CONTRATO CERRADO PARA LA PRESTACIÓN DE SERVICIOS DE "SOLUCIÓN DE INFRAESTRUCTURA DE RED (LAN, WIFI) SEGURIDAD PERIMETRAL Y SERVIDORES , QUE CELEBRAN, POR UNA PARTE, EL EJECUTIVO FEDERAL POR CONDUCTO DE LA SECRETARÍA DE TURISMO , REPRESENTADA POR LUIS FELIPE CANGAS HERNÁNDEZ , EN SU CARÁCTER DE DIRECTOR GENERAL DE ADMINISTRACIÓN , EN ADELANTE "LA DEPENDENCIA" Y, POR LA OTRA, SOLUCIONES INTEGRALES SAYNET SA DE CV ,EN LO SUCESIVO "EL PROVEEDOR" REPRESENTADA POR LA LIC. ELIZABETH SALDAÑA ROBLES, 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

1. **"LA DEPENDENCIA"** declara que:

1.1. Es una "LA DEPENDENCIA" de la Administración Pública Federal, de conformidad con artículos 1, 2 fracción I, 26 y 42 de la Ley Orgánica de la Administración Pública Federal, 4 de la Ley General de Turismo y demás disposiciones aplicables.

1.2. Conforme a lo dispuesto por los artículos 8, fracción VIII y 29 del Reglamento Interior de la Secretaría de Turismo, LUIS FELIPE CANGAS HERNÁNDEZ , en su cargo de DIRECTOR GENERAL DE ADMINISTRACIÓN , con R.F.C [redacted] es un servidor público adscrito a la misma que cuenta con facultades legales para celebrar el presente contrato, quien podrá ser sustituido en cualquier momento en su cargo o funciones, sin que por ello, sea necesario celebrar un convenio modificatorio.

1.3. De conformidad con en el Manual de Organización Específico de la Dirección General de Tecnologías de la Información y Comunicación de la Secretaría de Turismo en el Objetivo y Funciones por Área de la Dirección de Control y Soporte Técnico, suscribe el presente instrumento el ING. ADRIÁN BRINGAS REYES , en su carácter de DIRECTOR DE CONTROL Y SOPORTE TÉCNICO , con R.F.C. [redacted] , está facultado para administrar el cumplimiento de las obligaciones que deriven del objeto del presente contrato, quien podrá ser sustituido en cualquier momento, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, informando a "EL PROVEEDOR" para los efectos del presente contrato.

1.4. De conformidad con los artículos 8, fracción VIII, y 30 del Reglamento Interior de **"LA DEPENDENCIA"**, así como el Manual de Organización Específico de la Dirección General de Tecnologías de la Información y Comunicación de la Secretaría de Turismo en el Objetivo y Funciones por Área de la citada Dirección General, suscribe el presente instrumento el MTRO. MIGUEL ÁNGEL CORTÉS TORRES , en su cargo de DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN , R.F.C. [redacted] , facultado para facultado para suscribir los documentos, convenios y demás instrumentos jurídicos..

1.5. La adjudicación del presente contrato se realizó mediante el procedimiento de LICITACIÓN PÚBLICA y medio ELECTRÓNICO de carácter NACIONAL , al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 3, ARTÍCULO 26 FRACCIÓN I , 26 Bis fracción II, 27, 28 fracción I, y 29, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"LAASSP"**, y 39 y 51 de su Reglamento.

1.6. "LA DEPENDENCIA" cuenta con suficiencia presupuestaria otorgada mediante SI-51 con folio de autorización 00013 de fecha 21 de diciembre de 2022, emitido por la Dirección General de Tecnologías de la Información y Comunicación.

1.7. Para efectos fiscales las Autoridades Hacendarias le han asignado el Registro Federal de Contribuyentes N° STU750101H22

1.8. Tiene establecido su domicilio en Avenida Presidente Masarik, número 172, Colonia Bosques de Chapultepec, Alcaldía Miguel Hidalgo, Código Postal 11580, Ciudad de México, mismo que señala para los fines y efectos legales del presente contrato.

2. **"EL PROVEEDOR"** declara que:

2.1. Es una persona MORAL legalmente constituida mediante Escritura Pública número 18,204, de fecha 17 de agosto de 2004, otorgada ante la fe del licenciado Guillermo Eduardo Velázquez Quintana, Titular de la Notaria Pública número 21 del Estado de México, e inscrita en la Dirección General del Registro Público de Comercio de la Ciudad de México, bajo el folio mercantil número 322,539, con fecha 20 de septiembre de 2004., denominada SOLUCIONES INTEGRALES SAYNET SA DE CV , **cuyo objeto social es:** 3) Servicios de desarrollo, producción, mantenimiento, modificación, actualización y adecuación de sistemas de información, programas y aplicaciones de cómputo e informática;4) Servicios de informática y consultoría para diseñar y producir sistemas de información, programas y aplicación de cómputo e informática en general;6) Análisis, diseño, programación, desarrollo e integración de sistemas de cómputo orientados a la automatización de negocios, administración, adecuación, mantenimiento, implementación, consultoría, capacitación y soporte técnico en sistemas de cómputo y bases de datos y todo lo relacionado a la tecnología de información, diseño, instalación y mantenimiento de redes de tecnología de información, comercialización, importación y exportación de programas, sistemas, equipo y accesorios de cómputo, contratación y celebración de todo tipo de contratos relacionados a la tecnología de la información, arrendamiento y subarrendamiento de equipos y accesorios de cómputo;7) Contratar activamente o pasivamente, toda clase de servicios, celebrar contratos, convenios, así como adquirir por cualquiera las patentes, marcas industriales, nombres comerciales, opciones preferencia, derechos de propiedad literaria, industrial, artística o concesiones de alguna autoridad.Mediante escritura número 42,862 de fecha 27 de agosto de 2010, ante la fe del licenciado Luis Gerardo Mendoza Powell, Titular de la Notaria número 106 de la Ciudad de Atizapán de Zaragoza, Estado de México, hizo constar la protocolización del Acta de Asamblea General Extraordinaria de accionistas con el objeto de 3.- Donación de acciones, 4.- Renuncia del cargo de admisnistrador y de socios, 5.-Aumento de Capital, y 6.- La designación del Delegado especial, la cual fue inscrita en el Registro Público de la Propiedad y de Comercio, bajo folio mercantil número 322,539* el 11 de abril de 2011.Mediante escritura número 42,863 de fecha 27 de agosto de 2010, ante la fe del licenciado Luis Gerardo Mendoza Powell, Titular de la Notaria número 106 de la Ciudad de Atizapán de Zaragoza, Estado de México, hizo constar la protocolización del Acta de Asamblea General Extraordinaria de accionistas con el objeto de 3.- Cesión de Acciones, 4.- Renuncia y admisión de socios, 5.—Renuncia y nombramiento de Administrador Único, y 6.- La designación del Delegado especial, la cual fue inscrita en el Registro Público de la Propiedad y de Comercio, bajo folio mercantil número 322,539* el 11 de abril de 2011.Con escritura pública número 52,147 de fecha 08 de abril de 2014, ante la fe del licenciado Luis Gerardo Mendoza Powell, Titular de la Notaria número 106 de la Ciudad de Atizapán de Zaragoza, Estado de México, hizo constar la protocolización del Acta de Asamblea General Extraordinaria de accionistas para 3) Donación de acciones, 4) Renuncia e ingreso de socios, y 5) Designación del Delegado Especial. Con escritura pública número 59,188 de fecha 26 de diciembre de 2016, ante la fe del licenciado Luis Gerardo Mendoza Powell, Titular de la Notaria número 106 de la Ciudad de Atizapán de Zaragoza, Estado de México, hizo constar la protocolización del Acta de Asamblea General Extraordinaria de accionistas para 3) La venta, renuncia y admisión de nuevo socio y 4) Designación del Delegado Especial. Mediante escrito de fecha 06 de julio de 2017 el Titular de la notaria Número 106 de la Ciudad de Atizapán de Zaragoza, Estado de México, el Lic. Luis Gerardo Mendoza Powell, hace constar que esta protocolización del acta de asamblea general extraordinaria que contiene la venta y donación de acciones no requiere su inscripción en el Registro Público de la Propiedad y de Comercio. Asimismo escritura pública número 62,667 de fecha 04 de julio de 2018, ante la fe del licenciado Luis Gerardo Mendoza Powell, Titular de la Notaria número 106 de la Ciudad de Atizapán de Zaragoza, Estado de México, hizo constar la protocolización del Acta de Asamblea General Extraordinaria de accionistas para 3) La venta y donación de acciones, renuncia y admisión de nuevo socio y 4) La designación del Delegado Especial de la asamblea. Con escritura pública número 62,836 de fecha 01 de junio de 2020, ante la fe del licenciado Luis Gerardo Mendoza Powell, Titular de la Notaria número 106 de la Ciudad de Atizapán de Zaragoza, Estado de México, hizo constar la protocolización del acta de asamblea extraordinaria para la 3.- Aumento de capital variable de la sociedad y donación de acciones y 4.- Designación del Delegado especial de la asamblea.Con escritura pública número 69,850 de fecha 25 de agosto de 2021, ante la fe del licenciado Luis Gerardo Mendoza Powell, Titular de la Notaria número 106 de la Ciudad de Atizapán de Zaragoza, Estado de México, hizo constar la protocolización del acta de asamblea extraordinaria para la 3.- Propuesta para modificar el objeto social en los que respecta al numeral 6, 7 y 10 del Artículo Segundo de los Estatutos y 4.- Designación del

Delegado especial de la asamblea. La cual fue inscrita en el Registro Público de la Propiedad y de Comercio del entonces Distrito Federal, hoy Ciudad de México, bajo el folio mercantil número 322,539-1 de fecha 14 de septiembre de 2021

2.2. La Lic. Elizabeth Saldaña Robles, en su carácter de **Apoderada Legal,** cuenta con facultades suficientes para suscribir el presente contrato y obligar a su representada, como lo acredita con mediante escritura pública número 58,016 de fecha 24 de agosto de 2016, ante la fe del licenciado Luis Gerardo Mendoza Powell, Titular de la Notaria número 106 de la Ciudad de Atizapán de Zaragoza, Estado de México, inscrita en el Registro Público de la Propiedad y de Comercio bajo el folio mercantil electrónico número 322,539-1 de fecha 17 de noviembre de 2020, instrumento que bajo protesta de decir verdad manifiesta no le ha sido limitado ni revocado en forma alguna.

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

2.4. Cuenta con su Registro Federal de Contribuyentes SIS040817I1A

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

2.6. Señala como su domicilio para todos los efectos legales el ubicado en DRAMATURGOS 47, FRACCIONAMIENTO CIUDAD SATÉLITE, NAUCALPAN DE JUÁREZ, MÉXICO, C.P. 53100

3. **De "LAS PARTES":**

3.1. Que es su voluntad celebrar el presente contrato y sujetarse a sus términos y condiciones, para lo cual se reconocen las facultades y capacidades, 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 PROVEEDOR" acepta y se obliga a proporcionar a "LA DEPENDENCIA" la prestación del servicio de "SOLUCIÓN DE INFRAESTRUCTURA DE RED (LAN, WIFI) SEGURIDAD PERIMETRAL Y SERVIDORES , en los términos y condiciones establecidos en este contrato y sus anexos **I) ANEXO UNO (Anexo Técnico), II) Propuesta Técnica y III) Propuesta Económica,** que forman parte integrante del mismo.

SEGUNDA. MONTO DEL CONTRATO.

"LA DEPENDENCIA" pagará a "EL PROVEEDOR" como contraprestación por los servicios objeto de este contrato, la cantidad de $12,266,818.00 (DOCE MILLONES DOSCIENTOS SESENTA Y SEIS MIL OCHOCIENTOS DIECIOCHO PESOS 00/100 M.N.) más impuestos que asciende a la cantidad de $1,962,690.88 (UN MILLÓN NOVECIENTOS SESENTA Y DOS MIL SEISCIENTOS NOVENTA PESOS 88/100 M.N.),que hace un monto total de $14,229,508.88 (CATORCE MILLONES DOSCIENTOS VEINTINUEVE MIL QUINIENTOS OCHO PESOS 88/100 M.N.)

Los precios unitarios de conformidad con la II) PROPUESTA ECONÓMICA del presente contrato, expresados en moneda nacional es:

Clave control interno	Clave CUCoP	Descripción	Unidad de medida	Cantidad	Precio unitario	Precio total antes de imp.	Precio con impuestos
CONT-025-2023	SERVICIOS A CENTROS DE DATOS (HOSPEDAJE, ELECTRICIDAD, VIDEO VIGILANCIA, MONITOREO, AIRE ACONDICIONADO, SERVIDORES Y OTROS)	"SOLUCIÓN DE INFRAESTRUCTURA DE RED (LAN, WIFI) SEGURIDAD PERIMETRAL Y SERVIDORES"	S - SERVICIO	1	$12,266,818.00	$12,266,818.00	$14,229,508.88
						SUBTOTAL	$12,266,818.00
						IMPUESTOS	$1,962,690.88
						TOTAL	$14,229,508.88

El precio unitario es considerado fijo y en moneda nacional PESO MEXICANO hasta que concluya la relación contractual que se formaliza, incluyendo todos los conceptos y costos involucrados en la prestación del servicio de "SOLUCIÓN DE INFRAESTRUCTURA DE RED (LAN, WIFI) SEGURIDAD PERIMETRAL Y SERVIDORES , por lo que "EL PROVEEDOR" no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

TERCERA. ANTICIPO.

Para el presente contrato "LA DEPENDENCIA" no otorgará anticipo a "EL PROVEEDOR"

CUARTA. FORMA Y LUGAR DE PAGO.

"LA DEPENDENCIA" efectuará el pago a través de transferencia electrónica en pesos de los Estados Unidos Mexicanos, a mes vencido a mes vencido durante la vigencia del contrato la cantidad señalada en la cláusula segunda de este instrumento jurídico en caso de que la prestación del servicio no sea por el mes completo que se trate, únicamente se pagará los días que efectivamente se recibió el servicio a satisfacción para estos casos los meses se entenderán siempre de 30 días, conforme a los servicios efectivamente prestados y a entera satisfacción del administrador del contrato y de acuerdo con lo establecido en el "ANEXO UNO (Anexo ténico)" que forma parte integrante de este contrato.

El pago se realizará en un plazo máximo de 20 (veinte) días naturales siguientes, contados a partir de la fecha en que sea entregado y aceptado el Comprobante Fiscal Digital por Internet (CFDI) o factura electrónica a "LA DEPENDENCIA" , con la aprobación (firma) del Administrador del presente contrato, mencionado en la Declaración I.3; a través del Sistema Integral de Administración Financiera Federal (SIAFF).

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

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

El tiempo que "EL PROVEEDOR" utilice para la corrección del CFDI y/o documentación soporte entregada, no se computará para efectos de pago, de acuerdo con lo establecido en el artículo 51 de la **"LAASSP"**.

El CFDI o factura electrónica deberá ser presentada **por correo electrónico a** macortest@sectur.gob.mx, abringasr@sectur.gob.mx **o al siguiente domicilio:**

A NOMBRE DE: SECRETARÍA DE TURISMO

DOMICILIO FISCAL: AV. PRESIDENTE MASARIK 172, BOSQUES DE CHAPULTEPEC, MIGUEL HIDALGO, CIUDAD DE MÉXICO, CP. 11580.

