgo de ataques e incidentes sobre los componentes de seguridad involucrados en el otorgamiento del servicio solicitado.

El personal que designe el area tecnica del Instituto FONACOT contará con acceso de sólo lectura a los equipos de seguridad utilizados para la prestación del servicio y en loscasos que el administrador del contrato solicite se requiera, en acuerdo con Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado proporcionará acceso total a los equipos destinados a soportar el servicio, con el fin de supervisar y validar la configuración de los mismos.

Realizará, con base en estándares de seguridad, las acciones para el reforzamiento o

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

endurecimiento de las configuraciones de parámetros de seguridad (hardening, políticas, reglas, etc.) de los elementos de infraestructura involucrados en el servicio solicitado, en función de las vulnerabilidades conocidas, además de aquellas que sean solicitadas explícitamente por el area técnica del Instituto FONACOT.

Identificar y notificar vulnerabilidades, ataques, virus, malware y todo aquello que pueda impactar la seguridad informática del Instituto FONACOT, efectuado las acciones correctivas necesarias de forma remota o en sitio a fin de corregir la posible falla de seguridad.

2.3.1. **Servicio de Contención Perimetral.**

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado implementará una solución de contención perimetral paraproteger las Oficinas Centrales Sedes (Insurgentes y Plaza de la Republica) y sucursales del Instituto FONACOT, mediante equipos firewall de ultima generación, que proporcionarán al menos las siguientes funciones: Firewall, Control e Identificación de Aplicaciones, VPNs Site to Site basadas en IPSec y SSL, IPS, Control Contra Amenazas, Control de Acceso y Transmisión de datos, así como la Generación de Reportes. Todoslos equipos que conformen la solución seán administrados mediante una consola centralizada con herramientas graficas que permita simplificar la gestión y edición de políticas de una manera segura y sencilla.

La solución de contención perimetral propuesta por Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerará esquemas de alta disponibilidad en modo activo-activo, para el caso de Oficinas Centrales y Plaza de la Republica. Es responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerar la instalación, configuración, puesta a punto y administración del esquema de contenciónpropuesto.

La solución tendrá la capacidad de generar políticas de seguridad a partir de la identificación de aplicaciones independientemente del protocolo, puerto de comunicación, cifrado o tácticas evasivas, asimismo, deberá identificar nombres de usuario y/o direcciones IP, y utilizar esta información para tener visibilidad, aplicar políticas.

Los equipos propuestos por Tecnología en Seguridad y Comunicaciones S.A. de C.V., para otorgar el servicio de contención perimetral cumplirán con al menos las siguientes caraterísticas técnicas:

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrego de la misma

Ciudad de México a 17 de mayo de 2022.

7.3.1.1. Firewall Tipo 1

- El equipo estará basado en una plataforma Appliance del mismo fabricante
- Contará con al menos 4 puertos 10/100/1000, y 6 puertos GigabitSFP
- Contará con 2 fuentes de energía eléctrica redundantes
- Realizará las funciones de firewall conforme a los siguientes puntos:
  - Operar de manera simultánea en modo sniffer tanto en la capa 2 (nivel físico) como en la capa 3 (nivel lógico) del modelo OSI para efectuar la inspección del tráfico de datos de la red vía un puerto espejo
  - Efectuar ruteo virtual para al menos 10 ruteadores virtuales
  - Manejar tráfico entre diferentes zonas de seguridad y subredes, soportando al menos 80 zonas de seguridad y un mínimo de 10 firewalls virtuales.
  - Cada firewall virtual soportará como mínimo:
    - 1,000,000 sesiones simultaneas
    - 1000 reglas de seguridad
    - 1,000 reglas de NAT
    - 2,000 túneles VPN IPSec
- Soportará al menos 4,094 redes virtuales basadas en el protocolo 802.1q portodo el equipo.
- Operará NAT por origen, destino, dirección ip y puertos
- Soportará como mínimo los protocolos: PPoE, BGP, OSPF, rip2, DHCP Server y Relay
- Soportará los protocolos de cifrado: ike, 3des (128, 192 y 256 bits), aes, sha1 y md5.
- Identificará usuarios mediante LDAP, Directorio Activo, Radius y direccion IP
- Identificará aplicaciones como facebook, twitter, web 2.0, peer to peer. Ésta identificación será de manera independiente al puerto lógico y/o aplicaciones que usan los puertos 80 y 443 (identificación de aplicaciones que viajen a través de un túnel SSL o que utilicen tácticas evasivas)
- Capacidad para visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas para viajar cifradas, tales como ultrasurf, skype y ataques mediante el puerto 443.
- Permitirá elaborar políticas de seguridad con base al protocolo y puerto
- Incluirá tecnología superior a stateful firewalling
- Creará firmas para identificar las aplicaciones desarrolladas por el

INSTITUTO FONACOT

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022

- Descifrar de sesiones SSL para identificar las aplicaciones que se transmiten dentro de túneles SSL
- Creará políticas para el manejo de aplicaciones desconocidas basadas en TCP/UDP
- Identificará aplicaciones incluso cuando no utilicen puertos estándares. (En el caso de protocolos desconocidos se deberá asignar firmas propias)
- Descripción y control de tráfico ssh
- Descifrar aplicaciones dinámicas dentro de sesiones de proxy HTTP
- Controlar tráfico IPv4 e IPv6, (En IPv6 incluir visibilidad e inspección de amenazas en aplicaciones y control de contenido)
- Soportará IPv6 en interfaces trabajando en capa 2 y capa 3
- Realizará el control e identificación de aplicaciones conforme a los siguientes puntos:
  - Permitir, negar, calendarizar, inspeccionar políticas de uso con base en aplicaciones
  - Definición de hasta 8 clases de tráfico, con la finalidad de controlar aplicaciones cuyo consumo pueda ser excesivo como el streaming.
  - Permitir el monitoreo del uso de aplicaciones.
- Las funciones de VPN IPSec y SSL las realizará conforme a los siguientes puntos:
  - Soportará como mínimo 2000 túneles VPN IPSec con un rendimiento de al menos 2Gbps de traughput.
  - Aplicará políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles SSL.
  - Contará con SSL fall back y descifrado SSL (entrada y salida).
  - Contará con un software cliente de VPN SSL para los sistemas operativos Windows 7, Windows 8.1, Windows 10 y MAC OSX V10.10 o superior.
  - Permitirá la creación de políticas para tráfico VPN SSL
  - Soportará al menos 15,000 sesiones concurrentes vía SSL
  - Realizará la autenticación de VPN SSL a través de LDAP, Secure Id y/o Base de Datos Propia
- La función de IPS Control Contra Amenazas, se efectuará de acuerdo a lo siguiente:
  - Soportar protección contra malware en contenido HTML, Java script, Software Espía y Gusanos.
  - Ofrecer protección contra descargas involuntarias usando HTTP de archivos ejecutables maliciosos
  - Efectuar escaneo de virus en HTTP, SMTP y POP3
  - Ejecutar la inspección de archivos comprimidos que usan algoritmo deflate (zip, gzip, etc).
  - Soportar bloqueo de archivos por tipo (Tener registrados como mínimo 50 tipos)

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Adaptar firmas Phone, bots, de software espía y explotación de vulnerabilidades
- Realizar la actualización de firmas de ataques de forma diaria, semanal y de emergencia.
- Protección contra amenazas de Malware y Spyware
- Rendimiento como mínimo de 2Gbps de Troughput.
- Incluya mecanismos de IPS basados en:
  - Análisis de patrones de estado
  - Análisis de decodificación de protocolo
  - Análisis para detección de anomalías de protocolo
  - Análisis heurístico
  - IP desfragmentación
  - Reensamblado de paquetes de TCP
- Permitir el diseño de firmas de vulnerabilidades
- Haber pasado pruebas de los laboratorios NSS con al menos un 90% de efectividad para lo cual deberán incluir el reporte correspondiente
- Identificación de botnet por comportamiento
- Interceptar archivos ejecutables y realiza ejecución en un entorno Sanbox, para determinar si son archivos legítimos o malware tratando de entrar a la red
  - Realizará el control de acceso y transmisión de datos conforme a lo siguiente:
- Administrar el tráfico de aplicaciones, permitiendo la ejecución de aplicaciones autorizadas identificar nuevas aplicaciones.
- Crear políticas basadas en la visibilidad y control de quién está usando qué aplicaciones, a través de la integración con servicios de directorio.
- Autenticación vía LDAP, Directorio Activo, e directory y Base de Datos locales
- Crear políticas basadas por aplicación, categoría de aplicación, sub-categoría, tecnología y factor de riesgo.
- Crear políticas basadas en el control por usuario, grupos de usuarios o dirección IP.
- Crear políticas basadas en Traffic shaping por aplicación, usuario, fuente, destino, Túnel VPN-IPSec-SSL
- Controlar sin instalación de cliente de software, en equipos que soliciten salida a internet para que antes de iniciar la navegación, se despliegue un portal de autenticación residente en el firewall (captive portal) con soporte a autenticación por client certificate.
- Soporte autenticación Kerberos
- Protección contra ataques de negación de servicios.
- Control de host diferentes a Windows, vía autenticación basada en web

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 525, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Proporcionar un resumen gráfico de aplicaciones utilizadas vs amenazas encontradas diariamente.
- Permitir el control de transferencia de datos no autorizados con herramienta para realizar patrones definidos por usuario.
- Contar con la funcionalidad para la exportación de bitácoras (logs) de filtrado, vista de tráfico URL y amenazas
- Permitir la administración vía web, cli, syslog, snmp2.
- Administración basada en roles.
- Permitir la creación de reportes personalizados.
- Contar con herramienta para crear filtros de monitoreo de las sesiones históricas en el firewall ya sea por aplicación, IP origen y destino.
- Capacidad para generar un reporte gráfico que permita visualizar los cambios en el uso de aplicaciones en la red con respecto a un periodo de tiempo anterior
- Generación de reportes con mapas geográficos generados en tiempo real para la visualización de orígenes y destinos del tráfico generado.
- Proporcionar como mínimo los siguientes reportes:
  - Utilización de ancho de banda de entrada y salida por aplicación (TOP 10)
  - No. De Sesiones por aplicación (TOP 10)
  - Comparativo semanal de aplicaciones corriendo en la red que pudieran incrementar o decrementar su utilización (top 10)
  - utilización (en bytes) por aplicación (top 10).
  - Origen y destino del tráfico por aplicación-usuario (TOP 10)
  - Eventos / Ataques por: Origen, Categoría, Amenaza, Protocolo. (TOP 10)
  - Nivel de riesgo de la red.
  - Principales aplicaciones que circulan por el Firewall (TOP 25).
  - Principales direcciones IP destino por protocolo (TOP 25).
  - Las principales direcciones IP para cada uno de los protocolos y aplicaciones (TOP 50)

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Ciudad de México a 17 de mayo de 2022.

- Incluirá una tecnología de detección de amenazas avanzadas con la detección de vulnerabilidades, detección de evasión y aprendizaje de maquina (machine learning).
- Incluirá la inspección de malware en día cero para documentos tipo Ejecutables, dll, Office (Word, Excel, Powerpoint) , pdf, apk, jar (Java), y Adobe Flash.
  - Bidirectional Forwarding Detection (BDF)
- Identificará usuarios a través de integración con Active Directory,LDAP, eDirectory.
- Reporte de aplicaciones tipo SAAS.
- Funcionalidad de prevención de robo de credenciales detectando el momento en que los usuarios envían credenciales corporativas validas a un sitio. Este procedimiento puede realizarse de acuerdo a un grupo de usuarios de LDAP e identificación de usuarios activos en la red.

1.3.1.1. Firewall Tipo 2

- El equipo estará basado en una plataforma Appliance del mismo fabricante
- Contará con al menos 8 puertos 10/100/1000
- Efectuará la detección de falla mediante supervisión de rutas y monitoreo de interfaces
- Realizará las funciones de firewall conforme a los siguientes puntos:
  - Operar de manera simultánea en modo sniffer tanto en la capa 2 (nivel físico) como en la capa 3 (nivel lógico) del modelo OSI para efectuar la inspección del tráfico de datos de la red vía un puerto espejo
  - Efectuar ruteo virtual para al menos 3 ruteadores virtuales
- Manejará tráfico entre diferentes zonas de seguridad y subredes, soportando al menos 10 zonas de seguridad
- El firewall soportará como mínimo:
  - 64,000 sesiones simultaneas
  - 250 reglas de seguridad
  - 125 reglas de NAT
  - 500 túneles VPN IPSec
- Soportará al menos 246 redes virtuales basadas en el protocolo 802.1q
- Operará NAT por origen, destino, dirección ip y puertos
- Soportará como mínimo los protocolos: PPoE, BGP, OSPF, rip2, DHCP Server y Relay
- Soportará los protocolos de cifrado: ike, 3des (128, 192 y 256 bits), aes, sha1 y md5

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022

- Identificará usuarios mediante LDAP, Directorio Activo, Radius y dirección IP
- Identificará aplicaciones como facebook, twitter, web 2.0, peer to peer. Esta identificación será de manera independiente al puerto lógico y/o aplicaciones que usan los puertos 80 y 443 (identificación de aplicaciones que viajen a través de un túnel SSL o que utilicen tácticas evasivas)
- Capacidad para visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas para viajar cifradas, tales como ultrasurf, skype y ataques mediante el puerto 443.
- Permitirá elaborar políticas de seguridad con base al protocolo y puerto
- Incluirá tecnología superior a stateful firewalling
- Creará firmas para identificar las aplicaciones desarrolladas por el INSTITUTO FONACOT
- Descifrar de sesiones SSL para identificar las aplicaciones que se transmiten dentro de túneles SSL
- Creará políticas para el manejo de aplicaciones desconocidas basadas en TCP/UDP
- Identificará aplicaciones incluso cuando no utilicen puertos estándares. (Enel caso de protocolos desconocidos se deberá asignar firmas propias)
- Descripción y control de tráfico sshv
- Descifrará aplicaciones dinámicas dentro de sesiones de proxy HTTP
- Controlará tráfico IPv4 e IPv6, (En IPv6 incluir visibilidad e inspección de amenazas en aplicaciones y control de contenido)
- Soportará IPv6 en interfaces trabajando en capa 2 y capa 3
- Realizará el control e identificación de aplicaciones conforme a los siguientes puntos:
  - Permitir, negar, calendarizar, inspeccionar políticas de uso con base en aplicaciones
  - Definición de hasta 8 clases de tráfico, con la finalidad de controlar aplicaciones cuyo consumo pueda ser excesivo como el streaming.
  - Permitir el monitoreo del uso de aplicaciones.
- Las funciones de VPN IPSec y SSL se realizarán conforme a los siguientes puntos:
  - Soportar como mínimo 25 túneles VPN IPSec con un rendimiento de al menos 100Mbps de troughput.
  - Aplicar políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles SSL.
  - Contar con SSL fall back y descifrado SSL (entrada y salida).
  - Contar con un software cliente de VPN SSL para los sistemas operativos Windows 7, Windows 8.1, Windows 10 y MAC OSX V10.10 o superior.
  - Permitir la creación de políticas para tráfico VPN SSL
  - Soportar 4 conexiones concurrentes

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

- Realizar la autenticación de VPN SSL a través de LDAP, Seguridad vía Base de Datos Propia.