R.F.C. STU750101H22 .

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

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

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

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

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

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

QUINTA. LUGAR, PLAZOS Y CONDICIONES DE LOS SERVICIOS.

La prestación de los servicios, se realizará conforme a los plazos, condiciones y entregables establecidos por "LA DEPENDENCIA" en el I) ANEXO UNO (Anexo Técnico).

Los servicios serán prestados en los domicilios señalados en el I) ANEXO UNO (Anexo Técnico) y fechas establecidas en el mismo;

En los casos que, derivado de la verificación se detecten defectos o discrepancias en la prestación del servicio o incumplimiento en las especificaciones técnicas, "EL PROVEEDOR" contará con un plazo dedos días hábiles para la sustitución o corrección, contados a partir del momento de la notificación por correo electrónico y/o escrito, sin costo adicional para "LA DEPENDENCIA"

SEXTA. VIGENCIA.

"LAS PARTES" convienen en que la vigencia del presente contrato será del 16/03/2023 al 31/12/2023

SÉPTIMA. MODIFICACIONES DEL CONTRATO.

"LAS PARTES" están de acuerdo que la "LA DEPENDENCIA" por razones fundadas y explícitas podrá ampliar el monto o la cantidad de los servicios, de conformidad con el artículo 52 de la "LAASSP", siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) de los establecidos originalmente, el precio unitario sea igual al originalmente pactado y el contrato esté vigente. La modificación se formalizará mediante la celebración de un Convenio Modificatorio.

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

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

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

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

"LA DEPENDENCIA" se abstendrá de hacer modificaciones que se refieran a precios, anticipos, pagos progresivos, especificaciones y, en general, cualquier cambio que implique otorgar condiciones más ventajosas a un proveedor comparadas con las establecidas originalmente.

OCTAVA. GARANTÍA DE LOS SERVICIOS.

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

NOVENA. GARANTÍA(S)

A) CUMPLIMIENTO DEL CONTRATO.

Conforme a los artículos 48, fracción II, 49, fracción I, de la **"LAASSP"**; 85, fracción III, 103 de su Reglamento; y 166 de la Ley de Instituciones de Seguros y de Fianzas, "EL PROVEEDOR" se obliga a constituir una garantía la cual podrá ser **divisible**, la cual sólo se hará efectiva en la proporción correspondiente al incumplimiento de la obligación principal , mediante fianza expedida por compañía afianzadora mexicana autorizada por la Comisión Nacional de Seguros y de Fianzas, a favor de la TESORERÍA DE LA FEDERACIÓN , por un importe equivalente al 10.0% del monto total del contrato, sin incluir impuestos. Dicha fianza deberá ser entregada a "LA DEPENDENCIA" , a más tardar dentro de los 10 (diez) días naturales posteriores a la firma del presente contrato.

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

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

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

En caso de incremento al monto del presente instrumento jurídico o modificación al plazo, "EL PROVEEDOR" se obliga a entregar a "LA DEPENDENCIA" dentro de los 10 (diez días) naturales siguientes a la formalización del mismo, de conformidad con el último párrafo del artículo 91, del Reglamento de la **"LAASSP"**, los documentos modificatorios o endosos correspondientes, debiendo contener en el documento la estipulación de que se otorga de manera conjunta, solidaria e inseparable de la garantía otorgada inicialmente.

Cuando la contratación abarque más de un ejercicio fiscal, la garantía de cumplimiento del contrato podrá ser por el porcentaje que corresponda del monto total por erogar en el ejercicio fiscal de que se trate, y deberá ser renovada por "EL PROVEEDOR" cada ejercicio fiscal por el monto que se ejercerá en el mismo, la cual deberá presentarse a "LA DEPENDENCIA" a más tardar dentro de los primeros diez días naturales del ejercicio fiscal que corresponda.

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

DÉCIMA. OBLIGACIONES DE "EL PROVEEDOR"

a) Prestar los servicios en las fechas o plazos y lugares establecidos conforme a lo pactado en el presente contrato y anexos respectivos.

b) Cumplir con las especificaciones técnicas y de calidad y demás condiciones establecidas en el presente contrato y sus respectivos anexos.

c) Asumir la responsabilidad de cualquier daño que llegue a ocasionar a "LA DEPENDENCIA" o a terceros con motivo de la ejecución y cumplimiento del presente contrato.

d) Proporcionar la información que le sea requerida por la Secretaría de la Función Pública y el Órgano Interno de Control, de conformidad con el artículo 107 del Reglamento de la **"LAASSP". DÉCIMA PRIMERA. OBLIGACIONES DE "LA DEPENDENCIA"**

a) Otorgar todas las facilidades necesarias, a efecto de que "EL PROVEEDOR" lleve a cabo en los términos convenidos en la prestación de los servicios objeto del contrato.

b) Realizar el pago correspondiente en tiempo y forma.

c) Extender a "EL PROVEEDOR" , por conducto del 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.

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

"LA DEPENDENCIA" designa como Administrador del presente contrato a ADRIÁN BRINGAS REYES , **con RFC** [redacted] , en su carácter de DIRECTOR DE CONTROL Y SOPORTE TÉCNICO quien dará seguimiento y verificará el cumplimiento de los derechos y obligaciones establecidos en este instrumento.

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

Asimismo, **"LA DEPENDENCIA"** sólo aceptará la prestación del servicio 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.

"LA DEPENDENCIA" a través del administrador del contrato, rechazará los servicios, que no cumplan las especificaciones establecidas en este contrato y en sus Anexos, obligándose "EL PROVEEDOR" en este supuesto a entregarlo nuevamente bajo su responsabilidad y sin costo adicional para "LA DEPENDENCIA" , sin perjuicio de la aplicación de las penas convencionales o deducciones al cobro correspondientes.

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

DÉCIMA TERCERA. DEDUCCIONES.

"LA DEPENDENCIA" aplicará deducciones al pago por el incumplimiento parcial o deficiente, en que incurra "EL PROVEEDOR" conforme a lo estipulado en las cláusulas del presente contrato y sus anexos respectivos, las cuales se calcularán por un 1.0% % sobre el monto de los servicios , proporcionados en forma parcial o deficiente. Las cantidades a deducir se aplicarán en el CFDI o factura electrónica que "EL PROVEEDOR" presente para su cobro, en el pago que se encuentre en trámite o bien en el siguiente pago.

De no existir pagos pendientes, se requerirá a "EL PROVEEDOR" que realice el pago de la deductiva a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA´s), a favor de la Tesorería de la Federación, o de la Entidad. En caso de negativa se procederá a hacer efectiva la garantía de cumplimiento del contrato.
Las deducciones se aplicarán cuando el proveedor incurra en incumplimiento parcial o deficiente en la prestación del servicio conforme a los requerimientos de calidad, contenidos y especificaciones técnicas señaladas en el contrato y su Anexo Técnico. Dicha deductiva corresponde al 1% de los servicios proporcionados parcial o deficiente por cada día natural, hasta el 10% del monto total del contrato

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

La notificación y cálculo de las deducciones correspondientes las realizará el administrador del contrato de "LA DEPENDENCIA" , por escrito o vía correo electrónico, dentro de los tres días naturales posteriores al incumplimiento parcial o deficiente.

DÉCIMA CUARTA. PENAS CONVENCIONALES

En caso que "EL PROVEEDOR" incurra en atraso en el cumplimiento conforme a lo pactado para la prestación de los servicios, objeto del presente contrato, conforme a lo establecido en el ANEXO UNO (Anexo Técnico) parte integral del presente contrato, "LA DEPENDENCIA" por conducto del administrador del contrato aplicará la pena convencional equivalente al 1.0% , **por cada día natural de retraso de atraso** sobre la parte de los servicios no prestados, de conformidad con este instrumento legal y sus respectivos anexos.

El Administrador del contrato notificará a "EL PROVEEDOR" por escrito o vía correo electrónico el cálculo de la pena convencional, dentro de los tres días naturales posteriores al atraso en el cumplimiento de la obligación de que se trate.

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

El pago de la pena podrá efectuarse a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA´s), a favor de la Tesorería de la Federación, o la Entidad; o bien, a través de un comprobante de egreso (CFDI de Egreso) conocido comúnmente como Nota de Crédito, en el momento en el que emita el comprobante de Ingreso (Factura o CFDI de Ingreso) por concepto de los servicios, en términos de las disposiciones jurídicas aplicables.

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

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

DÉCIMA QUINTA. LICENCIAS, AUTORIZACIONES Y PERMISOS.

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

DÉCIMA SEXTA. SEGUROS.
DÉCIMA SÉPTIMA. TRANSPORTE

"EL PROVEEDOR" se obliga bajo su costa y riesgo, a trasportar los bienes e insumos necesarios para la prestación del servicio, desde su lugar de origen, hasta las instalaciones señaladas en el I) ANEXO UNO (Anexo Técnico) del presente contrato.

DÉCIMA OCTAVA. IMPUESTOS Y DERECHOS

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

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

DÉCIMA NOVENA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES

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

VIGÉSIMA. DERECHOS DE AUTOR, PATENTES Y/O MARCAS

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

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

En caso de que **"LA DEPENDENCIA"** tuviese que erogar recursos por cualquiera de estos conceptos **"EL PROVEEDOR"** se obliga a reembolsar de manera inmediata los recursos erogados por aquella.

VIGÉSIMA PRIMERA. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES.

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

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 **"LA DEPENDENCIA"** a **"EL PROVEEDOR"** 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 PROVEEDOR"** se compromete a recibir, proteger y guardar la información confidencial proporcionada por **"LA DEPENDENCIA"** 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.

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

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

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

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

Con fundamento en el artículo 55 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 102, fracción II, de su Reglamento, la "LA DEPENDENCIA" en el supuesto de caso fortuito o de fuerza mayor o por causas que le resulten imputables, podrá suspender la prestación de los servicios, de manera temporal, quedando obligado a pagar a "EL PROVEEDOR" , aquellos servicios que hubiesen sido efectivamente prestados, así como, al pago de gastos no recuperables previa solicitud y acreditamiento.

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

VIGÉSIMA TERCERA. TERMINACIÓN ANTICIPADA DEL CONTRATO

"LA DEPENDENCIA" 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 "LA DEPENDENCIA" , o se determine la nulidad total o parcial de los actos que dieron origen al presente contrato, con motivo de la resolución de una inconformidad o intervención de oficio, emitida por la Secretaría de la Función Pública, podrá dar por terminado anticipadamente el presente contrato sin responsabilidad alguna para "LA DEPENDENCIA" , ello con independencia de lo establecido en la cláusula que antecede.

Cuando "LA DEPENDENCIA" determine dar por terminado anticipadamente el contrato, lo notificará a "EL PROVEEDOR" hasta con 30 (treinta) días naturales anteriores al hecho, debiendo sustentarlo en un dictamen fundado y motivado, en el que se precisarán las razones o causas que dieron origen a la misma y pagará a "EL PROVEEDOR" la parte proporcional de los servicios prestados, así como los gastos no recuperables en que haya incurrido, previa solicitud por escrito, siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato, limitándose según corresponda a los conceptos establecidos en la fracción I, del artículo 102 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

VIGÉSIMA CUARTA. RESCISIÓN

"LA DEPENDENCIA" podrá en cualquier momento rescindir administrativamente el presente contrato y hacer efectiva la fianza de cumplimiento, cuando "EL PROVEEDOR" 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) La contravención a los términos pactados para la prestación de los servicios, establecidos en el presente contrato.

b) Si transfiere en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual;

c) Si cede los derechos de cobro derivados del contrato, sin contar con la conformidad previa y por escrito de "LA DEPENDENCIA"

d) Si suspende total o parcialmente y sin causa justificada la prestación de los servicios del presente contrato.

e) Si no se realiza la prestación de los servicios en tiempo y forma conforme a lo establecido en el presente contrato y sus respectivos anexos.

f) Si no proporciona a los Órganos de Fiscalización, la información que le sea requerida con motivo de las auditorías, visitas e inspecciones que realicen;

g) Si es declarado en concurso mercantil, o por cualquier otra causa distinta o análoga que afecte su patrimonio;

h) 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;

i) Si la suma de las penas convencionales o las deducciones al pago, igualan el monto total de la garantía de cumplimiento del contrato y/o alcanzan el 20% (veinte por ciento) del monto total de este contrato cuando no se haya requerido la garantía de cumplimiento;

j) 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 "LA DEPENDENCIA" en los términos de lo dispuesto en la CLÁUSULA VIGÉSIMA PRIMERA DE CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES del presente instrumento jurídico;

k) Si se comprueba la falsedad de alguna manifestación, información o documentación proporcionada para efecto del presente contrato;

l) En general, incurra en incumplimiento total o parcial de las obligaciones que se estipulen en el presente contrato y sus anexos o de las disposiciones de la **"LAASSP"** y su Reglamento.

m) Cuando "EL PROVEEDOR" y/o su personal, impidan el desempeño normal de labores de "LA DEPENDENCIA"

N) Si cambia de nacionalidad e invoca la protección de su gobierno contra reclamaciones y órdenes de **"LA DEPENDENCIA";**

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

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

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

Iniciado un procedimiento de conciliación "LA DEPENDENCIA" podrá suspender el trámite del procedimiento de rescisión.

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

"LA DEPENDENCIA" 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, "LA DEPENDENCIA" elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

De no rescindirse el contrato, "LA DEPENDENCIA" establecerá con "EL PROVEEDOR" , otro plazo, que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento, aplicando las sanciones correspondientes. El convenio modificatorio que al efecto se celebre deberá atender a las condiciones previstas por los dos últimos párrafos del artículo 52 de la **"LAASSP".**

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

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

VIGÉSIMA QUINTA. RELACIÓN Y EXCLUSIÓN LABORAL

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

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

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

Para el caso que, con posterioridad a la conclusión del presente contrato, "LA DEPENDENCIA" reciba una demanda laboral por parte de trabajadores de "EL PROVEEDOR" , en la que se demande la solidaridad y/o sustitución patronal a "LA DEPENDENCIA" , "EL PROVEEDOR" queda obligado a dar cumplimiento a lo establecido en la presente cláusula.

VIGÉSIMA SEXTA. DISCREPANCIAS

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

VIGÉSIMA SÉPTIMA. CONCILIACIÓN.

"LAS PARTES" acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente contrato podrán someterse al procedimiento de conciliación establecido en los artículos 77, 78 y 79 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 126 al 136 de su Reglamento.

VIGÉSIMA OCTAVA. DOMICILIOS

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

VIGÉSIMA NOVENA. LEGISLACIÓN APLICABLE

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

TRIGÉSIMA. JURISDICCIÓN

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

FIRMANTES O SUSCRIPCIÓN.

En esta parte se formaliza el documento suscribiéndolo, señalando en forma clara el lugar y la fecha en que se suscribe, el nombre, cargo y firma de las partes y representantes, tiene relación con lo establecido en el proemio, en las declaraciones en los puntos 1.2, 1.3, 1.4 y 2.2.