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- La función de IPS Control Contra Amenazas, se efectuará de acuerdo a lo siguiente:

  Soportar protección contra malware en contenido HTML, Java script, Software Espía y Gusanos.
  - Ofrecer protección contra descargas involuntarias usando HTTP de archivos ejecutables maliciosos
  - Efectuar escaneo de virus en HTTP, SMTP y POP3
  - Ejecutar la inspección de archivos comprimidos que usan algoritmo deflate (zip, gzip, etc).
  - Soportar bloqueo de archivos por tipo.
  - Adaptar firmas Phone-home de software espia y explotación de vulnerabilidades.
  - Realizar la actualización de firmas de ataques de forma diaria, semanal y de emergencia.
  - Protección contra amenazas de Malware y Spyware
  - Rendimiento como mínimo de 500 Mbps de Troughput.
  - Incluya mecanismos de IPS basados en:
    - Análisis de patrones de estado
    - Análisis de decodificación de protocolo
    - Análisis para detección de anomalías de protocolo
    - análisis heurístico
    - IP desfragmentación
    - Reensamblado de paquetes de TCP
  - Permitir el diseño de firmas de vulnerabilidades
  - Haber pasado pruebas de los laboratorios NSS con al menos un 90% de efectividad para lo cual deberán incluir el reporte correspondiente
  - Identificación de botnet por comportamiento
  - Interceptar archivos ejecutables y realiza ejecución en un entorno Sanbox, para determinar si son archivos legítimos o malware tratando de entrar a la red
- Realizará el control de acceso y transmisión de datos conforme a lo siguiente:
  - Administrar el tráfico de aplicaciones, permitiendo la ejecución de aplicaciones autorizadas Identificar nuevas aplicaciones.
  - Crear políticas basadas en la visibilidad y control de quién está usando qué aplicaciones, a través de la integración con servicios de directorio.
  - Autenticación vía LDAP, Directorio Activo y Base de Datos locales
  - Crear políticas basadas por aplicación, categoría de aplicación, sub-categoría, tecnología y factor de riesgo.
  - Crear políticas basadas en el control por usuario, grupos de usuarios

o dirección IP.
- Crear políticas basadas en Traffic shaping por aplicación, usuario,
  fuente, destino, Túnel VPN-IPSec-SSL.
- Controlar sin instalación de cliente de software, equipos que soliciten salida a internet para que antes de iniciar la navegación, se despliegue un portal de autenticación residente en el firewall (captive portal) con soporte a autenticación por client certificate.
- Soporte autenticación Kerberos
- Protección contra ataques de negación de servicios.
- Control de host diferentes a Windows, vía autenticación basada en web

- La Generación de Reportes considerará lo siguiente:
  - Proporcionar un resumen gráfico de aplicaciones utilizadas, y amenazas encontradas diariamente.
  - Permitir el control de transferencia de datos no autorizados con herramienta para realizar patrones definidos por usuario.
  - Contar con la funcionalidad para la exportación de bitácoras (logs) de filtrado, vista de tráfico URL y amenazas
  - Permitir la administración vía web, cli, syslog, snmp2.
  - Administración basada en roles.
  - Permitir la creación de reportes personalizados.
  - Contar con herramienta para crear filtros de monitoreo de las sesiones históricas en el firewall ya sea por aplicación, IP origen y destino.
  - Capacidad para generar un reporte gráfico que permita visualizar los cambios en el uso de aplicaciones en la red con respecto a un periodo de tiempo anterior
  - Generación de reportes con mapas geográficos generados en tiempo real para la visualización de orígenes y destinos del tráfico generado.
  - Proporcionar como mínimo los siguientes reportes:
    - Utilización de ancho de banda de entrada y salida por aplicación (TOP 10)
    - No. De Sesiones por aplicación (TOP 10)
    - Comparativo semanal de aplicaciones corriendo en la red que pudieran incrementar o decrementar su utilización (top 10)
    - utilización (en bytes) por aplicación (top 10).
    - Origen y destino del tráfico por aplicación-usuario (TOP 10)
    - Eventos / Ataques por: Origen, Categoría, Amenaza, Protocolo. (TOP 10)
    - Nivel de riesgo de la red.
    - Principales aplicaciones que circulan por el Firewall (TOP 25).
    - Principales direcciones IP destino por protocolo (TOP 25).

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 19 de mayo de 2022.

aplicaciones (TOP 50).

- Incluirá una tecnología de identificación de malware moderno contando con la detección de comportamientos maliciosos, detección de tácticas de evasión y aprendizaje de maquina (machine learning).
- Incluirá la inspección de malware en día cero para documentos tipo Ejecutables, dll, Office (Word, Excel, Powerpoint) , pdf, apk, jar (Java) y Adobe Flash.
- Bidirectional Forwarding Detection (BDF)
- Identificará usuarios a través de integración con Active Directory, LDAP, eDirectory.
- Reporte de aplicaciones tipo SAAS.
- Funcionalidad de prevención de robo de credenciales detectando el momento en que los usuarios envían credenciales corporativas validas a un sitio. Este procedimiento puede realizarse de acuerdo a un grupo de usuarios de LDAP e identificación de usuarios activos en la red.

Los equipos de contención perimetral se distribuirán conforme a lasiguiente tabla:

Item	Localidad	Cantidad Solicitada	Tipo de Firewall solicitado
1	OFICINAS CENTRALES VPN MPLS	2 (HA)	Tipo 1
2	OFICINAS CENTRALES INTERNET	2 (HA)	Tipo 1
3	PLAZA DE LA REPUBLICA VPN MPLS	2 (HA)	Tipo 1
4	PLAZA DE LA REPUBLICA INTERNET	2 (HA)	Tipo 1
5	Hermosillo	1	Tipo 2
6	GUADALAJARA ABASTOS	1	Tipo 2
7	Veracruz	1	Tipo 2
8	MONTERREY	1	Tipo 2
9	INE	2	Tipo 2

2.1.13 Filtrado de contenido Web

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P 03100, Cdmx

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicada realizará las actividades necesarias para la administración, de la herramienta de filtrado WEB

Actualmente el servicio se encuentra operando en las oficinas centrales del Instituto FONACOT en un esquema de un servidor para administración y reportes junto con un Appliance modelo V5000 capacidad de 2100 licencias vigentes.

El servicio operará conforme las siguientes particularidades:

La administración y reportes de la solución estará concentrada en un servidor dedicado y con acceso Web, en el mismo servidor debe estar también el acceso a la administración del appliance que formen parte de la solución ofertada.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerará efectuar la validación de resolución de DNS´s externos einternos y en caso de fallas, dar seguimiento con el proveedor del servicio de Internet y/opersonal del área técnica del Instituto FONACOT.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado configurará la solución para permitir migrar/actualizar las políticas de uso que actualmente están en funcionamiento en el Instituto FONACOT, con el objeto de conservar y garantizar el cumplimiento de las políticas o normas de seguridadcon relación a los sitios/categorías en la navegación Web establecidas por el área técnica del Instituto FONACOT.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., configurará la solución para generar y entregar reportes de forma mensual y/o a petición del área técnica del Instituto FONACOT pudiendo ser estos resúmenes ejecutivos, reportes detallados, gráficas y/o tablas.

Filtrado de contenido Web

La solución de filtrado Web ofertada será conforme se describe a continuación:

- La administración y reportes de la solucionde filtrado Web se concentrará en un solo equipo, en el mismo también tiene que estar la administración del appliance involucrado en la solución ofertada.
- El appliance dedicado al filtrado Web no podrán ser compartido
- Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado configurará la solución para que las 24 horas del día,en conjunto con la información de la red de inteligencia del fabricante, descubrade manera oportuna y dinámica, amenazas Web, sitios web en tiempo real con alto riesgo para la organización, tecnologías y técnicas para la identificación de datos, así como detectar y bloquear por tipo y tamaño archivos embebidos y/o descargados.
- Soportará modos de operación como proxy transparente o proxy explícito.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- El modo de operación proxy transparente incluirá: Soporte para usar WCCP (Web Cache Content Protocol) y PBR (Policy Based Routing).
- El modo de operación proxy explícito incluirá lo siguiente: configuración manual de browser y/o soporte para auto configuración del proxy mediante el uso de PAC, WPAC y políticas de Active Directory. La generación de políticas de Active Directory serán responsabilidad del Instituto FONACOT
  - Considerando la perspectiva descrita en el punto anterior la solución tendrá la capacidad de identificar y administrar lo siguiente:

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

- Usuarios autorizados para acceder a aplicaciones sensibles en tiempo real.
- Datos críticos e importantes para la organización que serán protegidos contra fugas intencionales o accidentales.
- Como los usuarios están comunicando datos sensibles y como los recursos en línea son utilizados de manera más segura y productiva por la organización.
- Donde los usuarios están permitidos acceder en línea y a donde los datos sensibles pueden ser enviados.
- Aprovechar el potencial de las nuevas herramientas web sociales, de comunicación y colaboración como Facebook, LinkedIn, Twitter y otros servicios basados en la nube, evitando amenazas de malware, ataques basados en la web que eluden el software antivirus o contenido inapropiado ni fuga de información confidencial.
  - La solución de filtrado Web ofertada incluirá al menos las siguientes capacidades/funcionalidades:
- Filtrado de navegación Web basado en *Proxy*
- Personalización de las páginas de bloqueo enviadas por los dispositivos instalados para este fin dentro de las instalaciones del Instituto FONACOT.
- Capacidad de filtrar tráfico http y https
- Capacidad de sincronizar su configuración (Políticas/Permisos/Excepciones/Usuarios) con centros de datos del fabricante para que equipos de usuarios que salen de la red del Instituto FONACOT continúen protegidos.
- Contará con software cliente (Endpoint) que forcé la configuración de la navegación e impida al usuario modificar los parámetros de proxy en sus navegadores.
  - La solución de filtrado Web estará integrada con el dominio de Active Directory del Instituto FONACOT.
  - La solución de filtrado/seguridad Web tendrá la capacidad para aplicar políticas en base a:
- Usuarios
- Grupos
- Unidades Organizaciones
- Direcciones IP
- Rangos de direcciones IPs
  - La solución de filtrado/seguridad Web tendrá la capacidad de entregar reportes basados en la combinación de apartados como:
- Objetos del AD (usuarios, grupos, OUs, etc.)
- Consumo de datos (de subida, de bajada, totales)
- Día, mes, año, periodos.
- Bloqueo, permitido.

La solución propuesta considerará un esquema de filtrado por regiones y administrada centralizadamente conforme a la siguiente distribución:

Región	Servicio
Nacional	Filtrado Web

Noreste	Filtrado Web
Occidente	Filtrado Web
Sureste	Filtrado Web
Plaza de la Republica CDMX	Filtrado Web
Oficinas Centrales CDMX	Filtrado Web

Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerará que en cada una de las regiones antes mencionadas se implementará un appliance físico o virtual.

2.3.2. CABLEADO ESTRUCTURADO

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado realizará las actividades para la instalación y mantenimiento de los nodos de cableado estructurado a nivel nacional, conservando la certificación Systimax del sistema de cableado implementado en el Instituto FONACOT. Los materiales suministrados para el sistema de cableado estructurado serán totalmente nuevos, libres de todo defecto o corrosión y del mismo fabricante del cableado que actualmente se encuentra instalado en el Instituto FONACOT. En los casos que se requiera, Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerará el suministro e instalación de patch panel, jacks, faceplates, organizadores de cables, charolas de fijación, racks, gabinetes, organizadores, tuberías, canalizaciones, escalerillas y cualquier material misceláneo que se requiera para la instalación.