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

POR:

"LA DEPENDENCIA"

NOMBRE	CARGO	R.F.C
LUIS FELIPE CANGAS HERNÁNDEZ	DIRECTOR GENERAL DE ADMINISTRACIÓN	[redacted]
ADRIÁN BRINGAS REYES	DIRECTOR DE CONTROL Y SOPORTE TÉCNICO	[redacted]
MIGUEL ÁNGEL CORTÉS TORRES	DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	[redacted]

POR:

"EL PROVEEDOR"

NOMBRE	R.F.C
SOLUCIONES INTEGRALES SAYNET SA DE CV	SIS040817I1A

Las partes testadas se eliminan con fundamento en lo establecido en los artículos 1°, 9, 11, fracción VI, y 104 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 113, fracción I, del citado precepto legal, que establece que, se considera información confidencial la que contiene datos personales concernientes a una persona física identificada o identificable. Por ello, se elaboró esta versión Pública del "Contrato CONT-025-2023", conforme a lo señalado en el artículo 118 de la ley en cita.

Cadena original:

[redacted]

Firmante: LUIS FELIPE CANGAS HERNANDEZ
RFC: [redacted]
Número de Serie: [redacted]
Fecha de Firma: 27/03/2023 10:45
Certificado:

[redacted]

Firma:

[redacted]

Firmante: MIGUEL ANGEL CORTES TORRES
RFC: [redacted]
Número de Serie: [redacted]
Fecha de Firma: 27/03/2023 10:55
Certificado:

[redacted]

Firma:

[redacted]

Firmante: ADRIAN BRINGAS REYES
RFC [redacted]
Número de Serie: [redacted]
Fecha de Firma: 27/03/2023 16:12
Certificado:

[redacted]

Firma:

Las partes testadas se eliminan con fundamento en lo establecido en los artículos 1°, 9, 11, fracción VI, y 104 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 113, fracción I, del citado precepto legal, que establece que, se considera información confidencial la que contiene datos personales concernientes a una persona física identificada o identificable. Por ello, se elaboró esta versión Pública del "Contrato CONT-025-2023", conforme a lo señalado en el artículo 118 de la ley en cita.

[redacted]

Firmante: SOLUCIONES INTEGRALES SAYNET SA DE CV
RFC: SIS040817I1A

Número de Serie: [redacted]
Fecha de Firma: 27/03/2023 17:41

Certificado:

[redacted]

Firma:

[redacted]

Las partes testadas se eliminan con fundamento en lo establecido en los artículos 1°, 9, 11, fracción VI, y 104 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 113, fracción I, del citado precepto legal, que establece que, se considera información confidencial la que contiene datos personales concernientes a una persona física identificada o identificable. Por ello, se elaboró esta versión Pública del "Contrato CONT-025-2023", conforme a lo señalado en el artículo 118 de la ley en cita.

ANEXO UNO: ESPECIFICACIONES TÉCNICAS

1. Descripción del Bien y/o Servicio

1.1 Identificación del proyecto

Solución de infraestructura de red (LAN, WIFI) seguridad perimetral y servidores

1.2 Objetivo

El Licitante brindará el servicio de suministro y equipamiento mediante soluciones integradas de red alámbrica e inalámbrica, seguridad informática y computo en los inmuebles de la Secretaría de Turismo (SECTUR) derivado de las funciones sustantivas y adjetivas que se realizan en ellos y contribuir a la misión de la SECTUR.

1.3 Vigencia

Fecha inicio del servicio
16 de marzo de 2023
La entrega del servicio funcionando y operado al 100 % a partir del 16 de marzo de 2023.

Para este efecto el Licitante contará para su implementación, con el plazo comprendido a partir de la notificación y hasta el 16 de marzo de 2023, el equipo puede ser no nuevo y encontrarse en óptimas condiciones de operación.

Fecha de fin de servicio
31 de diciembre de 2023
La etapa de cierre del servicio, aplicable a la infraestructura de cómputo Institucional, iniciará 45 días naturales previos a la conclusión de la vigencia.

1.4 Relación de los Servicios a Contratar

- Servicio de infraestructura de red.
- Servicio de Seguridad perimetral.
- Servicio de Antivirus
- Servicio de Respaldos
- Servicio de Infraestructura de Servidores
- Servicio de Monitoreo de red y Mesa de Ayuda
- Escaneo De Vulnerabilidades y certificados digitales
- Soporte a SITE, cuartos de comunicaciones y cableado estructurado

1.4.1. Requerimientos de recuperación de bienes al término del contrato:

a) El licitante en un término no mayor a 30 días naturales posteriores al término del contrato retirará la infraestructura activa de las instalaciones de la SECTUR previa demostración de que los equipos son de su propiedad.
b) Los equipos de infraestructura activa que no sean retirados en un plazo de 90 días naturales posteriores al término del contrato atribuible al licitante, la SECTUR tomará las medidas legales y administrativas correspondientes para que dichos bienes pasen a ser parte del inventario de la SECTUR.

1.4.2. Requerimiento de migración de servicios al término del contrato

Al término de la vigencia del contrato, el licitante está obligado a realizar las actividades propias de transferencia y migración de los servicios hacia un nuevo Prestador de servicios.

1.4.3 Otros requerimientos que deberá cumplir el licitante para la prestación del servicio.

a) Todos los requerimientos y especificaciones son mínimos.
b) Toda la solución se debe proporcionar como un servicio integral, por tanto, el licitante debe considerar que todos los requerimientos, especificaciones técnicas y servicios expresados en este anexo técnico, así como lo necesario para llevar a cabo la implantación, la operación, el soporte técnico, contar con los recursos humanos y materiales para cumplir con lo solicitado por la SECTUR.
c) Toda la infraestructura suministrada y empleada para la prestación del servicio integral por parte del licitante será de su propiedad y entera responsabilidad.
d) Toda la infraestructura pasiva suministrada para la prestación del servicio integral por parte del proveedor pasará a ser propiedad de la SECTUR al término del contrato. Entiéndase como infraestructura pasiva como los elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión.
e) El licitante será responsable de la legalidad y autenticidad de los derechos de autor, derechos de propiedad industrial o patentes del software y/o hardware utilizados para brindar el servicio integral.
f) El licitante sólo podrá exigir el pago de los conceptos que específicamente se encuentren detallados en la propuesta económica. Cualquier otro concepto que no aparezca en dicha propuesta no será exigible. Por lo anterior, el licitante debe considerar todos los costos inherentes de los servicios, requerimientos, especificaciones técnicas, niveles de servicio, documentos, recursos humanos, materiales, equipos, infraestructuras entre otros en el precio final de los servicios que son parte de su propuesta económica.
g) Es responsabilidad del licitante el diseño de la arquitectura tecnológica de cada una de las soluciones de servicio que proponga y en la que deberá considerar cada uno de los requerimientos, especificaciones técnicas y servicios de cada solución. Si durante el proceso de implementación, pruebas y operación de cada solución se detecta que esta no cubre adecuadamente algún requerimiento, especificación técnica y servicio expresado en este anexo técnico o existan problemas de compatibilidad e integración entre los componentes de cada solución, el licitante deberá realizar los cambios de arquitectura tecnológica, componentes, equipos, accesorios, software, licenciamiento y cualquier otro elemento que sean necesarios para solucionar esta deficiencia sin costo adicional para la Secretaría de Turismo.
h) Las características, capacidades y funcionalidades que no sean específicamente detalladas en este anexo técnico y que sean incluidas en cualquiera de las soluciones ya sea que estás estén integradas en el hardware, software o que se encuentren amparadas por el uso de la licencia serán puestas en operación y usados como parte integral del servicio.

1.5 Requerimientos del Servicio / Consideraciones para todos los componentes

Requerimientos funcionales:

Se requiere el suministro, distribución, instalación, configuración, puesta a punto y entrada en operación de equipos y componentes físicos especializados que provean:

- Servicio de infraestructura de red.
- Servicio de Seguridad perimetral.
- Servicio de Antivirus
- Servicio de Respaldos
- Servicio de Infraestructura de Servidores
- Servicio de Monitoreo de red y Mesa de Ayuda
- Escaneo De Vulnerabilidades y certificados digitales
- Soporte a SITE, cuartos de comunicaciones y cableado estructurado

Requerimientos no funcionales:

- Niveles de servicio conforme a lo detallado en la sección 5 "Niveles de Servicio".
- Soporte documental del servicio.

Requerimientos y controles de seguridad:

- Efectuar el borrado seguro de cualquier dispositivo de almacenamiento que sea retirado durante la vigencia del servicio.

Requerimientos de implementación y puesta en operación:

- El Licitante contemplará toda la logística necesaria para realizar el reemplazo de los equipos que componen la solución que proponga en cada uno de los inmuebles de la SECTUR.

Consideraciones generales para todos los componentes:

- Todos los equipos suministrados durante la vigencia del servicio serán de características iguales o superiores a los solicitados en las especificaciones técnicas de este documento
- El Licitante contemplará en su propuesta todos los accesorios, cables de alimentación, cables de red, cables de fibra, rieles, herrajes y todo lo necesario para la adecuada instalación e integración entre sí y en condiciones seguras de operación para todos los componentes de la solución que proponga.
- El Licitante deberá contemplar en su propuesta toda la canalización, ductos y herrajes para interconectar los racks que proponga hacia el rack de comunicaciones existente en el centro de datos de Masaryk, así como también, las adecuaciones al piso falso que requiere la implementación de la solución de seguridad informática.
- El Licitante deberá contemplar la solución de seguridad informática la adecuada integración con la infraestructura existente en el centro de datos de la SECTUR.
- El Licitante deberá contemplar la instalación de los circuitos eléctricos y protección eléctrica (aterrizaje de los equipos de las soluciones que sean instalados hacia el sistema de tierra existente) en el centro de datos de Masaryk planta baja para los equipos de las soluciones que sean instalados en el mismo. La SECTUR cuenta con un tablero de

distribución trifásico localizado en el centro de datos. La distancia máxima de los circuitos eléctricos es de 12 metros.

- La instalación física de todos los equipos, rack's, componentes, cableados, accesorios y cualquier dispositivo de la solución de seguridad informática usado para el proceso de implementación estará correctamente ensamblado, adecuadamente colocado y ser seguro bajo los criterios que marque el supervisor del servicio.
- La operación de la solución de seguridad informática propuesta por "LAS EMPRESAS" está garantizada conforme a los niveles de servicio solicitados en este anexo técnico durante toda la vigencia del contrato.
- El Licitante deberá tener actualizado el inventario y resguardos de los equipos de la solución propuesta, incluyendo altas, bajas, cambios y reubicación.
- El personal El Licitante" que labore durante la vigencia del contrato y efectúe trabajos relacionados con el servicio de este anexo técnico firmaran el documento de acuerdo de confidencialidad suministrado por el administrador del contrato.

Implementación y puesta en operación:

- Proporcionar un plan de trabajo de implementación de todos los equipos que compongan las soluciones de seguridad informática. Este puede ser implementado en fases, las cuales podrán ser actividades paralelas o secuenciales considerando la complejidad de la infraestructura en operación. El plan de trabajo será aprobado por el administrador del contrato. El plan de trabajo se ejecutará para proporcionar los servicios el 16 de marzo de 2023.
- El Licitante iniciaran la etapa de operación el (16 de marzo de 2023) hasta la vigencia del contrato que corresponda y consistirá en la administración, mantenimiento y soporte de los recursos que se encuentren instalados y operando de toda la solución.
- La instalación de los circuitos eléctricos en el centro de datos de Masaryk con la capacidad suficiente para soportar los rack's con su respectivo equipamiento.
- Adecuaciones y/o reposiciones de galletas del piso falso derivado de la instalación de los equipos.
- La instalación de los rack's de la solución.
- La instalación, configuración y puesta a punto de todos los equipos de la solución, su software y componentes.

En cada una de las actividades de implementación pueden realizarse actividades de validación, verificación y pruebas del hardware y software para ser aprobadas antes de su puesta en operación y paso a producción las cuales serán autorizadas por el administrador del contrato.

2. Características Técnicas y Funcionalidades

SECTUR tiene alojados en su Datacenter buzones de correo electrónico para 1500 cuentas habilitadas y da servicios de Internet a 900 usuarios activos, los cuáles son usados para desempeñar funciones orientadas a los objetivos institucionales y cuyas actividades requieren, entre otros los servicios de navegación segura, conexiones seguras y protección a la información que se genera.

Para preservar la operatividad de los servicios que SECTUR otorga a las áreas responsables para su adecuado funcionamiento, requiere contar con las soluciones y/o herramientas tecnológicas.

SECTUR tiene el propósito específico de cada una de las soluciones tecnológicas de acuerdo con lo siguiente:
Seguridad Perimetral para usuario y datacenter: Las soluciones de seguridad perimetral protegen a las redes institucionales de la entrada de código malicioso o malware, permiten filtrar el tráfico del exterior hacia la red institucional. Además, se han presentado ataques de ransomware ante los cuales no se puede reaccionar de manera preventiva, para lo anterior se requiere de la protección a al centro de datos y de los usuarios desde el perímetro y en sus estaciones de trabajo, para garantizar la disponibilidad, autenticidad e integridad de la información, previniendo también de posibles secuestros de la información.
El Licitante deberá cumplir con los siguientes servicios administrados:

- Servicio de infraestructura de red.
- Servicio de Seguridad perimetral.
- Servicio de Antivirus
- Servicio de Respaldos
- Servicio de Infraestructura de Servidores
- Servicio de Monitoreo de red y Mesa de Ayuda
- Escaneo De Vulnerabilidades y certificados digitales
- Soporte a SITE, cuartos de comunicaciones y cableado estructurado

2.1 Servicio de Infraestructura de Red

La solución de switches core propuesta deberá ser de alta disponibilidad, alto rendimiento y seguridad.
Se debe considerar por el proveer una red de datos de dos niveles, Núcleo (CORE) y Acceso además de un controlador de Red LAN inalámbrica (WLAN) igualando el número de Puntos de Acceso (Access Points), que se encuentran actualmente operando para lo cual se deberán considerar al menos 65AP´s
Lograr una red capaz de soportar la convergencia de tráfico de datos, voz, video y de la red inalámbrica, debe ser considerada como prioridad en la propuesta presentada por los Prestadores de Servicio, para ello el Prestador de Servicio debe proponer el equipamiento y sistemas necesarios para lograr tal propósito, entre ellos se destacan:

- Análisis del equipamiento actual de red LAN y la red WLAN
- Proporcionar equipo igual o elevando sus características y funcionalidades a las requeridas en el presente anexo técnico.

Solución requerida
La red actual de la SECTUR está conformada por redes LAN en los tres sitios principales, donde hay un equipo operando como unidad de Núcleo (CORE TIPO 2) en cada edificio y diferentes equipos de acceso.
El equipo propuesto deberá igualar o mejorar estas características. En la Tabla 1, se muestra la distribución de los equipos a remplazar por Edificio y por IDF.

ÁREA	TIPO	CANTIDAD	NÚMERO DE PUERTOS COBRE	TOTAL DE PUERTOS COBRE	NÚMERO DE PUERTOS FIBRA	CONTROLADORAS / PROCESADORAS	FUENTES DE PODER
MASARYK							
Centro de Datos	CORE TIPO 2	1	48	48	24	2	3
MDF-PB	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	5	48	240	0	DEFAULT	DEFAULT
IDF-P2	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	5	48	240	5	DEFAULT	DEFAULT
IDF-P5	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	4	48	192	4	DEFAULT	DEFAULT
IDF-P8	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	3	48	144	4	DEFAULT	DEFAULT
IDF-P11	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	3	48	144	2	DEFAULT	DEFAULT
Red DMZ	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	1	48	48	0	DEFAULT	DEFAULT
SCHILLER							
IDF	CORE TIPO 2	1	48	48	16	2	3
MDF-PB	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	3	48	144	3	DEFAULT	DEFAULT
MDF-P3	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	3	48	144	3	DEFAULT	DEFAULT
MDF-P6	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	3	48	144	3	DEFAULT	DEFAULT
MDF-P9	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	3	48	144	3	DEFAULT	DEFAULT

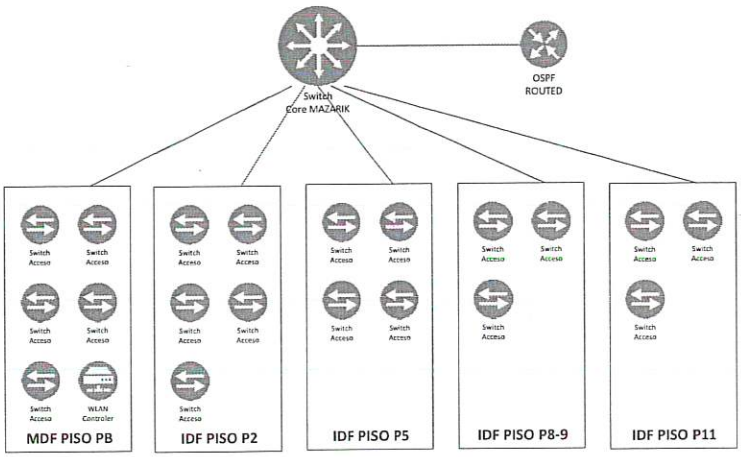
ÁREA	TIPO	CANTIDAD	NÚMERO DE PUERTOS COBRE	TOTAL DE PUERTOS COBRE	NÚMERO DE PUERTOS FIBRA	CONTROLADORAS / PROCESADORAS	FUENTES DE PODER
MDF-PH	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	2	48	96	2	DEFAULT	DEFAULT
VIADUCTO							
IDF	CORE TIPO 2	1	48	48	16	2	3
MDF-PB	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	4	48	192	4	DEFAULT	DEFAULT
IDF-P1	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	5	48	240	4	DEFAULT	DEFAULT
IDF-Capacitación	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	1	48	48	0	DEFAULT	DEFAULT
AIFA							
AIFA	SWITCH DE ACCESO 24 PUERTOS POE CAPA 2	1	24	24	0	DEFAULT	DEFAULT

Tabla 1. Distribución de los equipos a reemplazar por inmueble e IDF.

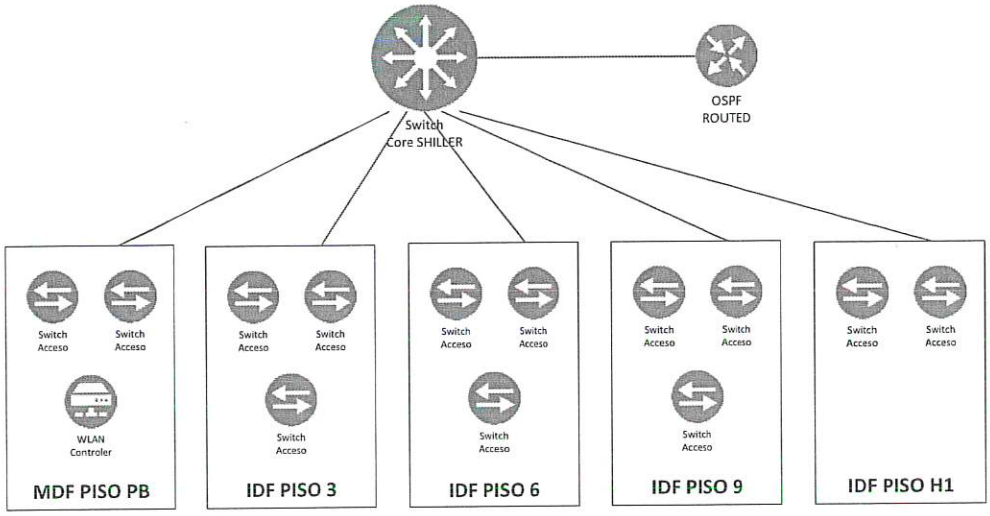
Adicionalmente el licitante deberá considerar que deberá proporcionar el soporte, mantenimiento y administración de un Switch de 48 puertos de la SECTUR, con las siguientes características:
Modelo: Summit X460
Marca: Extremme

En cuanto a la red inalámbrica WLAN, es necesario que se proponga una arquitectura centralizada donde un switch/controlador CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1) administre, monitoree, controle y valide la operación de la red inalámbrica como un todo superpuesto a la red cableada.
La solución propuesta por el licitante es en modo de arrendamiento, se solicita el equipamiento, instalación y administración de la solución propuesta que debe considerar el equipamiento de la tabla 1.

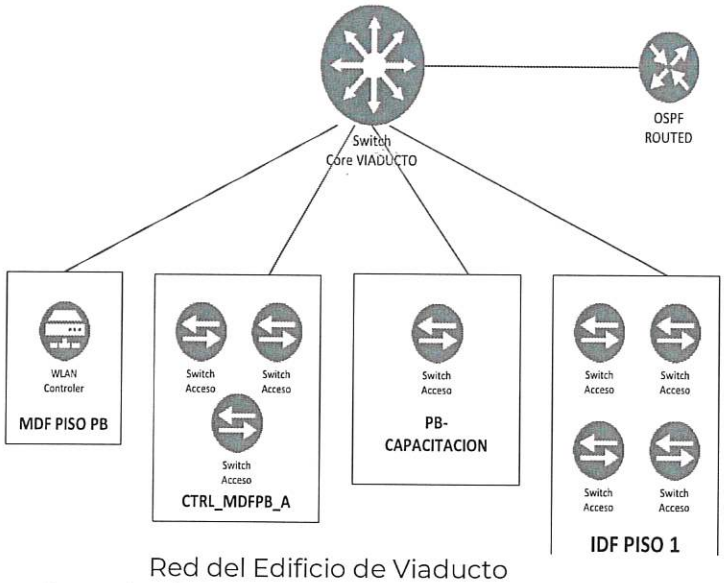
Diagramas Conceptuales de red



Red del Edificio de Presidente Masaryk



Red del Edificio de Schiller



Red del Edificio de Viaducto

Cada uno de los equipos Centrales (CORE TIPO 2) y de los equipos de acceso deberán cubrir las características señaladas en este anexo.

Red Inalámbrica

La Red inalámbrica WLAN de la SECTUR está formada por 65 Access Points (PUNTO DE ACCESO PARA INTERIORES TIPO 1) simplemente proporcionando entrada a la red LAN Institucional.
Por este motivo, se requiere de una solución centralizada que controle la función, operación y seguridad en la red inalámbrica (CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1). Esta solución deberá utilizar las mismas ubicaciones de cobertura existente y reforzar en la cobertura en caso de necesitarse.

Para garantizar un mayor grado de seguridad los AP actuales fueron requeridos para su operación en modo centralizado.

2.1.1 Funcionalidades de los equipos

Los equipos a proponer en la solución, independientemente si éstos son para el Núcleo (CORE TIPO 2) de la red o el Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2) a la misma deben contar con las siguientes características mínimas:

- Arquitectura no-bloqueable: Necesaria para soportar aplicaciones de tiempo real, tales como, la voz y el video que requieren obligatoriamente de esta característica de arquitectura interna que le permite manejar todos los puertos de red al 100% de su capacidad sin pérdida de paquetes.
- Alta Disponibilidad: Poder tener una disponibilidad de 99.999% para el Núcleo de la Red (CORE TIPO 2) y 99.99% para el Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2),

para lo cual todos los sistemas deben proveer mecanismos redundantes tales como procesamiento y control, fuentes de poder, ventiladores y sistema operativo en los equipos para el Núcleo (CORE TIPO 2), y por lo menos una fuente de poder y un sistema operativo para los equipos de Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2).

- Calidad de Servicio: Para poder diferenciar y tratar de manera adecuada todas las aplicaciones que corren en la red, todos los equipos propuestos deberán soportar las mismas características técnicas y así proveer Calidad de Servicio.
- Altos niveles Seguridad: Todas las unidades propuestas deberán contar con sistemas de seguridad de alto nivel tales como protección contra ataques de Negación de Servicio, Seguridad Avanzada para el Protocolo IP, monitoreo de flujos de IP en todos los puertos de red de los equipos. Capacidades para el despliegue de sistemas de control de acceso de red, así como el soporte para sistemas de autenticación de usuario. Los equipos deberán contar con un motor de seguridad que les permita reaccionar ante amenazas de seguridad, ataques, o comportamientos maliciosos e iniciar algún mecanismo de remediación.
- Fácil Administración: Todos los sistemas propuestos deberán contar con el mismo sistema operativo y línea de comandos. Esto aplica para los equipos para el Núcleo de la red, así como para los de Acceso. Adicionalmente se requiere que, si el participante sustituye equipos que actualmente se encuentran en la red de la SECTUR, los equipos propuestos deberán soportar algún tipo de emulación de la línea de comandos de los equipos existentes. El licitante deberá considerar proveer un Sistema de Administración de Redes compatible con los equipos propuestos, y permitir la administración, monitoreo, configuración y aprovisionamiento automatizado de los equipos de manera fácil y lógica.
- Red Convergente: La solución propuesta deberá ser capaz de soportar aplicaciones propias de una red convergente, para poder ser el medio de conducción de tráfico dedicado a datos, VoIP, video encapsulado en IP, y el tráfico proveniente de la red WLAN. Como parte de su propuesta técnica los Prestadores de Servicio deberán presentar un "Plan de Ingeniería de Tráfico" que describa la forma en cómo la red propuesta tratará cada uno de estos escenarios de tráfico, de manera eficiente y de fácil administración.

Cada uno de estos requerimientos generales, son mínimos e imprescindibles, por lo que deberán estar respaldadas mediante el soporte y manejo de protocolos y arquitecturas abiertas. Más adelante en este anexo, se presentan las especificaciones técnicas a detalle para cada uno de los tipos de nodos de red, solicitados en la presente convocatoria.

Niveles de Redundancia para Alta Disponibilidad del Servicio

- La solución propuesta debe proveer todos los niveles de redundancia necesarios para asegurar la alta disponibilidad.

Redundancia en Hardware

- Redundancia en los tipos de nodos para el Núcleo (CORE TIPO 2) de la red. Los equipos propuestos deben contar con:

Viaducto Presidente Miguel Alemán Valdés No. 81, Colonia Escandón 1 Sección, CP. 11800, Alcaldía Miguel Hidalgo, CDMX.
Tel: (55) 3002 6300 www.gob.mx/sectur

- Redundancia en tarjetas procesadoras (Switch Fabric) y de control/administración.
- Redundancia en Fuentes de Poder, que permita la agregación sobre demanda de mayor potencia, con la adición de Fuentes de acuerdo a la carga presente o agregada a la unidad. Por esta razón se requiere de equipos que cuenten con Fuentes de Poder en arreglo N+1.

- Redundancia en los tipos de nodos para el Acceso de la red. Los equipos propuestos deben contar con:
  - Redundancia en Fuentes de Poder
  - Redundancia en Software

- Los equipos propuestos para el Núcleo de la red, deberán contar para la redundancia en software con las siguientes funcionalidades:
  - Doble almacenamiento en memoria FLASH para imágenes del S.O. y archivos de configuración en la procesadora primaria.
  - Doble almacenamiento en memoria FLASH para imágenes del S.O. y archivos de configuración en la procesadora secundaria.
  - Sistema Operativo Modular compatible con la arquitectura POSIX, con procesamiento independiente para todas las tareas que controlen los diferentes algoritmos y protocolos soportados por la unidad. Cada proceso del S.O. debe ejecutarse independiente, para que, en caso de falla de alguno, los demás sigan operando sin interrupción. Esto debe extenderse no solo a fallos sino también a ataques dirigidos a un protocolo en particular.

- Redundancia a Nivel de Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2)
  - Los equipos requeridos para el Nivel de Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2), son principalmente equipos de arquitectura apilable y con enlaces de alta velocidad hacia el Nivel de Núcleo (CORE TIPO 2). Por lo que deberán contar con funcionalidades para aprovechar por lo menos dos enlaces de alta velocidad mediante la agregación.

- Descripción de los enlaces
  - Los enlaces entre los equipos de Núcleo (CORE TIPO 2) y Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2), deberán entregarse con conexiones de Gigabit Ethernet en Fibra Óptica.
  - Los enlaces hacia los usuarios de la red incluyendo equipos periféricos, deberán entregarse con conexiones 10/100/100BaseT.
- Calidad de Servicio
  - Las redes de la SECTUR están concebidas para tener un ambiente de red, donde varias aplicaciones vitales y servicios deben corren indistintamente por los diferentes medios de transmisión. Por lo mismo se requiere una jerarquía de los mismos. Las aplicaciones de importancia crítica sensibles a retardos, como la voz (VoIP) y la transmisión de video, deben garantizarse mediante la implementación de mecanismos de Calidad de Servicio. Por lo que es requisito que todos los equipos propuestos soporten al menos 8 niveles de QoS en Capa 2 definidos por

el estándar IEEE 802.1p que deberán mapearse a los niveles en Capa 3 soportados por los esquemas el estándar DiffServ.

- Los criterios para la clasificación de tráfico son los siguientes:
  - Tráfico Explícitamente Etiquetado - (i.e. los paquetes contienen información o etiquetas que indican al equipo de red el nivel de servicio requerido)
  - Capa 2: 802.1p - De acuerdo del estándar de la evolución de Ethernet que añade distintos campos, entre ellos tres bits de prioridad, lo que permite formar una diferenciación con 8 niveles de prioridad. Operando en Capa 2.
  - Capa 3: ToS y DiffServ – ToS (Tipo de Servicio) Que dentro del paquete IP (Capa 3), que junto con la definición del estándar DiffServ, en donde se especifica la calidad de servicio requerida.
  - Tráfico Implícitamente marcado, tráfico que no contiene información de QoS pero que debe ser inferida por el equipamiento de red.
  - Capa 1: Por puerto físico origen.
  - Capa 2: Por dirección MAC origen o destino – De la misma manera que en el rubro anterior, la dirección física de capa 2 puede proporcionar el parámetro de clasificación de tráfico.
  - Capa 3: Por dirección IP origen o destino – La dirección IP deberá ser parámetro suficiente para su clasificación por parte de los equipos de red.
  - Capa 4: Por socket UDP o TCP – Análisis de los paquetes a mayor profundidad, ya que pudiera ser tráfico crítico o sin importancia y demandante en cuanto a ancho de banda, para lo cual, el socket UDP o TCP debe proporcionar la información de la naturaleza del tráfico para su clasificación y tratada así por parte del equipamiento de red.

- Administración

  Los equipos propuestos deberán ser administrados por varias vías, mismas que se describen a continuación:
  - CLI, Línea de Comandos:
  - La línea de comandos (command line interface) Los comandos y el lenguaje deberán ser consistentes en todos los equipos de red, presentados de una manera estructurada y amigable, además de contar con ayudas para terminación de comandos y posibles parámetros.
  - De manera adicional, los equipos propuestos deberán soportar una manera de emular la línea de comandos de los equipos actualmente instalados con excepción de los encontrados en menor cantidad en la red.
  - La línea de comandos deberá ser accesada directamente mediante puerto serial, Telnet o Secure Shell para conexiones remotas seguras.