2.3.2.1. Instalación de nodos nuevos

El servicio consiste en instalar nodos nuevos en cualquier oficina del Instituto FONACOT a nivel nacional, de acuerdo a especificaciones, desde el patch panel hasta la placa para la conexión del equipo, se considerará instalar cableado UTP categoría 6a bajo la norma EIA/TIA 568B para el caso de apertura de nuevas oficinas. Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado realizará el etiquetado de todos los componentes del sistema de cableado tales como racks o gabinetes, cables, puertos, paneles, placas, etc.

2.3.2.2. Reubicación de nodos existentes

El servicio consiste en reubicar cualquier componente de nodos ya instalados en cualquier oficina del Instituto FONACOT a nivel nacional, de acuerdo a especificaciones, desde el patch panel hasta la placa para conexión del equipo.

2.3.2.3. Mantenimiento de nodos de red

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

El servicio consiste en realizar el mantenimiento de los nodos de red que se encuentren dañados a solicitud de la convocante, en cualquier oficina del Instituto FONACOT a nivel nacional, llevando a cabo la reposición de accesorios de acoplamiento, conectorización y montaje de los mismos.

2.3.1.1. Instalación de Fibra Óptica

El servicio consiste en instalar fibra óptica nueva tipo multimodo con al menos 2 hilos en cualquier Oficina del Instituto FONACOT. Es responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerar el suministro e instalación de cualquier componente relacionado con el tendido de fibra óptica tales como charolas, paneles, conectores, patchcord, canalización, etc. Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerará un máximo de 150m por cada cablede fibra óptica instalado.

2.3.1.2. Movimientos de infraestructura.

El servicio consiste en instalar y/o desinstalar equipo activo, gabinetes, racks, organizadores y/o patch panel en cualquier localidad del Instituto FONACOT a nivel nacional para su traslado y puesta en operación o bien para su baja del inventario. Esto puede ser requerido para lugares diferentes dentro de un área metropolitana o entidad federativa.

2.3.2. SERVICIO DE ADMINISTRACIÓN DE ENERGÍA REGULADA (UPS)

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obligará a implementar el servicio de energía regulada a fin de brindar un respaldo de energía eléctrica a los equipos de redes y comunicaciones, así como PC's en todas las localidades del Instituto FONACOT.

La solución propuesta considerará el suministro del equipamiento, la instalación y puesta a punto, actividades que serán realizadas por personal de Tecnología en Seguridad y Comunicaciones S.A. de C.V., dentrode los periodos establecidos en los niveles de servicio respectivos. Cabe aclarar que todaslas actividades se efectuarán en ventanas de servicio que no afecten la operación normal del Instituto FONACOT.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerará accesorios, material, consumibles, mano de obra, conectores, ductería, refacciones, componentes, adecuaciones y configuracionesnecesarias para la adecuada implementación y operación del sistema de administración de energía regulada, así como cualquier otro elemento para mantener la continuidad delservicio.

para la puesta a punto del servicio, Tecnología en Seguridad y Comunicaciones S.A. de C.V., realizará la instalación de cableado eléctrico desde los centros de carga hasta el sistema de administración de energía regulada (UPS)

Tecnología en Seguridad y Comunicaciones S.A. de C.V., entregará al área técnica del Instituto la memoria técnica en medioelectrónico, incluyendo al menos los siguientes aspectos:

Diagrama de conexión del sistema de administración de energía regulada,

Diagrama de conexión del sistema de tierra física y acondicionamiento eléctrico (en caso

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

de haberse requerido)

Validación del tiempo de respaldo del sistema de administración de energía regulada

Fotografías de instalación del sistema de administración de energía regulada, sistema de tierra física y acondicionamiento eléctrico.

La entrega al destino final de los equipos será de la total responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., los costos que se generen con motivo de la entrega del equipo corren por cuenta de Tecnología en Seguridad y Comunicaciones S.A. de C.V., por lo que éste asume la responsabilidad total por el aseguramiento y gastos asociados que se generen por el manejo y traslados de los activos que se suministren con motivo de este servicio.

Es responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., efectuar todas las pruebas de operación e integraciónde todos los elementos que conforman la solución ofertada, con la finalidad de asegurar la adecuada interoperabilidad y funcionalidad de dichos elementos.

Para el caso de las Oficinas Centrales sede Insurgentes del Instituto FONACOT, Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerará como parte del servicio, todos los elementos y/o componentes de enfriamiento que permitan que el servicio de energía regulada implementado en dicho sitio opere bajo las condiciones de temperatura adecuadas.

Los equipos que conformen el servicio de administración de energía regulada cumplirán con al menos las siguientes características técnicas:

Equipos de energía regulada de hasta 10 KVA:

Tecnología true on-line doble conversión
Frecuencia de entrada y de salida 50-60 Hz
Calidad de regulación de voltaje en línea y batería +/- 1%
Voltaje de salida 120 VAC
Factor de cresta en corriente 3 a 1
Temperatura de operación de 0º a 40º C
Humedad relativa de 0 a 95%.
Interruptor de bypass interno para mantenimiento y bypass automático.
Tarjeta de comunicación SNMP.
Interfase de comunicación RS232 en conector db9 y/o USB.
Base o soporte para que el equipo propuesto sea utilizado como torre o en rack.
Normas y certificaciones:

- UL 1778, CSA, FCC clase A(2),

Los equipos con capacidad mayor 16KV adicionalmente cumplirán con las siguientes características:

Será configurable para alcanzar un nivel de redundancia interna de n+1
Deberá proporcionar altos niveles de disponibilidad mediante redundancia al permitir

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

la configuración con un módulo de potencia excesa respecto de la cantidad requerida para ofrecer soporte a la carga conectada.

Deberá tener módulos de inteligencia redundantes.

Deberá proporcionar niveles altos de disponibilidad a las cargas conectadas a los UPS y ofrecerá vías redundantes de comunicación con las funciones clave de la unidad ups.

Deberá aumentar la disponibilidad y permitir la recuperación inmediata y sin inconvenientes tras fallas aisladas de módulos en configuración n+1 y/o a través del desvío (bypass)

Deberá ofrecer altos niveles de disponibilidad mediante baterías redundantes y/o baterías externas.

Contará con módulos de potencia reemplazables en caliente.

Garantizará que llegue un suministro puro e ininterrumpido a los equipos protegidos durante el recambio de módulos de potencia en configuración n+1 y/o através del desvío (bypass)

Permitirá el diseño modular.

Proporcionará velocidad de servicio, la funcionalidad de auto diagnóstico y la capacidad de reemplazar módulos en el sitio.

Calidad de Regulación de Voltaje en línea y batería +/-3% (de L-N)

Los equipos de administración de energía regulada se distribuirán conforme ala siguiente tabla, misma que podrá variar según las necesidades del Instituto.

Ubicación.	Tipo.	Cantidad
UPS Tipo 9		
Oficinas Centrales	Tipo 9 100 KVA	1
UPS Tipo 8		
Oficinas Centrales	Tipo 8 40 KVA	1
UPS Tipo 7		
Plaza de la Republica	Tipo 7 30 KVA	1
Plaza de la Republica	Tipo 7 30 KVA	1
Tlalnepantla	Tipo 7 30 KVA	1
UPS Tipo 6		
Hermosillo	Tipo 6 20 KVA	1
Monterrey	Tipo 6 20 KVA	1
Molinos	Tipo 6 20 KVA	1
Portales	Tipo 6 20 KVA	1
Celaya	Tipo 6 20 KVA	1

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de contratación: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Mérida	Tipo 6 20 KVA	1
Metro Seis	Tipo 6 20 KVA	1
Zaragoza	Tipo 6 20 KVA	1
Toluca	Tipo 6 20 KVA	1
UPS Tipo 5		
Acapulco	Tipo 5 16 KVA	1
Guadalajara	Tipo 5 16 KVA	1
Cancún	Tipo 5 16 KVA	1
Aguascalientes	Tipo 5 16 KVA	1
Chihuahua	Tipo 5 16 KVA	1
Culiacán	Tipo 5 16 KVA	1
La Paz	Tipo 5 16 KVA	1
Mazatlán	Tipo 5 16 KVA	1
Pachuca	Tipo 5 16 KVA	1
Puebla	Tipo 5 16 KVA	1
Querétaro	Tipo 5 16 KVA	1
San Luis Potosí	Tipo 5 16 KVA	1
Tampico	Tipo 5 16 KVA	1
Tijuana	Tipo 5 16 KVA	1
Tuxtla Gtz.	Tipo 5 16 KVA	1
Veracruz	Tipo 5 16 KVA	1
Villahermosa	Tipo 5 16 KVA	1
Cuernavaca	Tipo 5 16 KVA	1
Durango	Tipo 5 16 KVA	1
Torreón	Tipo 5 16 KVA	1
Campeche	Tipo 5 16 KVA	1
León	Tipo 5 16 KVA	1
Mexicali	Tipo 5 16 KVA	1
Morelia	Tipo 5 16 KVA	1

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Oaxaca	Tipo 5 16 KVA	1
GDL Federalismo	Tipo 5 16 KVA	1
Saltillo	Tipo 5 16 KVA	1
UPS Tipo 4		
Tlaxcala	Tipo 4 10 KVA	1
Colima	Tipo 4 10 KVA	1
Zacatecas	Tipo 4 10 KVA	1
Puerto Vallarta	Tipo 4 10 KVA	1
Cd Juárez	Tipo 4 10 KVA	1
Cd Obregón	Tipo 4 10 KVA	1
Celaya	Tipo 4 10 KVA	1
Tepic	Tipo 4 10 KVA	1
Congreso	Tipo 4 10 KVA	1
UPS Tipo 3		
Cd del Carmen	Tipo 3 8KVA	1
Los Mochis	Tipo 3 8KVA	1
Manzanillo	Tipo 3 8KVA	1
Monclova	Tipo 3 8KVA	1
Nogales	Tipo 3 8KVA	1
Reynosa	Tipo 3 8KVA	1
Xalapa	Tipo 3 8KVA	1
UPS Tipo 2		
Chilpancingo	Tipo 2 5KVA	1
Coatzacoalcos	Tipo 2 5KVA	1
Lázaro Cárdenas	Tipo 2 5KVA	1
Chetumal	Tipo 2 5KVA	1

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Cozumel	Tipo 2 5KVA	1
Cuautitlán	Tipo 2 5KVA	1
Ensenada	Tipo 2 5KVA	1
Fresnillo	Tipo 2 5KVA	1
Matamoros	Tipo 2 5KVA	1
Piedras negras	Tipo 2 5KVA	1
Playa del Carmen	Tipo 2 5KVA	1
Tapachula	Tipo 2 5KVA	1
Texcoco	Tipo 2 5KVA	1
Zamora	Tipo 2 5KVA	1
Monterrey 2	Tipo 2 5KVA	1
Cd Valles	Tipo 2 5KVA	1

Uruapan	Tipo 2 5KVA	1
Lerma	Tipo 2 5KVA	1
UPS Tipo 1		
Almacén mar adriático	Tipo 1 3 KVA	1
Ciudad victoria	Tipo 1 3 KVA	1
Córdoba	Tipo 1 3 KVA	1
Cuautla	Tipo 1 3 KVA	1
Ecatepec	Tipo 1 3 KVA	1
Empalme	Tipo 1 3 KVA	1
Irapuato	Tipo 1 3 KVA	1
San José del cabo	Tipo 1 3 KVA	1
San juan del rio	Tipo 1 3 KVA	1
Tehuacán	Tipo 1 3 KVA	1
Tuxtepec	Tipo 1 3 KVA	1

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Delicias	Tipo 1 3 KVA	
Cd Acuña	*Vigencia de la cotización*	*1 mes a partir de la entrega de la misma*
Guasave	Tipo 1 3 KVA	

Ciudad de México a 17 de mayo de 2022.

2.33. SOPORTE TÉCNICO.

El soporte técnico considerá las actividades para atender y solucionar los distintos requerimientos, incidentes y/o problemas relacionados con los componentes de infraestructura involucrados en la prestación de los servicios suministrados por el Tecnología en Seguridad y Comunicaciones S.A. de C.V.

Las actividades de soporte técnica serán ejecutadas por personal que cumpla con el siguiente perfil:

Estudios concluidos a nivel licenciatura de alguna de las carreras técnicas. Se presentará en la propuesta técnica copia de carta pasante, certificado, constancia, titulo y/o cédula profesional. Se presentará curriculo Vitae del personal de soporte técnico propuesto que incluya, almenos los siguientes puntos:

- Nombre(s) y apellido(s)
- Nivel de estudios
- Experiencia minima de 5 años en actividades de soporte de servicios de TIC
- Puesto de trabajo dentro de la empresa
- Proyectos en los que ha participado, con la siguiente información minima para cotejar: nombre de la empresa o institución, contacto, teléfono, correo electrónico
- Carta de al menos un diente firmada por el responsable del proyecto, avalando que dicho personal ha demostrado contar con la capacidad técnica para proporcionar servicios similares a los solicitados.

- Copia legible de identificación oficial.
- El Curriculo estará firmado por el personal propuesto.

Se acreditará que el personal propuesto es parte de la plantilla contratada por Tecnología en Seguridad y Comunicaciones S.A. de C.V., por lo tanto, se presentará el alta ante el IMSS.
Cumplirá con las siguientes certificaciones emitidas por el fabricante de la tecnología o por centro autorizado de entrenamiento del fabricante correspondiente el personal que se asigne por Tecnología en Seguridad y Comunicaciones S.A. de C.V., para cubrir este perfil cumplirá en conjunto con las acreditaciones requeridas; no es requisito que cada una de las personas cumpla con la totalidad de las acreditaciones solicitadas:

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Ciudad de México a 17 de mayo de 2022.