- Interface Web:
  - Los equipos también deberán contar con acceso mediante una interface Web para su administración, monitoreo y configuración de manera gráfica y remota. Deberá contarse con el soporte para http o https

- Sistema de Administración de Redes

  Esta deberá poder ser instalada en un servidor Windows XP, Vista W7, Solaris o Linux. Además de correr como una plataforma independiente, Contar con herramientas para:
  - Administración e Inventario de dispositivos: Que deberá descubrir los dispositivos y generar una base de datos central de los mismos. Los dispositivos deberán ser monitoreados continuamente para mantener actualizada la información.
  - Administrador de Configuraciones: Que posibilite la actualización automatizada y sencilla de sistemas operativos de los equipos. Que contenga un directorio local con las distintas versiones utilizadas. Que archive las configuraciones de los dispositivos de red periódicamente, con el fin de contar con un respaldo actualizado de manera automática. Que automatice la descarga de nuevas versiones del sistema operativo.
  - Administrador de Alarmas: Que deberá administrar las alarmas generadas por los equipos. Que cuente con una lista de alarmas previamente configuradas que reflejan los eventos más comunes. Que puedan configurarse alarmas personalizadas para eventos específicos con sus respectivos umbrales para cubrir necesidades específicas. Deberá generar una bitácora de los eventos registrando parámetros particulares como hora, criticidad, etc. y se deberá manejar un código de colores para su rápida revisión. Las alarmas también pueden provocar respuestas automáticamente como envió de correos electrónicos, alarmas sonoras, o ejecución de un script para su ejecución en los equipos de la red.
  - Sesiones de Administración Remota: Desde esta herramienta se deberán abrir sesiones de telnet, SSH o web. Adicionalmente, la plataforma de administración de red deberá permitir la invocación de una sesión de administración remota mediante un navegador web.
  - Gestionador de Scripts de Configuración. Se deberá contar con un editor de scripts de configuración, y desde esta plataforma de administración deberá desplegarse hacia los equipos de la red y programar o disparar su ejecución.
  - Presentación Gráfica: La plataforma deberá presentar gráficamente imágenes de los equipos y sus componentes como módulos de interfaz, tarjetas centrales, fuentes de poder, ventiladores, puertos físicos, etc. Al seleccionar los distintos elementos, se deberá presentar información y estado de los mismos. Adicionalmente se deberá generar una representación topológica de la red física.
  - Generador de Reportes: Mismo que deberá generar reportes, como: listados de vlans, historiales de alarmas, errores de transmisión, etc. Estos reportes deberán poder ser presentados de manera gráfica, en tablas, o exportados en distintos formatos para su uso en otras aplicaciones.
  - Estadísticas en Tiempo Real: Deberá contar con un sistema que genere histogramas que reflejen estadísticas en tiempo real, sobre puertos y dispositivos que reflejen la utilización de los mismos.
  - Visualizador de Topología de Red: Servicio que muestre de manera gráfica la topología de la red, en la que se puedan identificar las VLANs configuradas en la red, mostrando los puertos, enlaces y dispositivos de la VLAN seleccionada en el visualizador.

El Sistema de Administración de Redes deberá ser repositorio de TRAPS vía SNMP; administrar la red LAN y la red WLAN vía SNMP. Adicionalmente deberá poder monitorear cualquier dispositivo compatible con MIB II.

Se requiera que el Sistema de Administración de Redes pueda actuar como syslog server, para almacenar los event logs de todos los dispositivos que apunten al servidor de administración.

El Sistema deberá soportar los protocolos RMON, SNMPv1/v2 y SNMPv3 Vía RMON se deben graficar tasas de errores de tx, errores de rx, errores de fragmentación, errores de colisión o CRC.

El ahorro de energía se debe contemplar

- Ahorro de energía en los equipos tipo chasís con fuentes en arreglo N+1 para garantizar consumo de energía sobre demanda. Los equipos de Núcleo (Core), deberán contar con algún mecanismo de hibernación que se active cuando no haya tráfico en algún puerto de red. Al detectarse tráfico, los puertos deberán activarse de manera automática e imperceptible por los usuarios y aplicaciones.

2.1.2 Características Técnicas

EQUIPOS A NIVEL DE NÚCLEO DE LA RED (CORE TIPO 2)

ARQUITECTURA Y CAPACIDADES:

- Equipo modular de al menos cuatro ranuras para interfaces de servicio.
- Debe contar con desempeño de al menos 1.9 Tbps de conmutación.
- Debe soportar una capacidad de reenvío de paquetes de al menos 1400 Mpps.
- Debe ofrecer al menos 250 Gbps por ranura.
- Arquitectura sin bloqueos (Non-blocking)
- Soporte de interfaces 1, 10 GE.
- Soporte de tarjetas de procesamiento redundantes.
- Soporte de fuentes de poder y ventiladores redundantes.
- Soportar protocolos de enrutamiento RIP, OSPF, BGP, ruteo estático, en sus versiones más recientes estables liberadas, tanto en IPv4 como en IPv6.
- Soporte de al menos 512 mil direcciones MAC.
- Soporte de 4 mil VLANs

FUNCIONALIDADES:

- Opere con protocolos IPv4/IPv6.
- Soporte de IGMPv2/v3 y IGMPv2/v3 Snooping.
- Soporte de PIM-DM, PIM-SM y PIM-SSM.
- Capacidad instalada de VRRP o HSRP.
- Administración por Interface de línea de comandos (CLI), SNMPv2/v3.
- Soporte incluido de sFlow o similar.
- Soporte de múltiples niveles de privilegios de acceso por consola para administrador.
- Soporte de ACLs por puerto, en capas 2, 3 y 4.
- Soporte de Port Mirroring.
- Soportar encapsulamiento de VLANs Q-in-Q.

- Soporte de calidad de servicio (QoS) incluyendo:
- Clasificación de tráfico en capa 2, 3 y 4.
- Temperatura de operación de 0 a 40 °C.

SEGURIDAD:

- Soporte de autenticación 802.1X, dirección MAC y Portal.
- Soporte de RADIUS.
- Soportar defensa contra ataques de DoS.
- ADMINISTRACIÓN Y MANTENIMIENTO
- Soporte de SNMP v1, v2c y v3.
- Soporte de servidor externo de NTP.
- Soporte de gestión a través de línea de comando (CLI) o vía web.
- Soporte de administración por puerto de consola, Telnet y SSH
- Soporte de FTP y TFTP
- Soporte de registros de operaciones de usuarios.

EQUIPOS SWITCH DE ACCESO 48 PUERTOS POE CAPA 2

ARQUITECTURA Y CAPACIDADES

- Debe estar equipado con 48 puertos 10/100/1000 BaseT.
- Debe contar con desempeño de al menos 250 Gbps de conmutación.
- Debe soportar una capacidad de reenvío de paquetes de al menos 130 Mpps.
- Soporte de 48 puertos PoE de manera simultánea.
- Soporte al menos cuatro puertos SFP compartidos
- Soportar protocolos de enrutamiento RIP y ruteo estático.
- Soporte de al menos 8 mil direcciones MAC.
- Soporte de 4 mil VLANs
- Soporte de apilamiento o Stacking de 8 unidades, con velocidad de al menos 40 Gbps.

FUNCIONALIDADES

- Opere con protocolos IPv4/IPv6.
- Soporte de IGMPv2/v3 y IGMPv2/v3 Snooping.
- Soporte de PIM-SM y PIM-SSM.
- Capacidad instalada de VRRP o HSRP.
- Administración por Interface de línea de comandos (CLI), SNMPv2/v3.
- Soporte incluido de sFlow o similar.
- Soporte de múltiples niveles de privilegios de acceso por consola para administrador.
- Soporte de ACLs por puerto, en capas 2.
- Soporte de Port Mirror.
- Soporte de calidad de servicio (QoS) incluyendo:
- Clasificación de tráfico en capa 2.
- Soporte de ITU-Y.1731, y 802.1ag para detención de fallas.
- Temperatura de operación de 0 a 40 °C.

SEGURIDAD

- Soporte de autenticación 802.1X, dirección MAC y Portal.

- Soporte de RADIUS.
- Soportar defensa contra ataques de DoS.

ADMINISTRACIÓN Y MANTENIMIENTO

- Soporte de SNMP v1, v2c y v3.
- Soporte de servidor externo de NTP.
- Soporte de gestión a través de línea de comando (CLI) o vía web.
- Soporte de administración por puerto de consola, Telnet y SSH
- Soporte de FTP o TFTP
- Soporte de registros de operaciones de usuarios.

2.1.3 Normas, Estándares y Protocolos

Normas, Estándares y Protocolos para todos los Switches:

- IEEE 802.1D Media Access Control (MAC) Bridges
- IEEE 802.1p Virtual Bridged Local Area Networks
- IEEE 802.1Q Virtual Bridged Local Area Networks
- IEEE 802.1ad Provider Bridges
- IEEE Std 802.3ab 1000BASE-T specification
- IEEE Std 802.3ad Aggregation of Multiple Link Segments
- IEEE Std 802.3ae 10GE
- IEEE Std 802.3z Gigabit Ethernet Standard
- IEEE 802.1ag Connectivity Fault Management
- IEEE 802.1ab Link Layer Discovery Protocol
- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol
- IEEE802.1X Port based network access control protocol
- IEC 60950-1
- UL 60950-1
- CSA C22.2 No 60950-1

ESPECIFICACIONES TÉCNICAS DE LA SOLUCIÓN WLAN.

Equipo CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1

La controladora hace las funciones de control centralizados, sin embargo, el tráfico de los usuarios no debe pasar por la controladora.

CAPACIDADES

- Soportar al menos 245 Puntos de Acceso.
- Debe soportar la gestión de al menos 4,000 usuarios conectados.
- Desempeño del dispositivo de al menos 3.6 Gbps
- Debe contar con al menos 6 puertos 10/100/1000 Base-T y 2 x USB Port.
- Debe contar con un puerto de consola del tipo RJ-45
- Soportar al menos 16 SSID o VNS.
- Soportar al menos 30 SSID o VNS, para Mazaryk

FUNCIONALIDADES

- Debe manejar los estándares 802.11 a/b/g/n/ac.

- Soportar balanceo de carga entre las diferentes redes.
- Soporte de un portal básico para autenticación.
- Soportar asignación dinámica de canales para optimizar la cobertura y desempeño.
- Soporte de detección, y capacidad de evitar, interferencia mediante la re- calibración de la red
- Debe soportar los siguientes métodos de autenticación: 802.1x, MAC, Portal Web.
- Debe contar con tecnología para el control dinámico de la radio frecuencia (RF) y reaccionar automáticamente ante eventos de ruido e interferencia.
- Debe contar con un tablero centralizado de estado de la red inalámbrica.
- Soporte de calidad de servicio QoS.
- Deberá contar con políticas diferenciadas por SSID.

SEGURIDAD
- Soportar los siguientes métodos de autenticación: WEP, WPA/WPA2–PSK, WPA/WPA2 con 802.1x, WPA/WPA2.
- Soporte de RADIUS.
- Soporte de EAP-TLS, EAP-TTLS, EAP-SIM, EAP-FAST, PEAP
- Soporte para detección y prevención de intrusiones de nueva generación estable.

ADMINISTRACIÓN Y MANTENIMIENTO
- Soporte de SNMPv1/v2/v3
- Soporte de CLI e interfaz gráfica.

Equipo PUNTOS DE ACCESO TIPO 1
Son equipos con desempeño para cubrir escenarios típicos de oficinas o espacios con menos de 30 usuarios concurrentes.

CAPACIDADES
- Soporte de 802.11a/b/g/n/ac.
- Soporte de MIMO de al menos 4x4
- Soportar al menos 16 SSID.
- Soportar alimentación PoE o PoE+.
- Debe poder operar en la banda de 2.4 GHz y en la banda de 5.0 GHz.
- Soportar dos puertos GE BaseT 10/100/1000.

FUNCIONALIDADES
- Contar con mecanismos de optimización de la interfaz aire, para mejorar la experiencia de los usuarios.

SEGURIDAD
- Soportar los siguientes métodos de autenticación: WPA, WPA2 (AES), 802.11i, 802.1x, IPSec, IKEv2, PKCS #10, X509 DER / PKCS#12, SSL, WPA/WPA2 Empresarial.
- Soporte para detección y prevención de intrusiones de nueva generación estable.

ADMINISTRACIÓN Y MANTENIMIENTO
- Soporte de gestión a través de línea de comando (CLI) o vía web.

Normas, Estándares y Protocolos para la controladora y los Puntos de Acceso:

- Exclusivo para Puntos de acceso: IEEE 802.11a, 802.11ac, 802.11b, 802.11g, 802.11n.
- IEEE 802.11a, 802.11ac, 802.11b, 802.11e, 802.11g, 802.11i, 802.11n para la controladora
- UL 60950–1 para la controladora
- FCC Part 15 para la controladora
- EN 55022 para la controladora
- CISPR 24 para la controladora

2.1.4 Manuales y Documentación

El Licitante deberá incluir copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada.

2.2 Servicio de Seguridad Perimetral

El servicio deberá incluir como mínimo los elementos de hardware, software y funcionalidades requeridas en el presente anexo técnico. Como referencia y para garantizar la operación del servicio de seguridad de red, EL PROVEEDOR deberá ofertar en su propuesta, soluciones en donde el fabricante esté ubicado y reconocido dentro de los cuadrantes de Gartner o en algún otro reporte reconocido por la industria a nivel internacional.
El licitante deberá incluir para el Servicio Administrado de Seguridad Perimetral deberá presentar una carta de fabricante membretada en la cual señale que cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante, firmada por la persona autorizada por el fabricante de la solución propuesta.

2.2.1 Servicio de Firewall/IPS/Filtrado de Contenido.

EL PROVEEDOR deberá incluir en su propuesta, todo el Licenciamiento, Hardware y Software necesario, para proporcionar de inicio, la totalidad de Servicios de Seguridad con funcionalidades asociadas de IPS, Filtrado de Contenido WEB que se requieran, conforme a los perfiles y cantidades indicadas para cada tipo de Firewall. Deberá soportar configuraciones en alta disponibilidad solo para el sitio de Mazaryk.

2.2.1.1 Funcionalidades de los equipos

I. Control de políticas

a) Permite a los usuarios configurar políticas de seguridad en función del tiempo, usuario / grupo de usuarios / grupo de seguridad, protocolo de capa de aplicación, ubicación geográfica, dirección IP, puerto, grupo de nombre de dominio, categoría de URL, tipo de acceso.
b) Deben de ser capaces de manejar protocolos tales como RADIUS o KERBEROS.

II. Enrutamiento

a) Admite rutas estáticas, enrutamiento basado en políticas y protocolos de enrutamiento dinámicos como OSPF, BGP en sus últimas versiones estables.
b) El enrutamiento basado en políticas admite las siguientes condiciones coincidentes: dirección IP de origen, dirección IP de destino, tipo de servicio, tipo de aplicación, usuario / grupo de usuarios / grupo de seguridad, interfaz de entrada y prioridad DSCP.

c) Opere con protocolos IPv4/IPv6.

III. Protocolos Avanzados de VPN

a) Especificaciones IKE
- i. Versión 1, Versión 2
- ii. Modo de Negociación: Automático, Main, Aggressive
- iii. Encriptación: AES-256, AES-128, 3DES, DES
- iv. Autenticación: via clave compartida o por certificado
- v. Integridad Hash: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5.
- vi. Grupo DH: 1,2,5,14,15,16,18,19,20,21

b) Especificaciones IPSec:
- i. Modo de encapsulación: Transport, Tunnel
- ii. Protocolo de seguridad: ESP, AH
- iii. ESP Encriptación: AES-GCM-128, AES-GCM-256, AES-256, AES-128, 3DES, DES
- iv. ESP Autenticación: DES, 3DES, AES-GCM-128 , AES-GCM-256.

c) GRE

d) VPN SSL

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

ii. Plataformas soportadas con cliente:
a. Android
b. Mac OS X
c. Windows

IV. Identificación de aplicaciones

a) El sistema deberá identificar, categorizar y controlar y visualizar tráfico de más de 7000 aplicaciones de manera granular por usuario, grupos de usuarios y, horarios.
b) La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.

V. IPv6

a). Soporta el protocolo IPv6.

VI. Control de tráfico

a). Admite políticas de control de tráfico basadas en el protocolo de la capa de aplicación, incluida la configuración del ancho de banda máximo, el ancho de banda garantizado y la prioridad del tráfico del protocolo.
b). Admite garantía de ancho de banda basada en usuarios y direcciones IP.
c). Admite el tráfico basado en la ubicación geográfica y el análisis de amenazas.

VII. Gestión de políticas

a). Admite el filtrado de URL.
b). Es compatible con SafeSearch para filtrar el contenido no saludable devuelto por los motores de búsqueda como Google.
d). Las reglas de firewall deberán poder tener vigencia con base a fechas (incluyendo día, mes y año).

VIII. NAT

a). Admite funciones NAT completas.

b). Hacer traslación de direcciones estático, uno a uno. Hacer traslación de direcciones dinámico, muchos a uno.

IX. Prevención de intrusiones y antivirus.

a). Admite la personalización de plantillas de políticas de prevención de intrusiones basadas en escenarios.
b). Admite el filtrado basado en nombres de dominio malintencionados para bloquear C&C.
c). Admite antivirus para protocolos como HTTP, FTP, SMTP, POP3, IMAP.
d). Soporte de detección y bloqueo de ataques.
e) Deberá contar con la funcionalidad de detección de anomalías y evasiones (AET - Técnicas Avanzadas de evasión) validadas como mínimo por NSS Labs
f) Deberá contar con la capacidad de identificar como mínimo 800 millones de técnicas avanzadas de evasión

X. Protección de seguridad de tráfico cifrado.

a). Descifra el tráfico HTTPS, POP3S, SMTPS e IMAPS y realiza filtrado de datos, auditoría y protección de seguridad en el tráfico descifrado.
b). Descifra el tráfico y lo refleja en dispositivos de terceros para auditoría y detección de seguridad.

XI. Gestión Centralizada.

a) Admite la actualización mediante una unidad flash USB para reducir los costos de O&M.
b) Soportar los protocolos SNMP, SNMPv2c o SNMPv3

XII. Selección de enlace ascendente inteligente

a) Selecciona de forma inteligente los enlaces del operador en función de las direcciones IP de destino, admite la configuración de la interfaz activa / en espera y el equilibrio de carga por porcentaje
b) Soportar QoS basada en colas inteligentes.
c) Deberá contar con conceptos de Alta Disponibilidad y Balanceo de Enlaces, y no deberá tener restricciones con respecto a la tecnología usada en la misma
d) Deberá contar con mínimo 2 métodos de balanceo, tipo RTT y Ratio
e) Deberá contar con conceptos de QoS (Calidad de Servicio) integrados al ambiente de SD-WAN
f) Deberá contar con conceptos de priorización y clasificación de tráfico integrados al ambiente de SD-WAN
g) Deberá contar con la capacidad de creación de gateways tanto standalone, así como en cluster, e insertarlos en el ambiente de SD-WAN

XIII. IPS

a) Deberá proveer control de acceso e inspección profunda del tráfico.
b) Debera ser capaz de detectar tecnicas de evasión (Fragmentación de paquetes, segmentación TCP, etc).
c) Capaz de reducir el número de falsos positivos.
d) Deberá ser capaz de realizar analisis de protocolos.
e) Deberá ser capaz de realizar la detección de anomalias estadisticas. (Ej. Basado en la secuencia de los eventos).
f) Deberá ser capaz de almacenar la captura de los paquetes para analisis posterior.

XIV. Filtrado de Contenido.

a) El acceso de los usuarios deberá de ser comparado con listas o categorias de URL´s.
b) Deberá de ser capaz de notificar al usuario por mensaje en el navegador.

Viaducto Presidente Miguel Alemán Valdés No. 81, Colonia Escandón 1 Sección, CP. 11800, Alcaldía Miguel Hidalgo, CDMX.
Tel: (55) 3002 6300 www.gob.mx/sectur

c) Deberá de ser capaz de configurar la opción de PROXY HTTP, permitiendo declarar el PROXY HTTP dentro del EndPoint y deberá de ser capaz de configurar la opción de PROXY HTTP de forma transparente y mediante PROXY explicito
d) La categorización de URL deberá de ser capaz de funcionar en IPv4 o IPv6.

2.2.1.2 Características Técnicas

Las funcionalidades y características antes descritas aplican para cada uno de los tipos de Firewall tipo 1 requeridos para los inmuebles de Viaducto y Schiller, tipo 2 para Mazaryk.

FIREWALL TIPO 1 – Sito Schiller y Vladucto

Las especificaciones son las mínimas más no limitativas.

INDICADOR	REQUISITO DE ESPECIFICACIÓN TÉCNICA
Requisitos de configuración física.	18,000 Túneles de VPN IPSec.
Requisitos de interfaces	12 Número maximo de puertos 4 Puertos 10/100/1000 base T GE.
Requisitos de desempeño	10 Gb Rendimiento Maximo de Firewall (Throughput). 1 Gb Rendimiento en inspección (UDP 1518 bytes) 150 Mbps Rendimiento inspección SSL. 50,000,000 Número de conexiones simultáneas. 35,000 Número de conexiones nuevas por segundo. 1 Gbps IPsec VPN Throughput (AES-GCM-256). 18,000 Número máximo de IPSec túneles (site to site). 5,000 Número máximo de IPSec túneles (client to site).
VLANs	1024

FIREWALL TIPO 2 – Sito Central Mazarik (en HA)

Las especificaciones son las mínimas más no limitativas en modo cluster (HA) para el sitio de Mazaryk.

INDICADOR	REQUISITO DE ESPECIFICACIÓN TÉCNICA
Requisitos de configuración física.	18,000 Túneles de VPN IPSec.
Requisitos de interfaces	12 Número maximo de puertos 4 Puertos 10/100/1000 base T GE.
Requisitos de desempeño	20 Gbps Rendimiento Maximo de Firewall (Throughput). 3 Gbps Rendimiento en inspección (UDP 1518 bytes) 350 Mbps Rendimiento inspección SSL. 80,000,000 Número de conexiones simultáneas. 100,000 Número de conexiones nuevas por segundo. 2.5 Gbps IPsec VPN Throughput (AES-GCM-256). ≥ 18,000 Número máximo de IPSec túneles (site to site). ≥ 5,000 Número máximo de IPSec túneles (client to site).
VLANs	1024

2.2.1.4 Manuales y Documentación

El licitante deberá incluir para el Servicio de Protección Perimetral una carta de fabricante membretada en la cual señale que cuenta con la autorización de venta, reventa, distribución o

comercialización de los productos del fabricante, firmada por la persona autorizada por el fabricante de la solución propuesta.

.

El licitante deberá incluir para el servicio de Firewall al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada.

2.2.2 Servicio de AntiSpam

La SECTUR cuenta con el servicio de correo electrónico para 1600 usuarios, con 2 servidores centralizados, en los que se concentra la entrada de todos los correos. El servicio consta de 2 sistemas de Filtrado de Contenido vía SMTP CON ANTISPAM y Antivirus para el sistema de correo de forma perimetral en appliance en esquema Activo - Activo. Incluyendo el mantenimiento del hardware y licenciamiento que se alojaran en el sitio de Mazaryk.
Se requiere que el Sistema con Antispam y Antivirus para el Sistema de Correo de forma perimetral realice el análisis de todo el correo entrante y saliente de la organización. Es obligación de los licitantes dimensionar todos los elementos requeridos para cumplir con las capacidades operativas de la secretaria a partir de la información contenida en el presente anexo técnico.
Sera responsabilidad del licitante migrar las cuentas de correo en caso de ser necesario a la solución de ANTISPAM propuesta.

2.2.2.1 Funcionalidades de los equipos

El licitante deberá considerar que para prestar el servicio deberá proporcionar el equipamiento necesario, así como la instalación, configuración, puesta en marcha; así como el mantenimiento de los mismos durante la vigencia del contrato, en el entendido de que todos los equipos o equipo requeridos formarán parte del servicio ofrecido por parte del licitante y que la convocante no adquirirá ninguno de los mismos.

La solución anti-spam debe ser basada en un servicio (usando un dispositivo de hardware, totalmente administrable de forma remota por el licitante ganador y que radique físicamente en las instalaciones de la SECTUR el cual deberá estar configurado en Alta Disponibilidad.

2.2.2.2 Características Técnicas

Funciones sobre las cuales debe trabajar la solución:

- Filtrado de Anti-Spam en correo.
- Filtrado de Anti-Virus en correo.
- Hacer reglas por IP, dominio, usuarios y extensión de anexos o cualquier cadena de texto en un mensaje de correo.
- Reglas basadas en formato MIME.
- Reglas basadas en listas de bloqueo o de no-bloqueo, por IP, dominio, o remitente.
- Creación de cuarentenas o carpetas de auditoría de correo en base a reglas del Antispam de correo. Mismas que deberán ser reciclables a intervalos de tiempo determinado por la SECTUR.

Viaducto Presidente Miguel Alemán Valdés No. 81, Colonia Escandón 1 Sección, CP. 11800, Alcaldía Miguel Hidalgo, CDMX.
Tel: (55) 3002 6300 www.gob.mx/sectur

- Creación de listas negras o blancas independientes por usuario, accesibles por los mismos vía Web.
- Creación de políticas a nivel global por grupos o por usuario.
- Envío de mensajes de aviso de correo en cuarentena, personalizado a los usuarios, donde éstos puedan decidir qué hacer con su propia cuarentena.
- Sistema de respaldo de configuración de la solución.
- Protección anti-relay para correo de entrada o de salida.
- Sistema de revisión de mensajes en cuarentena basada en queries, por remitente, asunto, destinatario o IP, para su consulta, que permita revisar adjuntos y cuerpos de mensaje, en formato texto y html.
- Sistema de revisión de log´s de entrada y salida de tráfico de correo que permita realizar búsqueda de palabras, para su rápida consulta.
- Sistema de análisis de correo no entregado temporalmente o en cola de salida.
- Sistema de análisis de tipos de archivos para uso y creación de formatos MIME.
- Sistema de calificación de spam, que permita determinar que calificación corresponde al correo spam y cual al correo no-spam.
- Administración vía Web con manejo de contraseñas que puedan determinar el nivel o jerarquía de acceso para administración y/o consulta para diversos tipos de usuarios.

2.2.2.4 Manuales y Documentación

Deberá incluir para la solución de Antispam al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada.

2.3 Servicio de Protección de Usuario Final

Debido al avance de los ataques informáticos y de las mejores prácticas de seguridad, es necesario contar con una herramienta de detección, contención y respuesta de los puntos finales, recolectando, inspeccionando y centralizando la información importante que sucede en tiempo real, de tal forma que en el momento o incluso posterior a un ataque informático se pueda investigar, prevenir, contener y responder con la mayor información posible, por lo que "LA SECTUR", tiene la necesidad de proteger la información y fortalecer las zonas de riesgo de la infraestructura conectada en red que utilice servicios educativos. A la fecha se han venido incrementando los ataques de red, los cuales afectan vulnerabilidades de sistemas operativos, plataformas de desarrollo, versiones de sistemas, de negación de servicio o sobre escaneo de puertos y debilidades de sistemas y aplicaciones, fueron contenidos por la seguridad perimetral.

2.3.1 Funcionalidades de los equipos

Así mismo, dentro de la propuesta se deberá contemplar una solución de software antivirus para un número de máquinas de 1150 equipos.

2.3.2 Características Técnicas

- Protección para estaciones, dispositivos móviles y servidores contra todo tipo de amenazas de Internet: virus, gusanos, troyanos, phishing y spam en todas capas de la red.
- Análisis de todos los mensajes transmitidos a través de los servidores de correo.

- Procesamiento de mensajes, bases de datos y otros objetos en los servidores de correo / Domino
- Protección contra ataques phishing y spam.
- Bloqueo de correo masivo (spam) y epidemias virales
- Escalabilidad
- Instalación y administración centralizadas
- Protección proactiva contra programas desconocidos
- Seguridad al trabajar en redes WiFi
- Escaneado al vuelo de tráfico del correo e Internet.
- Reversión de cualquier cambio malicioso realizado en el sistema
- Redistribución inteligente de recursos durante el escaneado completo del sistema
- Puesta en cuarentena de objetos infectados y sospechosos
- Sistema para informes sobre el estado del sistema
- Actualización automática de las bases de datos.
- Compatible con cualquier sistema operativo, Estaciones de trabajo: (incluyendo 64bit) y Linux, Dispositivos móviles, Servidores de archivos: Microsoft Windows (incluyendo 64bit), y Linux, Servidores de correo y servidores para grupos: Microsoft Domino, Linux (Sendmail, Qmail, PostfixyExim).

2.3.4 Manuales y Documentación

Deberá incluir para la solución de Antivirus una carta de fabricante membretada en la cual señale que cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante, firmada por la persona autorizada por el fabricante de la solución propuesta.

.

Deberá incluir para la solución de Antivirus al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada.

2.4 Servicio Administrado de Respaldos

Los servidores y equipos de cómputo de los cuales se requiere el respaldo de información se encuentran ubicados en diferentes redes sin ningún dominio y se requiere que el licitante suministre todos los elementos físicos y lógicos para la implementación de un sistema de respaldo central que realice sus actividades de manera desatendida y programada.

2.4.1 Funcionalidades de los equipos

Los servidores de los cuales se requiere el respaldo de información se encuentran ubicados en el Centro de Datos y se requiere que el licitante suministre todos los elementos físicos y lógicos para la implementación de un sistema de respaldo central que realice sus actividades de manera desatendida y programada.

Generalidades de los respaldos:

Permita respaldo de sistemas operativos Windows Server 2008 en adelante y Linux Server de las distribuiciones de CentOS, Debian, Ubuntu y RedHat en entorno físico y virtual sobre Hyper-V y Vmware.
Soporte respaldos/recuperación en unidades de cinta Overland y NAS.
Opere con de duplicación y compresión.
Opera con catálogo y base de datos central.
Opere con consola central de administración.
Opera con integración a Directorio Activo de Microsoft.
Permita recuperación de sistemas de archivos completos basados en fecha de respaldo.
Permita la recuperación granular de archivos basados en fecha de respaldo.
Opere mediante esquemas de políticas de respaldo.
Opere realizando respaldos completos, incrementales o diferenciales.
Opera en base a agentes de respaldos/recuperación.
Cuente con licencia para respaldar 20 TB comprimidos.
Deberá soportar tamaños de bloque mínimos de 4 kb y deberá permitir seleccionar el tamaño de bloque deseado
Respaldo simultáneo de servidores en operación sin afectar la operación de las aplicaciones y servicios del servidor.