No.	Servicio	Certificación Requerida	Fabricante
1	Monitoreo de Infraestructura	Certificación Técnica	Fabricante de solución propuesta
2	Switching	Extreme certified specialist – switching (ECS) Extreme certified specialist-routing (ECS) Extreme certified specialist –policy (ECS) Extreme certified expert – networking (ECE)	Enterasys / Extreme
3	Archivos compartidos en red,	Certificación MCSA Windows server 2012 o superior.	Microsoft
4	Contención Perimetral	Certificación Técnica	Fabricante de solución propuesta
5	Filtrado de contenidos	AP-Web Administrator.	Forcepoint

El soporte técnico se realizará cuantas veces sea necesario en función de los requerimientos que se soliciten o presenten durante la vigencia del contrato, mismos quese podrán otorgar de manera remota o en sitio en las localidades del Instituto FONACOT
o. La naturaleza, escalamiento o criticidad del requerimiento impera o prevalece sobre la asistencia remota, a fin de que se puedan realizar las acciones de soporte directamente ensitio.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., asignará 1 persona con perfil de soporte técnico en el inmueble de oficinas centrales del Instituto FONACOT (Sede Insurgentes), para cubrir un horario de 9:00 a 18:00 hrs de lunes a viernes. Sábados guardia remota de 9:00 a 17:00 hrs. el resto del personal de Tecnología en Seguridad y Comunicaciones S.A. de C.V., operará de forma remota de forma remota.

Conforme a los niveles de servicio establecidos en este anexo técnico, es responsabilidadde Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerar la cantidad de personal que estime necesario para el desarrollode las actividades de soporte técnico a nivel nacional.

El Instituto FONACOT se reserva en todo momento el derecho para evaluar por los mediosy formas que considere pertinentes al personal asignado por Tecnología en Seguridad y Comunicaciones S.A. de C.V., para otorgar el servicio, así como solicitar su sustitución por asi considerarlo conveniente. En caso de que la solicitud de sustitución del personal se derive de una falta que afecte la imagen y/o la confidencialidad de la información del Instituto FONACOT, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obligará a cooperar con el área técnica del Instituto FONACOT para el descargo de pruebas y evidencias en las que hubiese incurrido su personal.

Al ingreso del nuevo personal presentará la ratificación respectiva, la persona que ingrese como

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

sustituto cumplirá con los mismos requisitos definidos en el perfil correspondiente, por lo que se entregará la documentación pertinente para su validación.

El soporte técnico incluye de manera general los conceptos de administración de servicios; monitoreo, switching; red inalámbrica, gestión de la seguridad, UPS; cableado estructurado; documentación; mantenimiento preventivo y mantenimiento correctivo. El personal de soporte realizará las siguientes actividades, mismas que son de manera enunciativa, más no limitativa, por lo que el área técnica del Instituto FONACOT se reserva el derecho para solicitar funciones adicionales, las cuales se vinculen con el otorgamiento del servicio requerido en este anexo técnico:

Realizar la evaluación sobre los bienes o servicios afectados.
Proponer y ejecutar soluciones temporales conocidas o nuevas a fin de permitir la continuidad en las operaciones de los usuarios, en el menor tiempo posible.
Llevar a cabo las acciones pertinentes para solucionar los requerimientos, incluyendo la administración de garantías con terceros.
Documentar toda acción realizada en la atención de los requerimientos de acuerdo a las políticas y herramientas sistematizadas para la administración de los requerimientos que defina el área técnica del Instituto FONACOT.
Proporcionar, alimentar y/o actualizar la información pertinente para disponer de las bases de datos de conocimiento y de configuraciones del Instituto FONACOT, la cual se conformará de manera progresiva durante el servicio, incrementando la capacidad resolutiva de soporte.
Elaborar reportes de capacidad, disponibilidad, usabilidad, entre otros. El área técnica del Instituto FONACOT podrá solicitar cualquier información que considere pertinente relacionada con la prestación del servicio.
Realizar la instalación, configuración y puesta a punto de la infraestructura (hardware y software) involucrada en el servicio requerido, para la continuidad de servicios de TIC.
Ejecutar los cambios de políticas, permisos y configuraciones de infraestructura involucrada en el servicio requerido.
Administrar los activos de red para permitir la conectividad de equipos de cómputo y teléfonos IP Instituciones.
Proporcionar el soporte para las conexiones tipo VPN site to site entre los equipos de seguridad proporcionados por Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado y un tercero. El suministro de los medios de comunicación(enlaces y líneas telefónicas) para acceso remoto no será responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado.

Proporcionar soporte especializado a usuarios que requieran la configuración de acceso a internet a través de la red inalámbrica del Instituto FONACOT en sus dispositivos móviles. Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerará que el personal de soporte técnico asignado para estas actividades será serespecialista en al menos en los sistemas operativos IOS, Android, Windows Phone, entre otros.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Ciudad de México a 17 de mayo de 2022.

Realizar las actividades para la instalación y configuración de los equipos de telecomunicaciones.
Elaborar y ejecutar planes de trabajo, análisis, integración, pruebas y evaluación del impacto de la misma atender un requerimiento que involucre la infraestructura considerada en el servicio, de conformidad a las políticas y procesos que defina el área técnica del Instituto FONACOT.

Supervisar el comportamiento de la infraestructura y analizar las tendencias de consumo de recursos de la infraestructura involucrada en el servicio requerido.
Efectuar y documentar las altas, bajas y cambios (ABC) de parámetros de usuarios, tales como filtros, políticas, reglas, permisos, configuraciones, entre otros dentro de la infraestructura involucrada en el servicio requerido.
Ejecutar las acciones para el respaldo y restauración de información y configuraciones de la infraestructura involucrada en el servicio requerido.
Realizar los trabajos de conexión y desconexión de componentes de cableado estructurado ya existente de acuerdo a los requerimientos del área técnica del Instituto FONACOT.
Realizar mantenimiento correctivo al cableado estructurado de acuerdo a los requerimientos del área técnica del Instituto FONACOT. Esto podrá incluir cambio de faceplates, jacks, ponchado de cable, etiquetado, escaneo, organización de cables, canalizaciones y ajustes en la fijación de rack y/o gabinetes automatizados.
Realizar la reubicación de equipo activo, componentes, charolas, barras de contactos, gabinetes, racks, organizadores y/o patch panel dentro de una misma oficina del Instituto FONACOT, esto podrá incluir, en los casos aplicables: la baja de servicios y aplicaciones, el apagado, desconexión/conexión, montaje/desmontaje, reacomodo del equipo, accesorios y dispositivos que integren cada bien.
Elaborar y/o actualizar la memoria técnica referente al cableado estructurado.
Habilitar/ Deshabilitar nodos de red en cualquier oficina del Instituto FONACOT.

Operar las herramientas y/o mecanismos de monitoreo provistos.
Realizar el monitoreo en un esquema de 7x24x365, considerando:

- Registro y seguimiento de las caídas, intermitencias y/o afectaciones de los activos involucrados en los servicios requeridos.
- Identificación y contención de actividades sospechosas confirmadas que se intenten filtrar hacia la red LAN o WAN vía local, Internet o VPN, por medio de los Firewalls involucrados en el servicio requerido.
- Definición en coordinación con el personal del área técnica del Instituto FONACOT la matriz de notificación de alertas y alarmas.

Como parte del soporte técnico, Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerará los siguientes puntos.

- Realizar los servicios encaminados a solucionar cualquier incidente o problema que impida o degrade la operación normal de los activos o servicios objeto de este anexo.
- Las partes, componentes o refacciones que se utilicen para proveer el servicio serán de la misma marca, tecnología y de características técnicas equivalentes o superiores a los originales, sin ningún costo adicional para la convocante, las cuales serán garantizadas por Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado, por un mínimo de 30 días naturales, posterior a su

instalación. La convocante se reserva el derecho de su aceptación cuando no sea posible contar con una pieza de tales características, lo cual debe acreditarse plenamente.

- En el caso de equipos ofrecidos en respaldo requieran de controladores o software específico para su funcionamiento, éstos serán entregados por Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado bajo su total responsabilidad observando las normas y leyes aplicables sobre derecho intelectual e industrial.
- Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado otorgará una garantía de hasta treinta días naturales posteriores al servicio proporcionado, aceptando su responsabilidad por las causasy efectos que se generen por omisión o vicios ocultos, entre otros.
- En caso de que la reparación de los equipos amerite la salida del domicilio, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado asume la responsabilidad total por el aseguramiento y gastos asociados que se generen por el manejo, retiro, reintegro y traslados de los bienes relacionados con el otorgamiento del servicio.
- Revisiones periódicas y planeación de capacidad para emitir recomendaciones de re-configuración.
- Intermediación de administración con Tecnología en Seguridad y Comunicaciones S.A. de C.V., de acceso WAN.
- Aislamiento de fallas relacionadas con la infraestructura involucrada en el otorgamiento del servicio.
- Efectuar altas, bajas y cambios en la configuración lógica de los equipos de seguridad involucrados en el otorgamiento del servicio requerido, previo análisis de impacto. El tiempo para realizar las modificaciones será como máximo de 24 horas desde que se levanta la solicitud.
- Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado será responsable del control, mantenimiento y actualización de la memoria técnica de los equipos de seguridad involucrados en el otorgamiento del servicio requerido. Garantizará, en todo momento, que la memoria técnica se encuentre documentada y actualizada.

El soporte técnico otorgará considerando la siguiente cobertura:
Soporte para la atención y solución de requerimientos referentes a los equipos considerados en la infraestructura suministrada por Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado: cubrirá un horario de operaciones de 7x24x365.

23.4. SERVICIOS BAJO DEMANDA

El Instituto FONACOT de conformidad con las necesidades de operación podrá requerir

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

a Tecnología en Seguridad y Comunicaciones S.A. de C.V. en caso de resultar adjudicado, servicios bajo demanda, a través de una solicitud expresa del administrador del contrato.

Los servicios que suministre Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado bajo este concepto cumplirán con las características técnicas que se describen en este anexo técnico y estas tomarán como referencia para el suministro de equipos y soluciones, considerando que en función al constante desarrollo tecnológico, los activos a entregar durante el periodo que abarca el servicio, serán provistos con características iguales o superiores, y que en ninguno de los casos serán por debajo de las características técnicas establecidas en este anexo técnico, debiéndose proveer todas las interfaces, cables de corriente, componentes, dispositivos, software operativo del hardware, drivers, etc., que permitan su adecuada operación.

Para los servicios bajo demanda, se tomarán como referencia los costos unitarios presentados en la propuesta económica de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado, independientemente de la fecha en que se solicite el servicio. El pago de este servicio se realizará mensualmente.

Para los servicios bajo demanda, Tecnología en Seguridad y Comunicaciones S.A. de C.V., considerará lo referente a instalación, puesta a punto, administración, soporte técnico, mantenimiento preventivo, garantías, licenciamiento, accesorios y cualquier otro elemento que sea necesario para el otorgamiento de los servicios.

2.4. PLAN DE RETORNO

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado desarrollará un plan de retorno, mismo que será sujeto a revisiones del área técnica del Instituto FONACOT. El plan de retorno iniciará 30 días naturales previos a la conclusión del contrato y contará al menos los siguientes puntos:

- Integración de documentación técnica:
  - Documentación que describa la configuración de componentes de hardware y software relacionado con los servicios de este anexo
  - Documentación que describa la operación de procesos, respaldos, restauraciones y monitoreo de todos los componentes de infraestructura (hardware y software).
  - Diagrama de infraestructura (hardware y software)
  - Archivos de configuración.
  - Listado de usuarios y privilegios de todos los componentes de infraestructura (hardware y software).
- Como parte del Plan de Retorno Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obliga a apoyar durante los30 días previos a la conclusión del contrato en la implementación y puesta a punto de todos los componentes de infraestructura (hardware y software) para continuidad del servicio ya sea por parte del Instituto FONACOT o de un nuevo prestador de servicio.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

2.5. POLÍTICAS

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se sujetará al marco normativo y mecanismos de control que el Instituto FONACOT defina para el seguimiento, aseguramiento de calidad y requerimientos de auditoría de los servicios, sin costo adicional para el Instituto FONACOT.

Para la administración y provisión de los servicios objeto del presente anexo técnico, Tecnología en Seguridad y Comunicaciones S.A. de C.V., se apegará a los modelos descritos en las normas ISO 20000 e ISO 27001. El área técnica del Instituto FONACOT se reserva el derecho de validar el cumplimiento de estos modelos, así como la infraestructura, documentación, procesos y prácticas involucradas con los servicios objeto del presente anexo técnico, por sí mismo o por medio de un tercero, con la frecuencia y profundidad que considere necesario, para lo cual Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obliga a dar todas las facilidades y asignar los recursos que sean necesarios. Para solventar las observaciones encontradas en las auditorías, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado entregará planes de trabajo detallados con las acciones correctivas y preventivas respectivas, el cumplimiento de estos planes de trabajo formará parte integrante de la evaluación de los servicios objeto del presente contrato. Si la auditoría pudiera afectar los niveles de servicio, la misma será planificada de común acuerdo entre el área técnica delInstituto FONACOT y Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obliga a realizar la transferencia de conocimientos sobre la operación de los servicios materia de este anexo técnico. El Instituto FONACOT se reserva la facultad para que la transferencia de conocimientos se otorgue a personal propio del área técnica del Instituto FONACOT o de terceros.

2.6. GESTIÓN DEL SERVICIO.

El Instituto FONACOT ha adoptado modelos de gestión de servicios de tecnología (ISO 20000, ITIL), administración de proyectos (PMO) y seguridad de la información (ISO27001), por lo que Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado deberá cuidar en todo momento que el modelo de gestión de los servicios esté alineado a los modelos de operación y procesos que se definan.

Será responsabilidad Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado dar seguimiento al desempeño de los procesos que se describen a continuación.

2.6.1. ESCRITORIO DE SERVICIO.

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización 1 mes a partir de la entrega de la misma

El Instituto FONACOT cuenta con un Escritorio de Servicio, por medio del cual los usuarios realizan solicitudes relacionadas con los sistemas y servicios informáticos, los cuales son registrados, clasificados y asignados a grupos resolutores para su atención, usando actualmente la herramienta Itop

Fecha de presentación de la cotización noviembre 2022.

A todo requerimiento registrado en el Escritorio de Servicio le corresponde un número de reporte. Los reportes se harán del conocimiento del personal Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado a través de la herramienta del Escritorio de Servicio utilizada por el Instituto FONACOT. Cualquier gestión que realice el personal de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado para la atención de los requerimientos, será registrada en el historial individual del reporte almacenado endicha herramienta.

El Instituto FONACOT otorgará la transferencia de herramientas que permita al personal de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado interactuar con la herramienta del escritorio de servicio.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado deberá proveer, con recursos propios, todas las herramientas de trabajo y logística que juzgue necesarias para el desempeño de su personal a fin de atender los requerimientos relacionados con la infraestructura involucrada con el otorgamiento de los servicios requeridos. Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado proveerá al menos los siguientes recursos a su personal:

- Equipo de cómputo personal, accesorios y dispositivos periféricos.
- Software base (Sistemas Operativos), aplicativos de creación y manejo de documentos, así como todas las licencias de uso respectivas para su uso. Es responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado mantener actualizadas las PC´s o Lap tops en hardware y software de acuerdo a las actualizaciones que se realicen por parte del Instituto FONACOT en su infraestructura,a fin de mantener la compatibilidad operacional.
- Software antivirus y programas para detección y eliminación de "troyanos", "spywares", "back doors" y cualquier tipo de "malware", debidamente actualizado.
- Elementos de papelería y consumibles para los equipos de cómputo (papel, libretas, tóner para impresora, etc).
- Equipos de telefonía celular, radios trunking y cualquier otro medio de comunicación que Tecnología en Seguridad y Comunicaciones S.A. de C.V., juzgue necesarios para la correcta operación de los distintos perfiles de trabajo. De manera obligada, al menos el 80% del personal de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado para otorgar el servicio requerido en este anexo técnico, contarán con dispositivos móviles.

- Servicio de mensajería, paquetería, valija, etc.
- Será responsabilidad total de Tecnología en Seguridad y Comunicaciones S.A. de C.V., los gastos de traslados, alimentación y seguridad social que se generen por motivo del personal asignado para la prestación delservicio.

Las funciones que deberá considerar Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado para interactuar con el Escritorio de Servicio del Instituto FONACOT son:

- Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado deberá en conjunto con el área técnica del Instituto FONACOT definir una matriz de escalación, la cual contenga al menos la información de los contactos (nombre, perfil, nivel de escalación, teléfono oficina, teléfono móvil) para su localización en todo momento, así como los tiempos establecidos para su escalación.Por su parte, el área técnica del Instituto FONACOT proporcionará una matriz de escalación de contactos y responsables de la administración del servicio a fin de coordinar la restauración de los servicios. Dichos niveles de escalación serán configurados en la herramienta del Instituto FONACOT.
- Registrar los avances, el tipo de fallas presentadas y la forma como se solucionaron, en la herramienta del Instituto FONACOT.

1.6.2. ADMINISTRACIÓN DE INCIDENTES

El objetivo de la administración de incidentes es restablecer lo antes posible la operación normal del servicio, minimizar el impacto negativo sobre las operaciones del negocio, así como asegurarse de que se mantiene el mejor nivel de servicio posible, la mejor calidad y disponibilidad, en función a los niveles de servicio descritos en este anexo técnico.

1.6.3. ADMINISTRACIÓN DE PROBLEMAS

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado a través del proceso de Administración de Problemas reducirá el número y la severidad de los incidentes y problemas alrededor de la infraestructura involucrada en el otorgamiento del servicio, identificando la causa que los originan (conocer el error), documentando la solución y generando las acciones necesarias (como solicitudes de cambio) para evitar que vuelvan a ocurrir.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado realizará actividades para alimentar la Base de Datos de Conocimiento (KDB – Knowledge Data Base) del Instituto FONACOT. En esta Base de Datos se almacenarán de manera estructurada las soluciones, procedimientos, resoluciones temporales (WA – Workaround), etc, y estará disponible para facilitar la atención y resolución de las eventualidades que ocurran en la infraestructura relacionada con los servicios proporcionados. El área técnica del Instituto FONACOT, proporcionara Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado el procedimiento para acceder a la Base de Datos de Conocimiento.

2.6.4. ADMINISTRACIÓN Y CAMBIOS DE LA CONFIGURACIÓN

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado llevará a cabo las actividades relacionadas con cambios sobre la infraestructura y servicios, considerando, por lo menos, lo siguiente:

- Coordinar procesos y procedimientos para todos los cambios, diferenciando los cambios estándar (cambios sin mayor impacto que puedan realizarse sin análisis de impacto previo) y los cambios de impacto (RFCh, aquéllos que por el nivel de impacto deban ser analizados previo a su implantación).
- Identificar los prerrequisitos para los cambios estándar.
- Preparar análisis de impacto, plan de trabajo para implementación (señalando las relaciones y tareas de otras áreas y/o proveedores del Instituto FONACOT, así como fechas propuestas para la ejecución), beneficios del cambio, los riesgos de no efectuarlo, a fin de presentarlo para aprobación por parte del área técnica del Instituto FONACOT y en su caso atender las recomendaciones resultantes. Como parte del plan de trabajo Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado preverá los ajustes a políticas, procedimientos, memorias técnicas, planes de transferencia de conocimientos (si fuera necesario), así como planes de retorno en caso de fallas.
- Tecnología en Seguridad y Comunicaciones S.A. de C.V., será responsable de operar, controlar y mantener el control de activos requeridos para los diferentes ambientes de servicio, conservando un control de versiones sobre los cambios realizados a la infraestructura (hardware y software) así como de sus configuraciones, mismas que se mantendrán documentadas en CMDB de la herramienta del Escritorio de Servicio del InstitutoFONACOT.

2.6.5. SERVICIOS DE COORDINACIÓN.

Para realizar la coordinación y seguimiento de las actividades referentes a los servicios requeridos en este anexo técnico, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado asignarán al menos una persona, de acuerdo con los siguientes términos:
Perfil requerido del Coordinador:

- Estudios concluidos a nivel licenciatura. Presentará en la propuesta técnica copia de la cédula profesional o título profesional que avale esta situación.
- Certificado en ITIL V3 nivel Intermediate en operation support and analysis (OSA) o service operation (SO), Se presentrará en la propuesta técnica copia y original del certificado correspondiente para cotejo. Si durante la vigencia del contrato se liberara una o más versiones de ITIL, se actualizará al personal asignado para cubrir este perfil.
- Experiencia mínima de tres años como responsable de la administración de

TESECOM

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

servicios de TIC. Se presentará en la propuesta técnica copia del currículo vitae donde se muestren los siguientes puntos:

- Nombre(s) y apellido(s)
- Nivel de estudios
- Experiencia mínima de 3 años como responsable de la administración de servicios de TIC a través del desempeño del rol de Director o Gerente de Proyecto similar al solicitado.
- Antigüedad y puesto de trabajo dentro de la empresa
- Proyectos en los que ha participado
- Carta de al menos un cliente firmada por el responsable del proyecto, avalando que dicho personal ha demostrado contar con la capacidad técnica para proporcionar servicios similares a los solicitados y desempeñado el rol de Director o Gerente de Proyecto.
- Copia legible de identificación oficial.
- El Curriculo estará firmado por el personal propuesto.

Se acreditará que el personal propuesto es parte de la plantilla contratada por el Tecnologia en Seguridad y Comunicaciones S.A. de C.V., por lo tanto, se presentará el alta ante el IMSS.

- Certificación vigente como Project Management Professional, emitida por el Project Management Institute (PMI). Se presentará en la propuesta técnica copia y original (para su cotejo) del certificado que avale esta situación.

El personal con este perfil realizará al menos las siguientes funciones, por lo que el área técnica del Instituto FONACOT se reserva el derecho para solicitar funciones adicionales, las cuales se vinculen con el otorgamiento del servicio requerido en este anexo técnico:

- Asegurar el adecuado cumplimiento en el otorgamiento del servicio requerido.
- Verificar el cumplimiento de los niveles de servicio establecidos en esta convocatoria.
- Elaborar y presentar los RFCh para su aprobación, de conformidad a las políticas y procedimientos que establezca el Instituto FONACOT.
- Establecer la comunicación entre todas y cada una de las partes involucradas en la atención de los requerimientos.
- Ser el enlace con el Instituto FONACOT para el seguimiento de los requerimientos que se soliciten durante la vigencia del contrato.
- Elaborar o gestionar procedimientos operativos, scripts para registro de requerimientos, reportes o informes, a fin de atender los requerimientos involucrados en el servicio.
- Proponer medidas y mecanismos de mejora continua para el otorgamiento de los servicios de TIC y la atención de requerimientos.
- Elaborar y/o actualizar la documentación relativa a la prestación del servicio.
- Cumplir con las políticas y procedimientos autorizados por el Instituto FONACOT.
- Participar en las reuniones de trabajo que convoque el Instituto FONACOT.
- Elaborar procesos y procedimientos operativos.

- Mantener actualizado el control de activos de la infraestructura involucrada en los servicios requeridos, considerando al menos los siguientes puntos:
  - Ubicación.
  - Tipo de Equipo.
  - Marca.
  - Descripción.
  - Números de serie.
  - Responsable.
  - Fecha en que se entrega a la Entidad.
  - Fecha de baja de las instalaciones de la Entidad.
  - Modelo.

Este personal cubrirá un horario de 9:00 a 18:00 horas de lunes a viernes de forma remota. De conformidad a las necesidades del Instituto FONACOT se podrá requerir la asistencia de este personal. Las funciones del personal con perfil de Coordinador se valuarán con base en el cumplimiento de proyectos que sean requeridos por el Instituto FONACOT, los cuales pueden recaer en las esferas de acción o responsabilidad del mismo coordinador o del personal para el soporte técnico. Para el seguimiento de estos proyectos se tomará como base la documentación referencial que avale la conclusión de los proyectos.

2.7. ASPECTOS GENERALES

La infraestructura que suministre Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado para proporcionar los servicios solicitados cumplirá con las características técnicas solicitadas.

La entrega al destino final de los equipos es de la total responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado, los costos que se generen con motivo de la entrega del equipo corren por cuenta de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado, por lo que éste asume la responsabilidad total por el aseguramientoy gastos asociados que se generen por el manejo y traslados de los activos que se suministrencon motivo de los servicios requeridos.

El licenciamiento Microsoft que se requiera para la operación de los servicios solicitados en este anexo técnico será proporcionado por el área técnica del Instituto FONACOT.

Toda documentación entregable, se apegará a los formatos, metodologías y lineamientos que definirá el área técnica del Instituto FONACOT con Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado.

1. MANUALES, CATALOGOS Y FOLLETOS

Tecnología en Seguridad y Comunicaciones S.A. de C.V. entregará en medio electrónico o

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

impreso los manuales, folletos, catálogos, aaquella información que respalde las características técnicas de los equipos para la prestación delservicio conforme a lo solicitado este Anexo Técnico.

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., 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 inglés.
- Información impresa obtenida de Internet, la cual incluya la dirección URL en idioma español o inglés

2. PATENTES, MARCAS Y DERECHOS

Con fundamento en lo dispuesto en la Ley Federal del Derecho de Autor y en virtud de la naturaleza de los servicios requeridos por el Instituto FONACOT, Tecnología en Seguridad y Comunicaciones S.A. de C.V., está de acuerdo en que al Instituto FONACOT le corresponde la propiedad de los documentos, respaldos, scripts, archivos de configuración e información que se requiera para la prestación de los servicios objetodel presente anexo.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., asume la responsabilidad total en caso de que al proporcionar los servicios materiade este anexo, infrinjan derechos de propiedad intelectual e industrial de terceros sobre patentes,marcas y derechos de autor, entre otros, por lo que el Tecnología en Seguridad y Comunicaciones S.A. de C.V., se obliga y acepta eximir al Instituto FONACOT de cualquier responsabilidad civil o penal.

3. MUESTRAS

NO APLICA

4. PRUEBAS Y DESARROLLO A EFECTUAR A LAS MUESTRAS

NO APLICA

5. LUGAR, PLAZO Y HORARIO DE LA PRESTACIÓN DEL SERVICIO

El plazo del servicio será del 01 de julio al 31 de diciembre de 2022.

El servicio se otorgará considerando las siguientes ubicaciones y coberturas:

- El horario para la prestación de los servicios para los edificios que se ubican en los edificios de Insurgentes Sur, Plaza de la Republica será de 8:00 a 21:00 horas de lunes a viernes y de 8:00 a 17:00 hrs, sábados de forma remota
- El horario para la prestación de los servicios para los edificios que se ubican en las Direcciones Regionales, Estatales, Plaza, Modúlos y/o Representaciones será de 8:00 a 20:00 horas de lunes a viernes hora local y de 8:00 a 17:00 hrs, también hora local.

Los horarios antes descritos pueden varia conforme a las necesidades del Instituto FONACOT.