Se requiere que los sábados a las 20:00 horas o cuando se acuerde con la SECTUR se programe la realización de respaldos, del total de la información contenida en los servidores relacionados en este inciso cuyo volumen es de 20 TB comprimidos, sin la intervención manual de un administrador a menos que ocurra alguna contingencia extraordinaria. La información deberá respaldarse simultáneamente de todos los servidores sin bajar ninguno de los servicios (on-line) y con usuarios haciendo uso de aplicaciones durante el proceso de respaldo. El licitante deberá suministrar, instalar y poner a punto todos los agentes necesarios para que el respaldo se efectúe satisfactoriamente.
Se requiere que todos los días a partir de las 23:00 horas o cuando se acuerde con la SECTUR se efectúen respaldos incrementales o diferenciales, comprimidos, de manera automática sin la intervención manual de un administrador, a menos que ocurra alguna contingencia y la solución deberá soportar una capacidad ilimitada de agentes. La información deberá respaldarse simultáneamente de todos los servidores sin bajar ninguno de los servicios (on-line) y con usuarios haciendo uso de aplicaciones durante el proceso de respaldo.
El agente debe permitir al administrador la recuperación de un archivo ubicado en la unidad de respaldo del mismo equipo por fecha de respaldo.

Entre la información que al menos se debe reportar al administrador a través de las vías de la consola de alertamiento, se debe informar el resultado del respaldo, si fue realizado satisfactoriamente y el tiempo en que fue realizado o en su caso los problemas que se presentaron, la cantidad de bytes que se transmitieron y el servidor o equipo del usuario que lo efectúo.
En la consola de administración instalada en el servidor de respaldo suministrado se debe habilitar un servicio de Web para la administración del respaldo y restauración de la información vía html, para que el administrador de la red pueda administrar sus respaldos y recuperar su información vía internet.
El licitante deberá suministrar, instalar y poner a punto todos los agentes necesarios para que el respaldo se efectúe satisfactoriamente.

Además del respaldo a los servidores descritos, el licitante dará respaldo a los servidores que le indique la SECTUR, siempre que en su conjunto no rebase la cantidad de 20 TB de respaldo de diferentes sistemas operativos y plataformas.

Adicional SECTUR solicita que en la propuesta del Licitante se incluya una unidad de almacenamiento exclusiva para los respaldos.

2.4.2 Características Técnicas

El sistema de Respaldos deberá cumplir con las capacidades siguientes:

- Proteger diversos tipos de nodos de origen, incluyendo el nodo basado en el agente, el nodo sin agentes, CIFS, Exchange Online, SharePoint Online, OneDrive, etc.
- Realiza la copia de seguridad de datos en servidores de punto de recuperación.
- Replica datos de copia de seguridad en servidores de puntos de recuperación remotos y locales.
- Archiva datos.
- **Copia:**
  - Archivos de origen seleccionados a una ubicación de la copia de seguridad secundaria.
  - Puntos de recuperación a ubicaciones de la nube y locales como la carpeta de recursos compartidos
- **Crea**
  - Máquinas de Virtual Standby a partir de datos de copia de seguridad en el hipervisor local Hyper-V y Vsphere.
  - Máquina virtual instantánea en el hipervisor local Hyper-V o VSphere.
- **Restaura**
  - Datos de copia de seguridad y realiza una reconstrucción completa.
  - Objetos de correo electrónico y objetos que no lo son de Microsoft Exchange mediante la utilidad Restauración Granular de Exchange.
- **Es compatible con**
  - La administración basada en roles
  - La instantánea de hardware
  - Prueba de recuperación asegurada para los puntos de recuperación.

Para la Unidad de respaldo el Licitante debe contemplar una solución de almacenamiento NAS, dispositivo de almacenamiento conectado a la red LAN.

- En este sistema de almacenamiento NAS se hará el respaldo de todos los servidores físicos o virtuales de la SECTUR Las características técnicas mínimas de la unidad de almacenamiento NAS son:
  I. Capacidad de 64 TB útiles en Raid 5 para el inmueble de Masaryk.
  II. Memoria interna de 2 GB DDR3L, con posibilidad de expansión hasta 16 GB.
  III. Al menos 2 interfaces de red de 1 Gbps conector RJ-45.
  IV. Al menos 1 Puerto USB 3.0.
  V. Soporte de hasta 4 discos internos de SSD/HDD SATA de 2.5" o 3.5 ".
  VI. RAID 0, 1, 5, 6 y 10.
  VII. Protocolos de servicio: CIFS/SMB, AFP, NFS, HTTP y HTTPS y FTPS.

VIII. Integración con Directorio Activo
IX. Soporte de virtualización con VMware Sphere, Hyper-V, Citrix, OpenStack
X. Consola de administración en idioma español
XI. Gestión de Almacenamiento:
   a. Tamaño máximo de volumen individual: 108TB
   b. Número máximo de volúmenes internos: 512
   c. Máximo de iSCSI Target: 32
   d. Máximo de iSCSI LUN: 256
   e. Compatibilidad con clon/instantánea de iSCSI LUN
XII. Software y licencia de administración y operación integrada al hardware.

2.4.4 Manuales y Documentación

Deberá incluir para la solución de Respaldos una carta de fabricante membretada en la cual señale que cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante, firmada por la persona autorizada por el fabricante de la solución propuesta.

Deberá incluir para la solución de Respaldos al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada.

2.5 Servicio de Infraestructura de Servidores

La SECTUR tiene la necesidad de la adquisición o arrendamiento de servidores tipo gabinete o enclosure de servidores (Blade), para dar soporte a los distintos servidores de aplicaciones internas y externas de la SECTUR

Deberá cumplir con las especificaciones siguientes:

Servidor tipo Blade

La solucion de servidores tipo Blade deberá contar con 10 servidores tipo blade con las siguientes características:

DESCRIPCIÓN	GABINETE O ENCLOSURE DE SERVIDORES TIPO BLADE
Características mínimas	EL PROVEEDOR de la infraestructura de servidores tipo blade deberá de considerar el gabinete o enclosure para este tipo de servidores con las siguientes características mínimas: Gabinete o enclosure que soporte o aloje servidores tipo navaja o blade con mínimo 16 bahías para el alojamiento de 10 de los servidores. Para montaje en rack standard de 19" Sistema de chasis de al menos 10 unidades de rack Debe de incluir mínimo 1 módulos de administración de todos los elementos incluidos en el gabinete o enclosure.

Viaducto Presidente Miguel Alemán Valdés No. 81, Colonia Escandón 1 Sección, CP. 11800, Alcaldía Miguel Hidalgo, CDMX.
Tel: (55) 3002 6300 www.gob.mx/sectur

	Al menos 1 puerto de video que permita la conexión de un monitor para la administración local y remota del gabinete o enclosure. Bahías o slots para la instalación de elementos de conexión a red de datos redundantes con mínimo 2 puertos de conectividad Ethernet 10GB Ethernet.
Bahías o slots	Mínimo 10 bahías para servidores blade o nodos utilizables. Capacidad de integración hot swap de los servidores o nodos. Soportar procesadores E5-2697 v3. Se debe considerar que los Slots deben contar con la siguiente capacidad en memorias RAM como mínimo: Slot 1: 192Gb Slot 2: 512 Gb Slot 3: 512 Gb Slot 4: 256 Gb Slot 5: 256 Gb Slot 6: 192 Gb Slot 7: 512 Gb Slot 8: 512 Gb Slot 9: 256 Gb Slot 10: 64 Gb Soportar virtualización con Hiper-V y VSphere. Soportar al menos 500 GB de disco duro en configuración RAID, con almacenamiento en SAN.
Fuentes de poder	Incluir la mínima cantidad de fuentes de poder soportadas con redundancia, necesarias para que el chasis opere en su carga de trabajo total, es decir, todos los servidores y opciones de conectividad instaladas. Redundancia de fuentes de poder N+1. Tecnología Hot Swap.
Módulo de gestión y administración	Botón de encendido. Gestión centralizada de todos los servidores Blade o nodos. Herramientas de gestión y administración centralizada con interfaz gráfica y acceso remoto. Debe de contar con software de administración remota embebido y con un puerto de red dedicado que permita contar con el monitoreo de los elementos de hardware, firmware; así como el manejo de alertas que emita el sistema.
Ventiladores	Incluir la mínima cantidad de ventiladores soportada con redundancia que permita que el chasis opere en su carga total de trabajo y enfriamiento para todos los servidores Blade o nodos. Redundancia de fuentes de poder N+1. Tecnología Hot Swap.
Módulos o slots para conectividad LAN	Incluir dos módulos o slots exclusivos para la interconexión LAN del chasis Cada módulo debe de ser escalable, de alto desempeño y baja latencia 1/10GB Ethernet. Todos los puertos internos y externos deben de estar licenciados y habilitados para su uso. Desempeño de al menos 110 Tbps. Debe de incluir la instalación y configuración de los equipos en el chasis.

Módulos de interconexión para conectividad de almacenamiento SAN	Incluir mínimo 2 módulos exclusivos para la interconexión SAN del chasis. Los puertos deberán de operar entre 8 Gbps a 16 Gbps. Todos los puertos internos y externos deberán de estar licenciados y habilitados para su uso. Deberá de incluir la instalación y configuración de los equipos en el chasis.
Sistema de almacenamiento.	Incluir sistema de almacenamiento con capacidad de: 60 TB usables configurados en RAID 6. La conectividad será mediante cables de fibra óptica redundante. Soporte comunicación por canal de fibra e iSCSI. Ventiladores redundantes HotSwap. Permita operar esquemas de Thin y Think provisioning. Compatible con sistemas operativos Windows Server 2008 en adelante. Compatible con sistemas operativos Linux Centos, Debiam, Ubuntu y RedHat. Todos los puertos internos y externos deberán de estar licenciados y habilitados para su uso. Deberá de incluir la instalación y configuración de los equipos. Debe incluir todos los insumos de instalación necesarios y para la interconexión del sistema NAS vía Red.

El licitante deberá considerar licenciamiento para hipervisor VMware VSphere 7X y el VCenter correspondiente para 4 servidores blade como parte del servicio para la solución de Blades y el servidor donde se albergara dicha licencia de virtualización.

Servidores Tipo Microserver

La Secretaria requiere 4 servidores tipo Microserver con las siguientes características:

- Procesador: Xeon Quad Core 3.40 GHz o superior
- Memoria RAM: 16 GB
- Disco Duro: 1 TB

La Secretaria requiere 3 servidores tipo Torre con las siguientes características:

- Procesamiento: Un procesador físico con 8 núcleos y 3 GHz. no mayor a dos años de liberación de la serie por parte del fabricante.
- Memoria RAM física: 64 GB.
- Sistema de disco en RAID 5 con capacidad 2 TB.
- Red: 2 tarjetas para RJ-45 de 1 GB de ancho de banda.
- Alimentación eléctrica: Una fuente para voltajes 110/220 autosence con nema estándar nacional.

Así mismo, el proveedor deberá de proveer el mantenimiento correctivo a los servidores propiedad de la SECTUR

1. Servidor marca DELL propiedad de la SECTUR:
Marca: DELL

Modelo: PowerEdge R640
Etiqueta de servicio: HGDW8N2.

2. Servidor marca HP propiedad de la SECTUR:
   Marca: HP
   Modelo: Proliant 360 Gen10.

El licitante deberá tener la solución de servidores tipo Blade lista y funcionando a partir del 16 de marzo de 2023.

2.5.4 Manuales y Documentación

Incluye: instalación, configuración, puesta a punto e integración con los equipos de las otras partidas, realizando lo siguiente: armado de opciones y montaje en el chassis, actualización de Firmware de todos los componentes de hardware, definición de puertos de NAS y LAN, configuración del módulo de administración remota.

2.7 Servicio de Monitoreo de red y Mesa de Ayuda

2.7.1 Monitoreo de red

El licitante deberá proporcionar una solución de monitoreo que permita alertar en tiempo real los dispositivos, tanto aplicaciones como recursos de la red de la SECTUR. Este monitoreo lo deberá operar e instalar en la red de la institución con la finalidad de mantener la operación 7x24. El monitoreo deberá comprender en ese horario de servicio a través de un centro de monitoreo del licitante, enlazándose mediante un método seguro, VPN sitio a sitio o enlace dedicado.
La SECTUR entregará durante los primeros 10 días, después de la firma del contrato, un inventario de aplicaciones, servidores, switches, ruteadores y dispositivos que necesiten ser monitoreados, a partir de esta entrega el licitante contará con 5 días naturales para la implementación de la solución de monitoreo.

2.7.1.1 Funcionalidad:

- La solución de monitoreo deberá considerar al menos 200 monitores, donde los monitores o probes, son los servidores, switches, routers y aplicaciones de la institución.
- Se deberá entregar la administración del rendimiento o performance o detección 7x24.
- El licitante deberá desarrollar al menos 3 tableros ejecutivos que proporcionen una vista de negocio ejecutivo, una vista operativa y una de capacidad.
- Se deberá detectar eventos de seguridad en la red

2.7.1.2 Infraestructura necesaria

- El licitante deberá proporcionar el sistema de monitoreo tanto de software y hardware para que se aloje en SECTUR en el sitio de Mazaryk.
- El licitante deberá contar con un centro de monitoreo formalmente establecido y con certificaciones ISO27001 e ISO 20000-1, el centro de monitoreo deberá detectar, validar y notificar los eventos de red que sucedan 7x24 en la institución.
- El licitante deberá proporcionar al menos 2 pantallas planas de plasma o LCD con el servicio de al menos 32 pulgadas y su respectiva tarjeta controladora con el dispositivo que emita la señal.

- Contar con línea de atención telefónica con atención 7x24 durante la vigencia del contrato
- Deberá contar con un área exclusiva para el SOC la cual deberá ser independiente de las demás áreas que integran las instalaciones del licitante.
- Contará con controles de acceso biométrico.
- Contará con sistemas de respaldo de energía, sistemas contra incendios, sistemas de video vigilancia y CCTV.
- Contará con enlaces redundantes de internet para garantizar la continuidad del servicio.

2.7.1.3 Notificación y Escalamiento

- El licitante deberá notificar las alertas del sistema de monitoreo a través de alguno de los siguientes medios: correo electrónico, teléfono celular, oficina o envío de SMS durante el presente contrato.
- El escalamiento se deberá revisar al menos cada 3 meses.

2.7.1.4 Especificaciones Técnicas

- El sistema de monitoreo debe estar basado en una arquitectura inteligente que se compone de visualizaciones interactivas que tienen como objetivo proyectar el estatus en tiempo real de la infraestructura de la red y de las aplicaciones críticas y debe cumplir las siguientes características:
- Sistema de información en base a tableros de control (DashBoard).
- Tableros de control operativos que muestran la comunicación visual efectiva y precisa de los datos de las aplicaciones en tiempo real.
- Tableros de control ejecutivos que muestran la disponibilidad de las aplicaciones de la organización en tiempo real.
- Los tableros de control deben almacenar y desplegar la información histórica para conocer las tendencias e indicadores para la toma de decisiones.
- El sistema debe estar desarrollado en Web 2.0 o Superior
- La extracción de información de los dispositivos y aplicaciones que se despliega en los tableros de control se debe realizar a través de SNMP, trap de SNMP, XML, HTML o bases de datos SQL, MySQL u Oracle.
- La extracción de información de dispositivos y aplicaciones debe no debe ser intrusivo, es decir no debe instalarse algún agente.
- La agrupación de Tableros de control debe ser de acuerdo a las aplicaciones o cadenas de servicios en base a la infraestructura.
- Monitoreo de aplicaciones a través de transacciones
- Realización de asociaciones de dispositivos de red
- Realización de guías de aplicativo de los servicios.
- Debe desplegar la disponibilidad de servicios (el tiempo en el que está disponible el sistema o dispositivo).
- Debe desplegar el tiempo de respuesta del sistema o dispositivo hacia el usuario final.
- Debe desplegar el tiempo de respuesta de una transacción de punta a punta.
- Debe desplegar la capacidad del sistema o dispositivo para ejecutar los procesos o las tareas programadas, considerando parámetros como la utilización de disco duro, memoria física, procesador o CPU.