Los domicilios de las ubicaciones antes descritas, se detallan en el Anexo "Domicilios"

Tecnología en Seguridad & Comunicaciones S.A. de C.V

6. PLAZO PARA LA SUSPENSION DEL SERVICIO

El plazo para la suspensión del servicio será de 10 días naturales. 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.

7. PAGO

Con fundamento en el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, los pagos del servicio se realizarán en moneda nacional dentro de los 20 días naturales posteriores a la presentación del Comprobante Fiscal Digital por Internet CFDI (factura electrónica impresa y archivo XML) y previa validación y aceptación de la misma, por parte por el Administrador del Contrato o persona autorizado por este, de la Subdirección General de Tecnología de la Información y Comunicación conforme a sus respectivas responsabilidades y recibidos los servicios a entera satisfacción del Administrador del contrato, a fin de proceder con el pago vía transferencia electrónica.

El pago de los servicios se realizará mensualmente, considerando meses calendario por lo servicios efectivamente devengados.

Las facturas electrónicas (formato CFDI, PDF y su archivo .XML), deberán cumplir con los requisitos fiscales vigentes, en moneda nacional, la cual deberá ser enviada a la dirección de correo electrónico del Administrador del contrato horacio.sanchez@fonacot.gob.mx.

8. ENTREGABLES

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado proporcionará los entregables relacionados en este apartado, para que sean revisados y autorizados por el Administrador del Contrato, por conducto de la Dirección de Infraestructura Tecnológica, o personal autorizado por este, quien en su caso notificará y solicitará formalmente a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado 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.

Los entregables, incluye los siguientes puntos, no obstante, el área técnica del Instituto FONACOT se reserva el derecho para solicitar reportes adicionales, las cuales se vinculen con el otorgamiento del servicio requerido en este anexo técnico.

8.1. ENTREGABLES INICIALES

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022

Entregable	Descripción	Periodo de entrega
Memoria Técnica	Descripción detallada la implementación y parametrización de cada uno de los servicios base de este anexo técnico.	Máximo los 30 días hábiles posteriores a la conclusión de la Implementación de todos los Servicios.
Cartas de entrega / recepción deservicios	Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado entregará documento en hoja membretada y firmada por el administrador del contrato por parte de Tecnología en Seguridad y Comunicaciones S.A. de C.V., con la descripción de la infraestructura puesta a punto decada uno de los servicios. Y fecha de su liberación	Máximo a los 5 días hábiles posteriores a la liberación de cada servicio.

8.2 ENTREGABLES MENSUALES

Durante los primeros cinco días hábiles de cada mes, Tecnología en Seguridad y Comunicaciones S.A. de C.V., entregará los reportes con la Información Soporte para el pago de la Factura correspondientes al mes vencido anterior

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Servicios	Reportes	Periodo de Entrega
La información corresponderá en cada caso al servicio que aplique, el área técnica del instituto FONACOT se reserva el derecho para solicitar reportes adicionales, los cuales se vinculen con el otorgamiento del servicio requerido en este anexo técnico	• Graficas de Disponibilidad, Capacidad de infraestructura por servicio. • Resumen ejecutivo de del estatus de los diferentes reportes registrados en la Mesa de Servicio • Inventario de infraestructura (Actualización DMDB) • Reporte Ejecutivo de las actividades relevantes realizadas durante el mes por servicio. • Reporte de respaldos realizados • Alarmas y Logs en Infraestructura instalada que presenten fallas o inconsistencias • Desempeño Servidores: CPU, Memoria, Disco Duro • Reporte ejecutivo de la capacidad de espacio de almacenamiento ocupado por los distintos servicios. • Memorias técnicas de cableado • Planes de trabajo de proyectos ejecutados • Tabla de Resumen de Pagos • Resumen de Infraestructura Solicitada bajo demanda • Reporte de Disponibilidad de Servicios Bajo Demanda •	Durante los 5 días hábiles posteriores al mes vencido

En caso de incumplimiento a cualquiera de los entregables antes señalados, se aplicarán las mismas penas convencionales a que haya lugar.

Ciudad de México a 17 de mayo de 2022.

8.3. ENTREGABLES FINALES

10.3.1.Memoria técnica

Previo a la finalización del servicio se entregará con 30 días naturales previos al término del contrato, a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obliga a entregar al área técnica delInstituto FONACOT el Plan de Retorno con al menos la siguiente información:

a. Documentación que describa la configuración de componentes de hardware y software relacionado con los servicios de este anexo
b. Documentación que describa la operación de procesos, respaldos, restauraciones y monitoreo de todos los componentes de infraestructura (hardware y software).
c. Diagrama de infraestructura (hardware y software) y archivos de configuración correspondientes.
d. Listado de usuarios y privilegios de todos los componentes de infraestructura (hardware y software).
e. Análisis de capacidad (Capacity Planning) de todos los componentes de infraestructura (hardware y software).
f. Manuales de gestión del servicio.
g. Plan de trabajo para el retiro de toda la infraestructura propiedad de a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado, considerando iniciar a partir del siguiente día natural posterior a la conclusión del contrato.
h. Proceso del borrado seguro de la infraestructura involucrada en el otorgamiento del servicio.
i. Apoyar en la implementación y puesta a punto de todos los componentes de infraestructura (hardware y software) para continuidad del servicio por parte del Instituto FONACOT o de un nuevo licitante del servicio.

9. NIVELES DE SERVICIO

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado cumplirá con los siguientes niveles de servicio siendo estos aplicables a los servicios que a continuación se detallan, se puntualiza que no se consideraran prorrogas para la entrega de algún servicio, por retrasos imputables a terceros.

9.1. INICIO DE OPERACIONES

- A partir del siguiente día natural del fallo, el Tecnología en Seguridad y Comunicaciones S.A. de C.V., deberá iniciar operacionesconsiderando los siguientes alcances:
  - Asignación de personal con perfil de Coordinador conforme a lo establecido en el punto SERVICIOS DE COORDINACIÓN.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

- Asignación de personal con perfil de soporte técnico conforme a lo establecido en el punto SOPORTE TECNICO.

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

9.2. PUESTA A PUNTO DEL SERVICIO INTEGRAL ADMINISTRADO

- Máximo a los 15 días naturales posteriores a la notificación de fallo, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado concluirá la implementación y puesta a punto de los siguientes servicios:
  - Monitoreo de infraestructura.
  - Switches de acceso.
  - Servicio de red inalámbrica en edificios Sede.
  - Servicio de red inalámbrica en localidades
  - Archivos compartidos en red
  - Filtrado de contenidos web
  - Herramienta de administración de la red.
  - Esquema de alta disponibilidad Tipo A.
  - Esquema de alta disponibilidad Tipo B.
  - Servicio de administración de energía regulada (UPS).

Es responsabilidad de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado mantener la continuidad de los servicios durante el periodo de implementación y puesta a punto de los nuevos servicios.

Los servicios no especificados en este rubro, se realizarán bajo demanda específica del administrador del contrato del Instituto FONACOT, por lo que los niveles de servicio para la puesta a punto en producción, o migración en su caso, se definirán con base en un plan de trabajo entregado por Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado, mismo que será aprobado por el área técnica del Instituto FONACOT.

9.3. CABLEADO ESTRUCTURADO

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado será responsable de atender los requerimientos de cableado estructurado, conforme a los tiempos que se indican en la siguiente tabla:

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización, 1 días a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Cableado estructurado	Tiempo de atención
-Instalación de nodos nuevos. -Reubicación de nodos existentes. -Instalación de Fibra Óptica. -Mantenimiento de nodos de red	6 horas dentro del horario de labores del Instituto FONACOT, para oficinas centrales, sede alterna y localidades metropolitanas 12 horas dentro del horario de labores del Instituto FONACOT. Para las localidades foráneas ,

Los tiempos de atención para los servicios de cableado estructurado consideran cualquier actividad necesaria para que Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado proporcioné un plan de actividades que establezca el tiempo de solución, mismo que será aceptado por el área técnica.

34. SERVICIOS BAJO DEMANDA

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado dispondrá máximo de 30 días hábiles a partir de la solicitud expresa del administrador del contrato para la puesta a punto de los servicios bajo demanda que se requieran.

35. INCIDENTES POR FALLAS

Tecnología en Seguridad y Comunicaciones S.A. de C.V será responsable de solucionar los incidentes que por cualquier causa genere la interrupción de los servicios informáticos o imposibilite la operación de algún equipo contenido en los servicios solicitados en este anexo técnico.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., dispondrá de los siguientes tiempos para la solución de incidentes:

Prioridad	Descripción	Tiempo de solución
Alta	Servicios : Contención perimetral. Monitoreo de Infraestructura. Filtrado de contenidos web Archivos compartidos en red.	4 horas.

	Equipos: Firewalls. Switches principales (CORE TIPO A Y B). Switches de acceso. Red inalámbrica. Energía regulada (UPS.)	2 horas para equipo operando en Oficinas Centrales y Plaza de la República. 4 horas para equipo operando en localidades metropolitanas dentro del horario de labores del Instituto FONACOT. 8 horas para equipo operando en las localidades foráneas dentro del horario de labores del Instituto FONACOT.
Media	Servicios: Herramientas de administración de la red	6 horas dentro del horario de labores del Instituto FONACOT.
	Equipos Energía regulada (UPS.)	4 horas para equipo operando en oficinas centrales y sede alterna, dentro del horario de labores del Instituto FONACOT 6 horas para equipo operando en localidades metropolitanas dentro del horario de labores del Instituto FONACOT. 8 horas para equipo operando en las localidades foráneas, dentro del horario de labores del Instituto FONACOT.

Los tiempos de solución consideran cualquier acción que requiera realizar Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado para restablecer la operación normal del servicio o equipo correspondiente, incluyendo el suministro de equipos de respaldo.

El tiempo de solución, comienza a contabilizarse a partir de que el personal de soporte técnico recibe la notificación a través de la herramienta del escritorio de servicio del Instituto FONACOT.

9.6 Cambios Estándar

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Prioridad	Ventana de servicio	Tiempo de solución
Alta	8:00 a 21:00 horas de lunes a viernes y de 8:00 a las 17:00 horas los sábados y domingos.	20 minutos
Media	8:00 a 21:00 horas de lunes a viernes y de 8:00 a las 17:00 horas los sábados y domingos.	60 minutos

Tiempo de solución, es el tiempo que transcurre desde que el personal de soporte técnico recibe a través de la herramienta del escritorio de servicio del Instituto FONACOT la solicitud y la solución, quede debidamente documentada en dicha herramienta.

Los cambios estándares se definirán de manera conjunta entre Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado y el personal técnico del Instituto FONACOT considerando que la prioridad se determinara por el tipo de servicio. Los acuerdos podrán ser revisados y modificados en el momento que estime pertinente el área técnica del Instituto FONACOT.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obligará a cumplir con los Acuerdos de Nivel Operacional (OLA´s)que se lleguen a definir durante la vigencia del contrato con la finalidad de asegurar la continuidad de los servicios informáticos y su otorgamiento de conformidad con los niveles de servicio establecidos. Los OLA´s se podrán celebrar entre Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado, el área técnica del Instituto FONACOT y otros proveedores de TIC que designe el Instituto FONACOT, definiendo los niveles de operación que entre ellos deben ofrecerse; se tomará como punto de partida los esquemas operativos, los procesos formalizados y las fronteras de responsabilidad que de ellos derivan. El área técnica del Instituto FONACOTse reserva el derecho de realizar modificaciones de los OLA´s, de emitir su aprobación y de solicitar su actualización en caso de que así lo considere necesario. El cumplimiento de estos acuerdos será exclusiva responsabilidad del Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado y de los otros proveedores y no eximirán de las penalizaciones y deducciones a que haya lugar.

9.7. Solicitud de Cambio (RFCh)

Ciudad de México a 17 de mayo de 2022.

Los RFCh se evaluarán con base en los tiempos establecidos en el plan de trabajo que haya sido previamente autorizado por el personal técnico del Instituto FONACOT. Su seguimiento se otorgará con base en la "Solicitud de Cambio (RFCh)" y la documentación referencial que avale la conclusión de los cambios aprobados por el área técnica del Instituto FONACOT.

10. GARANTÍA DE CUMPLIMIENTO DEL CONTRATO

Conforme a los artículos 48 fracción II y 49 Fracción II de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 103 de su Reglamento, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado garantizará mediante fianza expedida por institución mexicana autorizada legalmente para ello, el fiel y exacto cumplimiento del contrato, por un importe del 10% (diez por ciento) del monto total máximo del ejercicio fiscal correspondiente, sin considerar el Impuesto al Valor Agregado, ésta deberá expedirse a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores (Instituto FONACOT) y entregarse en la Dirección de Recursos Materiales y Servicios Generales, amás tardar dentro de los diez días naturales posteriores a la firma del contrato, la no entrega de lagarantía será motivo de recisión del contrato.

11. GARANTÍA DE RESPONSABILIDAD CIVIL

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obligará a proporcionar al administrador del contrato la póliza expedida por institución autorizada por las Leyes Mexicanas a favor del Instituto del Fondo Nacional para el Consumo de los Trabajadores, por un importe mínimo de $1,000,000.00 (Un millón de pesos 00/100 M.N.) que garantice la protección de daños y perjuicios que pudieran presentarse como resultado de las actividades propias de Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado por la ejecución de los servicios quese contraten derivados del presente contrato, la cual deberá ser entregada dentro de los 4 días hábiles siguientes a la emisión del Fallo correspondiente.

12. PENA CONVENCIONAL Y DEDUCTIVA

12.1. PENA CONVENCIONAL

En términos de lo previsto por los artículos 53 de **La Ley**, 95 y 96 de **El Reglamento**, el Instituto FONACOT, según corresponda aplicará a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado las penas convencionales por cada día natural de atraso en el incumplimiento de las siguientes obligaciones:

14.1.1. INICIO DE OPERACIONES

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Asignación de personal con perfil de Coordinador conforme a lo establecido en el punto SERVICIOS DE COORDINACION.

Asignación de personal con perfil de soporte técnico conforme a lo establecido en el punto SOPORTE TECNICO para la administración de los servicios informáticos que se encuentran en operación en el Instituto FONACOT.

Considerando que el no contar con personal con perfil de coordinación y soporte técnico afectaría el inicio de operaciones del servicio, se aplicará una pena convencional por causa imputable al LICITANTE ganador, del 1% por cada día de atraso sobre el monto total del contrato considerando el costo señalado en la propuesta económica.

14.1.2. PUESTA A PUNTO DEL SERVICIO INTEGRAL ADMINISTRADO

- Switches de acceso.
- Servicio de red inalámbrica en edificio Sede.
- Servicio de red inalámbrica en localidades.
- Esquema de alta disponibilidad Tipo A.
- Esquema de alta disponibilidad Tipo B

Por atraso imputable a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado en la puesta a punto de los servicios antes mencionados, se aplicará una pena convencional del 3% por cada día de atraso sobre el costo total mensual del servicio correspondiente, considerando los costos señalados en lapropuesta económica.

- Archivos Compartidos en Red.

- Filtrado de contenidos Web.

Por atraso imputable a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado en la puesta a punto de los servicios anteriores,se aplicará una pena convencional del 10% por cada día de atraso sobre el costo total mensual del servicio correspondiente, considerando los costos señalados en la propuestaeconómica.

- Herramienta de administración de la red.
- Servicio de administración de energía regulada (UPS).

Por atraso imputable a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado en la puesta a punto de los servicios anteriores,se aplicará una pena convencional del 5% por cada día de atraso sobre el costo total mensual del servicio correspondiente, considerando los costos señalados en la propuestaeconómica.

- Cableado estructurado
  - Por atraso imputable a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado en la entrega del plan de actividades,se aplicará una pena convencional del 3% por cada día de atraso sobre el costo totalde

la cantidad de nodos solicitados en el requerimiento.

- Por atraso imputable a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado en los tiempos establecidos en el plande actividades que haya sido previamente autorizado por el personal técnico del Instituto FONACOT, se aplicará una pena convencional del 5% por cada día de atraso sobre el costo total de la cantidad de nodos solicitados en el requerimiento.

Vigencia de la cotización: 1 mes a partir de la entrega de la misma
Ciudad de México, 16 de marzo de 2022.

- Servicio bajo demanda.

  Por atraso imputable a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado en la puesta a punto del servicio bajo demanda, se aplicará una pena convencional del 10% por cada día de atraso sobre elcosto unitario correspondiente, tomando en consideración los costos establecidos ensu propuesta económica.

- Solicitud de Cambio (RFCh).

Por atraso imputable a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado, en el cumplimiento del plan de trabajo autorizado por el personal técnico del Instituto FONACOT, se aplicará una pena convencional del 1% diario sobre el costo mensual del servicio Soporte Tecnivo, considerando el costo señalado en la propuesta económica.

14.1.3. SERCVICIO O EQUIPOS NO OTORGADOS

Cuando el servicio o el equipo no sea otorgado por causas imputables a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado, no procederá pago alguno, asimismo, se aplicará una pena convencional del 5%por cada día de atraso del costo mensual del servicio, considerando los costos en la propuesta económica por los conceptos o bienes involucrados.

El pago, quedará condicionado, proporcionalmente, al pago y/o deducción que el prestador de servicio deba efectuar por concepto de penas convencionales mediante pago en efectivo o con cheque certificado en la caja del inmueble ubicado en Avenida Insurgentes Sur No. 452 planta baja, Col Roma Sur, Delegación Cuauhtémoc, C.P. 06760, CDMX., la que emitirá el recibo correspondiente, en el entendido de que en el supuesto que sea rescindido el contrato, no procederá el cobro de dicha penalización, ni la contabilización de la misma para hacer efectiva la garantía de cumplimiento del contrato. Lo anterior, sin perjuicio del derecho de que la Convocante pueda optar entre exigir el cumplimiento del contrato o rescindirlo, de conformidad a lo establecido en el Artículo 54 de **La Ley**.

Para el pago de las penas convencionales, la Convocante informará por escrito al prestador de servicio el cálculo de la pena convencional correspondiente, indicando el número de días de atraso, así como la base para su cálculo y el monto a que se hizo acreedor.

Para efectuar este pago, el prestador de servicio 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.

La acumulación de dichas penas no excederá del importe de la garantía del cumplimiento del contrato, es decir del 10% (diez por ciento) antes de I.V.A., de conformidad con el Artículo 53 de **La Ley** y 96 de **El Reglamento**.

12.2. DEDUCTIVAS.

En los términos de lo previsto en el artículo 53 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el área técnica del Instituto FONACOT aplicará a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado las deducciones a los conceptos del servicio que en su caso presenten deficiencias.

Disponibilidad de servicios.

La siguiente tabla muestra los porcentajes de deducción que se aplicarán sobre el costo mensual de los servicios correspondientes señalados en la propuesta económica:

Calidad de Servicios Lograda (Disponibilidad)		
Limite inferior	**Limite Superior**	**Porcentaje de la mensualidad a retener como deducción**
99.7%	100%	0%
99.3%	99.6999%	5%
99.1%	99.2999%	10%
98.9%	99.0999%	15%
98.7%	98.8999%	20%
98.5%	98.6999%	25%
98.3%	98.4999%	30%
98.1%	98.2999%	35%
97.9%	98.0999%	40%
97.7%	97.8999%	45%

D= Porcentaje de disponibilidad durante el periodo.

El área técnica del Instituto FONACOT considerará de forma mensual la disponibilidad (D) de los servicios contemplando los tiempos establecidos en las coberturas limitada o amplia (TC) y Tiempos Fuera (TF) acumulados de acuerdo a la siguiente fórmula:

$$D = \frac{(TC - TF) \times 100}{TC}$$

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

Por falta de disponibilidad de un servicio que afecte u ocasione indisponibilidad o degradación de más servicios, se aplicará la deductiva correspondiente por cada uno de los servicios afectados o inaccesibles

Incidentes por fallas

La siguiente tabla muestra los porcentajes de deducción que se aplicarán sobre el costo total mensual del servicio Soporte Técnico considerando los costos señalados en la propuesta económica.

Calidad de Servicios Lograda (Cambio Estándar)		
Límite inferior	**Límite Superior**	**Porcentaje de deducción**
97%	100%	0%
94%	96.999%	10%
91%	93.999%	15%
88% o menor	90.999%	20%

El área técnica del Instituto FONACOT considerará la siguiente fórmula para obtener el porcentaje de deducción mensual relacionado con la solución de incidentes por fallas que se encuentren fuera del nivel de servicio solicitado.

$$\frac{D= (ST - SF) \times 100}{ST}$$

D= Deducción.
ST= Solicitudes totales mensuales
SF= Solicitudes totales mensuales fuera de nivel de servicio

Cambios Estándar.

La siguiente tabla muestra los porcentajes de deducción que se aplicarán sobre el costo total mensual del servicio Soporte Técnico considerando los costos señalados en la propuesta económica

Calidad de Servicios Lograda (Cambio Estándar)		
Límite inferior	**Límite Superior**	**Porcentaje de deducción**
97%	100%	0%
94%	96.999%	10%
91%	93.999%	15%
88% o menor	90.999%	20%

El área técnica del Instituto FONACOT considerará la siguiente fórmula para obtener el porcentaje de deducción mensual relacionado con las solicitudes de cambios estándar que se encuentren fuera del nivel de servicio solicitado.

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

$$D = \frac{(ST - SF) \times 100}{ST}$$

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

D= Deducción.

Ciudad de México a 17 de mayo de 2022.

ST= Solicitudes totales mensuales
SF= Solicitudes totales mensuales fuera de nivel de servicio

13. NORMAS APLICABLES

Normas de redes

UL 60950-1, CAN/CSA C22.2, No. 60950-1, FCC 47 CFR Part 15 (Class A), ICES-003 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZ CISPR-22 (Class A)

Normas para firewall

CE, CB, FCC, UL/cUL, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, CVE Compatibility, IPv6 Ready, ICSA Firewalls.

Normas UPS

CSA, FCC part 15 class A,
UL1778

Actualmente el Instituto cuenta con procesos y funciones base para la administración de servicios de TI, según el marco de mejores prácticas de ITIL (Information Technology Infrastructure Library por sus siglas en ingles), y en proceso de implementación del MGSI (Marco de Gestión de Seguridad de la Información), por lo que Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado reflejará dicha experiencia en el curriculum de su empresa en el "soporte al servicio" , "entrega del servicio" y "seguridad de la Información" fundamentado cuando menos en estos estándaresen proyectos similares. Lo anterior con objeto de facilitar la adaptación de estos y contribuircon la transferencia de conocimientos y prácticas al Instituto.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado implementará y administrará los servicios de este anexo técnicobasado en las normas del punto anterior para mantener la confidencialidad, integridad y disponibilidad de la infomación en los servicios y bloquear toda aquella actividad o flujo ajenoo perjudicial para el Instituto FONACOT como de sus empleados y colaboradores.

Para la administración y provisión de los servicios objeto del presente anexo técnico Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado adoptará los modelos descritos en las normas ISO 20000 e ISO 27001. El Instituto FONACOT se reserva el derecho de auditar el cumplimiento de estos modelos, así como la infraestructura, documentación, procesos y prácticas involucradas con los serviciosobjeto de la presente licitación, con el fundamento

que considere necesario, para lo cual a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obliga a dar todaslas facilidades y asignar los recursos que sean necesarios. Para solventar las observaciones encontradas en las auditorías, a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicada entregará planes de trabajo detalladoscon las acciones correctivas y preventivas respectivas, el cumplimiento de estos planes de trabajo formará parte integrante de la evaluación de los servicios objeto del presente contrato. Si la auditoria pudiera afectar los niveles de servicio, la misma será planificada decomún acuerdo entre el Instituto FONACOT y a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado.

14. CONFIDENCIALIDAD

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se sujetará al marco normativo y mecanismos de control que el InstitutoFONACOT defina para el seguimiento, aseguramiento de calidad y requerimientos de auditoría de los servicios, sin costo adicional para el Instituto FONACOT.

Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obliga a guardar bajo términos de confidencialidad y reserva la información de la cual pueda tomar conocimiento con relación a las operaciones, actividades o negocios del Instituto FONACOT o cualquier otra que estuviera a su alcance como resultado del otorgamiento del servicio requerido; por lo que Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obliga asimismo y a supersonal, a cumplir con las condiciones establecidas en el Anexo "Confidencialidad", mismo quese deberá incluir en la propuesta técnica debidamente firmada por el representante legal del Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado.

Toda la documentación que con motivo de la prestación de los servicios, el Instituto FONACOT entregue a Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado, así como toda la información que Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado 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 Propiedad Industrial, debiendo Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado 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.

15. ADMINISTRADOR DEL CONTRATO

De acuerdo a lo establecido en el penúltimo párrafo del artículo 84 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el Mtro. Horacio Sánchez Tinoco, Subdirector General de Tecnología de la Información y Comunicación, será el responsable de administrar y verificar el cumplimiento del contrato.

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

15.1. MODIFICACIONES QUE SE RESERVA EL ADMINISTRADOR DEL CONTRATO

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

De conformidad a las estrategias y necesidades operacionales, el administrador del contrato del Instituto FONACOT se reserva los siguientes derechos sobre los objetos considerados en el servicio requerido en el presente Anexo técnico:

Modificación de la base instalada de hardware y software:

- La modificación de base instalada se refiere a sustituir un activo considerado en el presente Anexo técnico, por algún otro bien de características similares o superiores. Lo anterior, con la finalidad de que este último sea considerado como objeto de los servicios requeridos en este anexo técnico.
- La sustitución será a petición expresa del administrador del contrato del Instituto FONACOT. No se considerará ninguna modificación en los costos unitarios en la facturación por este concepto.
- En el caso de que la modificación signifique disminución en la cantidad de equipos, se considerarán los descuentos respectivos en la factura del mes vencido, tomando como base los costos unitarios de la unidad correspondiente.
- Modificación de ubicación de equipos:
- La modificación de la ubicación se refiere al cambio de domicilio en el que se encuentre operando el equipo y que puede ser dentro de la misma ciudad o incluso cambio de ciudad dentro del territorio de la República Mexicana. No se considerará ninguna modificación en los importes en la facturación.
- Sustitución del Personal
- El administrador del contrato del Instituto FONACOT podrá solicitar su sustitución por así considerarlo conveniente en cualquier momento durante la vigencia del contrato. En caso de que la solicitud de sustitución del personal se derive de una falta que afecte la imagen y/o la confidencialidad de la información del Instituto FONACOT, Tecnología en Seguridad y Comunicaciones S.A. de C.V., en caso de resultar adjudicado se obligará a cooperar con el administrador del contrato del Instituto FONACOT para el descargo de pruebas y evidencias en las que hubiese incurrido su personal.

El administrador del contrato podrá solicitar la baja de servicios que ya no requiera el Instituto FONACOT en cualquier momento durante toda la vigencia del servicio.

Anexo "Domicilios"

No.	Región	Sucursal	Domicilio
1	Metropolitana	Oficinas Centrales	Insurgentes Sur 452, Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, Distrito Federal.

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

2	Metropolitana	Plaza de la Republica (Plaza de la Republica)	Plaza de la República No. 32, Planta Baja, Col. Tabacalera, Del. Cuauhtémoc, C.P. 06030, Distrito Federal.
3	Metropolitana	Mixcoac	Molinos esquina Santiago Rebull No. 61 Col. Mixcoac C.P. 3910 Del. Benito Juarez, Distrito Federal.
4	Metropolitana	Modulo Chilpancingo (Insurgentes)	Insurgentes Sur 452, Planta Baja, Col. Roma Sur, Del. Cuauhtémoc, C.P. 06760, Distrito Federal.
5	Metropolitana	Portales	Municipio Libre No. 83, Col. Portales, Del. Benito Juárez, C.P. 03300, México, Distrito Federal.
6	Metropolitana	Tlalnepantla	Av. Sor Juana Inés de Cruz, No. 22 Despacho 106-4, Colonia Centro de Tlalnepantla, C.P. 5400, Tlalnepantla de Baz Estado de México
7	Metropolitana	Cuautitlán Izcalli	Av. Huhuetoca s/n, SORIANA, Loc. 6, Col. Claustro de San Miguel, Cuautitlán Izcalli, Estado de México.
8	Metropolitana	Vallejo	Norte 45 No. 853-B, Col. Industrial Vallejo, Del. Gustavo A. Madero, C.P. 02300, México, Distrito Federal.
9	Metropolitana	Ecatepec	Vía Morelos No. 24, Col. Jajalpa, C.P. 55090, Ecatepec, Estado de México.
10	Metropolitana	Congreso Del Trabajo	Av. Ricardo Flores Magón No. 44, Col. Guerrero, Del. Cuauhtémoc, C.P. 06300, México, Distrito Federal.
11	Metropolitana	Zaragoza	Blvd. Puerto Aéreo No. 81, 1er piso, Col. Federal, Del. Venustiano Carranza, C.P. 15700, México, Distrito Federal.
12	Metropolitana	Chalco	Boulevard Cuauhtémoc, MZ. 53 LT. 6, Local 2, Col. Emiliano Zapata, Chalco de Covarrubias, Estado de México, C.P. 56608.
13	Metropolitana	Texcoco	Prolongación 16 de Septiembre No. 310, Loc. 30, Col. Barrio de San Pablo Centro, C.P 56116, Texcoco, Estado de México.
14	Metropolitana	Coapa	Av. Canal de Miramontes 3280, locales 27, 28, 29, 30, Coaplaza, Col. Villacoapa, Del. Tlalpan, C.P. 14390
15	Metropolitana	Plaza de la República	Plaza de la República No. 32, Planta Baja, Col. Tabacalera, Del. Cuauhtémoc, C.P. 06030, Distrito Federal.
16	Norte	Chihuahua	Calle Séptima y Allende No. 1002, Zona Centro, C.P. 31000, Chihuahua, Chihuahua.
17	Norte	Delicias	Circuito Plaza de la Republica 4 Norte Colonia Centro Entre calle Central y calle 2da. Norte C.P. 33000.
18	Norte	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.
19	Norte	Mexicali	Av. Reforma No. 692, sección primera de la Ciudad de Mexicali, Baja California Norte.
20	Norte	Tijuana	Blvd. Díaz Ordaz No.14910, Col. Las Brisas, Plaza Las Brisas, Tijuana, Baja California Norte.

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-060331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES".

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

21	Norte	Ensenada	Av. Delante fracción A y B, LL 007, Mza. 02, Col. Cardos Pacheco, C.P. 22890, Municipio de Ensenada, Baja California Norte.
22	Norte	Hermosillo	Blvd. Luis Donaldo Colosio No. 323, Col. Valle Grande, C.P. 83205, Hermosillo, Sonora.
23	Norte	Cd. Obregón	Durango No. 245 Sur, Col. Centro, C.P. 85000, Ciudad Obregón, Sonora.
24	Norte	Empalme	Plaza Reforma, Loc.5, Col. Moderna, C.P.85330, Empalme, Sonora.
25	Norte	Nogales	Av. de los Nogales No. 277, Loc. 3, 4 y 5, Plaza Coyoacán, Col. Colinas del Yaqui, C.P. 84093, Nogales, Sonora.
26	Norte	Culiacán	Gral. José Aguilar Barraza No. 1297 Poniente, Col. Centro, C.P. 80029, Culiacán, Sinaloa.
27	Norte	Mazatlán	Av. Ejército Mexicano No. 1401-A, Col. Ferrocarrilera, C.P. 82010, Mazatlán, Sinaloa.
28	Norte	Los Mochis	Av. Cuauhtémoc No. 201 Poniente, Col. Bienestar, C.P. 81280, Los Mochis, Sinaloa.
29	Norte	La Paz	Calz. Forjadores de Sudcalifornia No. 286, Col. Bellavista, C.P. 23078, La Paz, Baja California Sur.
30	Norte	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.
31	Noreste	Monterrey	Av. Manuel L. Barragán No. 325 Norte, Col. Residencial Anáhuac, Plaza Fiesta Anáhuac, C.P. 66457, San Nicolás de los Garza Monterrey, NL.
32	Noreste	Monterrey II	Av. Ruiz Cortines y General Bonifacio Salinas 600, Col. León XIII, C.P. 67120 Guadalupe N.L. Sucursal Soriana Lindavista.
33	Noreste	Nuevo Laredo	Calle Héroe de Nacataz y Reynosa s/n, anexo al Centro Cívico, Zona Centro, CP 88000, Nuevo Laredo, Tamaulipas.
34	Noreste	San Luis Potosí	Independencia No. 1630, Col. Barrio San Miguelito, C.P. 78339, San Luis Potosí, San Luis Potosí.
35	Noreste	Zacatecas	Blvd. José López Portillo No. 303, edificio STPS, Col. Dependencias Federales, C.P. 98618, Zacatecas, Zacatecas.
36	Noreste	Fresnillo	Paseo del Mineral No. 1018, Col. Luis Donaldo Colosio, C.P. 99000, Fresnillo, Zacatecas.
37	Noreste	Durango	Aquiles Serdán No. 954, planta alta, Zona Centro, C.P. 34000, Durango, Durango.
38	Noreste	Saltillo	Blvd. Isidro López Zertuche No. 2567-A, Col. Universidad, C.P. 25260, Saltillo, Coahuila.
39	Noreste	Ciudad Acuña	Libramiento Emilio Mendoza Cisneros No. 1315, centro comercial MERCO, Col. Benjamín Canales, C.P. 26236, Cd. Acuña, Coahuila.
40	Noreste	Monclova	Calle de la Fuente No. 221, Loc. 4 y 5, Plaza Blanca, Col. Telefonistas, C.P. 25700, Monclova, Coahuila.

TECNOLOGÍA EN SEGURIDAD Y COMUNICACIONES S.A. DE C.V.
RFC: TSC-050331-163
Domicilio Fiscal: Patricio Sanz No. 526, Col. Del Valle,
Alcaldía Benito Juárez, C.P. 03100, Cdmx.

TESECOM

ASUNTO: CONTRATACIÓN DEL SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD, GESTIÓN Y MONITOREO DE LAS TELECOMUNICACIONES.

Vigencia de la cotización: 1 mes a partir de la entrega de la misma

Ciudad de México a 17 de mayo de 2022.

41	Noreste	Piedras Negras	Blvd. Eliseo Mendoza Berrueto s/n, Plaza Comercial, Loc. 5, Col. San Felipe Norte, C.P. 26070, Piedras Negras, Coahuila.
42	Noreste	Torreón	Av. Morelos No. 138 Poniente, Col. Centro, C.P. 27000, Torreón, Coahuila.
43	Noreste	Gómez Palacio	Av. Hidalgo No. 113 Sur, Loc. 4, Col. Centro, Gómez Palacio, Durango.
44	Noreste	Tampico	Av. Hidalgo No. 2401, Col. Reforma, C.P. 89140, Tampico, Tamaulipas.
45	Noreste	Reynosa	Aldama No. 1100, Loc. 26, Centro Comercial Río Grande, Col. Centro, C.P. 88500, Reynosa, Tamaulipas.
46	Noreste	Ciudad Victoria	Matamoros No. 237, oficinas de la STPS, Col. Centro, C.P. 87000, Ciudad Victoria, Tamaulipas.
47	Noreste	Matamoros	Ave. Prolongación González No. 2035 Col. Parque Industrial, Plaza Comercial Soriana Laguneta, C.P. 87479, Matamoros, Tamaulipas.
48	Sureste	Mérida	Paseo Montejo No. 492-A por la 43, Col. Centro, C.P. 97000, Mérida, Yucatán.
49	Sureste	Campeche	Av. 16 de Septiembre s/n, Palacio Federal, Col. Centro, C.P. 24000, Campeche, Campeche.
50	Sureste	Cancún	Av. Tulum, Retorno 1, Lote 3, Manzana 1, Súper manzana 22, Col. Centro, C.P. 77500, Benito Juárez, Quintana Roo.
51	Sureste	Chetumal	Av. Othón Pompeyo Blanco No. 204, 1er piso, Col. Centro, C.P. 77000, Chetumal, Quintana Roo.
52	Sureste	Cozumel	Plaza del Sol, Mercado de Artesanía, Local Planta Alta 8 Andador 5ta. Avenida Sur No. 1 Col. Centro C.P. 77600.
53	Sureste	Playa Del Carmen	Av. Benito Juárez, Lt. 3, Loc. 12, Plaza Papagayos, Col. Centro, C.P. 77710, Playa del Carmen, Quintana Roo.
54	Sureste	Tuxtla Gutiérrez	3a Norte Poniente No. 1395, entre la 12 y 13 Poniente Norte, Col. Moctezuma, C.P. 29030, Tuxtla Gutiérrez, Chiapas.
55	Sureste	Tapachula	4a calle Ote. No. 6, Col. Centro, C.P. 30700, Tapachula, Chiapas.

79	Centro	Pachuca	Carr. Pachuca- Tulancingo No. 1000, Loc. D9 al D12, Plaza Universidad, Col. Abundio Martínez, C.P 42184, Mineral de la Reforma, Hidalgo.
80	Centro	Tizayuca	Carretera México- Pachuca Km. 50, oficina de CANACINTRA Tizayuca, Zona Industrial Tizayuca, C.P. 43800, Tizayuca, Hidalgo.
81	Centro	Cuernavaca	Plan de Ayala No. 1200, Col. Chapultepec, C.P. 62450, Cuernavaca, Morelos.
82	Centro	Cuautla	Galeana No. 33, Loc. 101, planta alta, Col. Centro, C.P. 62740, Cuautla, Morelos.
83	Centro	Acapulco	Av. Costera Miguel Alemán No. 1803, Frac. Magallanes, C.P. 39690, Acapulco, Guerrero.
84	Centro	Chilpancingo	Priv. de Jacarandas S/N, P.B., puerta 4 STPS, Col. Burócratas, C.P. 39090, Chilpancingo, Guerrero.
85	Centro	Puebla	Calle 9 Norte No. 208, Col. Centro, C.P. 72000, Puebla, Puebla.
86	Centro	Tlaxcala	Av. Ocotlán No. 15, Col. Ocotlán, C.P. 90100, Tlaxcala, Tlaxcala.
87	Centro	Tezuitlan	El Encanto, entrada al Hospital General Sección 3ra. No. 20, C.P. 73954, Chignautla, Puebla.
88	Centro	Tehuacán	Calle 1 Norte No. 618, Loc. 8, 9 y 10, Plaza Montecarlo, Col. Francisco Sarabia, C.P. 75730, Tehuacán, Puebla.
89	Centro	Oaxaca	Carbonera No. 902, Esquina González Ortega, Col. Barrio Trinidad de las Huertas, C.P. 68120, Oaxaca, Oaxaca.
90	Centro	Salina Cruz	Av. Manuel Ávila Camacho No. 50, Palacio Federal, Salina Cruz, Oaxaca.
91	Centro	Tuxtepec	Av. 20 de Noviembre s/n, Col. La Piragua, C.P. 68300, Tuxtepec, Oaxaca.
92	Centro	Toluca	Ignacio Allende Sur No. 116, Col. Centro, C.P. 50000, Toluca, Estado de México.
93	Centro de Datos Alterno	Santa Fe	Prolongacion Paseo de la Reforma No.5396, Cuajimalpa, C.P. 05000, Ciudad de Mexico
94	Centro de Datos Principal	Querétaro	Privada Princesa No. 4, Parque Industrial El Marques, C.P. 76246, Km 195.5, Autopista Mexico-Queretaro

ATENTAMENTE.

Ing. Gerardo Diaz Sierra.
Representante Legal.
Tecnología en Seguridad y Comunicaciones S.A. de C.V.

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

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

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

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

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

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

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

II. Aprobación del Orden del Día

I. LISTA DE ASISTENCIA Y VERIFICACIÓN DEL QUÓRUM LEGAL.

II. LECTURA Y APROBACIÓN DEL ORDEN DEL DÍA.

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

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

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

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

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

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

VI. ASUNTOS GENERALES.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Fundamentación

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

Motivación

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

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

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

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

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

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

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

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

Fundamentación

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

Motivación

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

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

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

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

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

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

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

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

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

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

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

VI. Asuntos Generales

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

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

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

Erick Morgado Rodríguez
Abogado General
Presidente del Comité de Transparencia

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

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