- Debe desplegar el porcentaje de utilización de ancho de banda de enlaces principales dentro de la red como son: Switch Core, Router, Puertos de Switch, Wireless.
- El tablero principal debe ser diseñado estructuralmente para que despliega los elementos productivos de la red desde las aplicaciones, telecomunicaciones y hasta el usuario final.
- Interacción con los indicadores de niveles de servicio en tiempo real.
- Procesamiento analítico en línea de los indicadores de niveles de servicio.
- Presentar tableros sobre actividad sobre la red de acuerdo con puertos, categoría, direcciones IP orígenes y destinos, país.
- Debe detectar actividades sospechas sobre la red y alertar sobre las mismas.
- Deberá contar con listas de amenazas que se integren al monitoreo para poder realizar análisis y detección, debe incluir al menos las siguientes listas de amenazas: direcciones IP, malware, botnet, dominios, spam, hash, URL´s y redes TOR.
- Priorizar eventos de red en base a criticidad
- Analizar bitácoras de los dispositivos de seguridad en tiempo real
- Monitoreo 7x24
    - Centro de operaciones que realiza las notificaciones de las incidencias que afectan a la infraestructura (Seguridad, Aplicativos, Telecomunicaciones) en base a un escalamiento operativo e informativo
    - Sistema de ticket para el registro de control de cambios o mantenimiento a los sistemas y dispositivos.
    - Notificación de incidencias vía telefónica, correo electrónico y vía SMS
    - Reportes de disponibilidad de servicios semanales, mensuales y bimestrales.
    - Monitoreo de disponibilidad de servicios desde internet
    - Monitoreo de disponibilidad de servicios vía VPN

2.7.2 MESA DE AYUDA

El licitante deberá proporcionar un servicio de mesa de ayuda para recibir, dar seguimiento, resolver y cerrar tickets de las solicitudes de servicio, incidentes, monitoreo de seguridad y monitoreo de red que se contemplan en el servicio. Este servicio deberá operar en modalidad 7x24 durante la vigencia del contrato.
La SECTUR entregará durante los primeros 10 días, después de la firma del contrato, una lista de personal autorizado para el contacto con la mesa de ayuda del licitante ganador.

2.7.2.1 Funcionalidad:

- Disponibilidad de la mesa de ayuda en modelo 7 x 24 (las 24 horas del día, los 7 días de la semana, durante la vigencia del contrato).
- El licitante realizará el soporte técnico a través de su Mesa de ayuda para la atención de reportes y fallas, en sitio o remoto conforme a su estrategia, para cumplir con los requerimientos de Nivel de Servicio.
- El licitante deberá generar un número de ticket o número de reporte único por cada reporte que se reciba en la mesa de servicio con la finalidad de llevar un control adecuado de los tiempos de solución.
- Gestionar el control de cambios, atendiendo un proceso certificado por ISO 20000-1 o ITIL.

- Gestión de los tickets mediante en la mesa de servicios certificada en ISO 20000-1 o ITIL para atender las solicitudes realizadas por el personal autorizado por la SECTUR

2.7.2.2 Infraestructura necesaria

- El licitante deberá contar con un sistema de recepción y seguimiento de tickets
- Contar con línea de atención telefónica con atención 7x24 durante la vigencia del contrato
- El licitante deberá contar con medios de comunicación para reportar fallas de equipo (Mesa de ayuda). Los medios para reportar fallas, al menos deberán ser un número convencional, un celular y un correo electrónico.

2.7.2.3 Notificación y Escalamiento

- El licitante deberá notificar el seguimiento de los tickets mediante correo electrónico a los contactos involucrados.
- El escalamiento se deberá revisar al menos cada 3 meses.

2.7.2.4 Especificaciones Técnicas

- El licitante realizará el soporte técnico a través de su Mesa de ayuda para la atención de reportes y fallas, en sitio o remoto conforme a su estrategia, para cumplir con los requerimientos de Nivel de Servicio.
- Se requiere de la administración y operación de una mesa de servicios que proporcione los servicios de soporte de primer, segundo y tercer nivel para los servicios
- La mesa de servicios deberá operar siguiendo el marco de referencia ITIL, para lo cual el licitante deberá presentar el certificado de al menos 6 ingenieros certificados en ITIL versión 4.
- Los problemas que se cataloguen como de primer nivel serán resueltos directamente con el personal de la mesa de servicios con apoyo de la base de conocimientos con que cuente el licitante.
- En la atención del primer nivel de soporte si no tiene registro en su base de conocimiento, deberá invariablemente canalizar el soporte a un técnico especializado en el tipo de problema o falla presentada.
- Los problemas que se cataloguen como de segundo nivel serán atendidos por personal especializado del licitante directamente del fabricante del hardware o software dependiendo de la naturaleza del problema reportado.
- Las tareas mínimas que realizará la mesa de servicio son: Recibir solicitud, abrir el ticket, registrar detalle del incidente, analizar la falla o evento, canalizar al soporte técnico interno, escalar en su caso el incidente, dar seguimiento, informar de la solución empleada y cerrar el ticket del incidente.

La información que debe contener una solicitud de falla o evento es:

- Número de ticket.
- Fecha y hora de apertura del ticket.
- Fecha y hora de inicio de reporte de la falla.
- Nombre completo de quien levanta el reporte.
- Nombre completo de la persona que atienda el ticket.
- Vía de notificación de la falla o evento (correo electrónico o telefónico).
- Datos del equipo o servicio afectado.

- Detalle de la falla reportada.
- Diagnóstico de la falla.
- Solución empleada o implementada.
- Fecha y hora de cierre del ticket.

- La mesa de servicios deberá invariablemente por cada ticket abierto, enviar un correo electrónico a las cuentas especificadas por el administrador del contrato detallando la apertura del ticket y los correos posteriores necesarios para el seguimiento y cierre del mismo.
- El licitante deberá generar un número de ticket o número de reporte único por cada reporte que se reciba en la mesa de servicio con la finalidad de llevar un control adecuado de los tiempos de solución.
- De manera mensual. El licitante deberá de entregar estadísticas de desempeño de servicio comparadas con los Niveles de Servicio y Niveles de Disponibilidad especificados. Las diferencias significativas serán registradas e informadas, indicando las causas de los desvíos. El reporte especificará acciones correctivas para restaurar el desempeño del servicio a los niveles comprometidos.

Escaneo de Vulnerabilidades y certificados digitales

El licitante a través del Centro de Operaciones de Seguridad ejecutará escaneos de vulnerabilidades de sus sitios web públicos, para el cumplimiento con los estatutos del Gobierno Digital de acuerdo a lo requerido por SECTUR.

Se requieren 5 escaneos de vulnerabilidades semestralmente para 5 FQDN´s, SECTUR decidirá a que aplicaciones se deberá aplicar dicho escaneo

La solución de escaneó de vulnerabilidades deberá ayudar a Sectur a identificar, evaluar y mitigar automáticamente los riesgos de seguridad de las aplicaciones web, incluidos los categorizados por el Proyecto de seguridad de aplicaciones web abiertas (OWASP), como Inyección de SQL, Secuencias de comandos entre sitios (XSS), Falsificación de solicitudes entre sitios (CSRF) y otros.

Debe ser una herramienta no invasiva, basada en la nube, sin impacto en las operaciones de los sitios Web de Sectur.

Deberá poder escanear cualquier aplicación web que sea de acceso público, independientemente de dónde esté alojada, incluso en las instalaciones, ubicación conjunta o en un servidor de nube pública. Las aplicaciones web pueden analizarse independientemente de si están detrás de un firewall o un equilibrador de carga.

La herramienta de vulnerabilidades no deberá recopilar ninguna información de identificación personal (PII) o registros de la base de datos de la aplicación, independientemente de si esta información es de acceso público. No debe recoger ningún dato que pueda verse comprometido. Solo deberá alertar del problema.

Al detectar vulnerabilidades, se deberá generar automáticamente un informe detallado que permita identificar, evaluar y mitigar las vulnerabilidades de las aplicaciones web. Durante el análisis, se deberá recopilar información sobre la aplicación para aumentar la precisión y encontrar vulnerabilidades, incluidos datos sobre las tecnologías y los componentes que utiliza la aplicación, la estructura de la aplicación, así como listas de formularios, campos y cookies de páginas.

Viaducto Presidente Miguel Alemán Valdés No. 81, Colonia Escandón 1 Sección, CP. 11800, Alcaldía Miguel Hidalgo, CDMX.
Tel: (55) 3002 6300 www.gob.mx/sectur

Los escaneos se deberán ejecutar a una velocidad razonable, para no sobrecargar el servidor web o infraestructura de red.
Los reportes de la solución deberán presentar un resumen ejecutivo, donde presente un vistazo rápido a su nivel de riesgo basado en las vulnerabilidades descubiertas en el sitio web de su aplicación, incluido un desglose por nivel de gravedad.
Cumplimiento de Normas, esta sección del reporte muestra si cumple con los requisitos para cumplir con varias medidas de cumplimiento estándares de la industria, que incluyen:

- OWASP Top 10 – Open Web Application Security
- PCI DSS – Payment Card Industry Data Security Standard
- HIPAA – The Health Insurance Portability and Accountability Act of 1996

En el reporte a detalle deberá contener:

- Nombre de la vulnerabilidad: el nombre oficial de cada vulnerabilidad se lista para cada sección numerada
- CVSS: puntuación y vector del sistema de puntuación de vulnerabilidad común de la base de datos de vulnerabilidad nacional.
- Recomendaciones de remediación: describe brevemente los métodos mediante los cuales puede mitigar esta vulnerabilidad en su sistema
- La ruta en su servidor web donde se localizó la vulnerabilidad.
- La severidad de la vulnerabilidad. Se podrá cambiar este valor, según la percepción que tenga Sectur de la gravedad.
- Confianza, probabilidad de que su sitio web tenga esta vulnerabilidad
- Detalle del problema, descripción de cómo el escáner detectó la vulnerabilidad.

2.8.1 CERTIFICADOS DIGITALES

El licitante a través de su Centro de Operaciones de seguridad entregara los certificados digitales SSL que SECTUR requiere para sus sitios web Certificados digitales SSL, se requieren al menos 10 certificados SSL, los dominios de dichos certificados serán provistos por SECTUR de acuerdo a sus necesidades y el tamaño mínimo de clave pública tendrá que ser de acuerdo a la recomendación emitida por el ente certificador.
Adicionalmente se requiere 1 certificado wildcard para el dominio sectur.gob.mx.
Dichos certificados deberán de brindar seguridad al visitante de nuestras páginas web, debe ser una manera de decirles a nuestros usuarios que el sitio es auténtico, real y confiable para ingresar datos personales. Las siglas SSL responden a los términos en inglés (Secure Socket Layer), el cual es un protocolo de seguridad que hace que sus datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario web, y en retroalimentación, es totalmente cifrada o encriptada.
Al tener un certificado SSL confiable, nuestros datos están encriptados, con lo que podremos asegurar que nadie puede leer su contenido. Todo esto nos lleva a entender que la tecnología que brinda un certificado SSL es la transmisión segura de información a través de internet, y así confirmar que los datos están libres de personas no deseadas.
Dichos certificados SSL deben consistir en una clave pública y una clave privada. La clave pública se utilizará para cifrar la información y la privada para descifrarla. Cuando un navegador Web se dirige a uno de nuestros dominios asegurado, una presentación SSL autentica al servidor (sitio

Web) y al cliente (navegador Web). Con este método de cifrado se establece una clave de sesión exclusiva y posibilita el inicio de una transmisión segura.

2.9 Soporte a SITE, cuartos de comunicaciones y Cableado Estructurado

El licitante deberá otorgar a la SECTUR el servicio de protección al SITE y a dos cuartos de comunicaciones de la SECTUR, implementando la chapa electrónica y cámaras de video en el SITE y cuartos de comunicaciones. El sistema de control de acceso para el SITE y cuartos de comunicaciones deberá ser biométrico, con teclado, lector de huellas digitales y una cámara de video vigilancia que cumpla con las siguientes características: Sistema de vigilancia con capacidad de conexión IP y capacidad de almacenamiento de las grabaciones de por lo menos 30 días para el SITE, para lo cual el almacenamiento no podrá ser considerado mediante un medio extraíble. Búsqueda rápida de registro y verificación de usuarios que entran al sistema. Nueve modos de operaciones para controlar la operación de la puerta. Comunicación TCP/IP y comunicación Ethernet Software PLA-64 usando un PC como Anfitrión para el registro centralizado, monitoreo en red y control. Contraseña para proteger el acceso no autorizado a la red mediante un sistema de administración con acceso protegido por contraseña. Se deberá considerar un Teclado de Funciones Múltiples para poder ingresar una contraseña de acceso manual en caso de falla de lector biométrico. Se requieren al menos 8 cámaras IP con resolución mínima 720 x 480, 5 lectores biométricos y las chapas electromagnéticas necesarias que garanticen la seguridad del SITE y los cuartos de comunicaciones. También se deberán considerar 2 cámaras adicionales con resolución mínima 720 x 480 y las cuales podrán contar con una unidad de almacenamiento externa y alimentación POE. Adicional, la SECTUR requiere una solución para la vigilancia exterior de los edificios de sus tres sedes Schiller, Mazarik y Viaducto, la solución debe contar con al menos 11 cámaras para exterior turret IP de 5 Megapixel con Lente 2.8 mm, 40 mts IR, protección contra agua y polvo IP67, micrófono y bocina integrados, tecnología contra falsas alarmas, rango dinámico (WDR) de 120 dB, también debe incluir 3 cámaras para exterior turret IP de 4 Megapixel, imagen a color 24/7 para alimentación POE, con Lente 2.8 mm, luz blanca 30 mts, protección contra agua y polvo IP67, rango dinámico (WDR) de 120 dB que soporte H.265+/ONVIF y considerar 3 NVR con 8 canales IP con 8 Puertos POE+, que soporte cámaras con tecnología contra falsas alarmas, 2 bahías para disco duro con capacidad de almacenamiento de las grabaciones de por lo menos 30 días (debe ser interno, no se aceptan medios extraibles), switch POE hasta 250 mts, salida a través de puerto HDMI en HD y 4K. El licitante debe incluir todos los insumos, cableados, habilitadores y servicios necesarios para que la solución que proponga, quede correctamente instalada, configurada y en operación.

El licitante deberá considerar que el enrolamiento de los trabajadores de la SECTUR para los controles de acceso deberá ser de forma manual y total responsabilidades del licitante. La administración centralizada de todos los componentes del SITE se llevará a cabo desde el sitio Mazaryk y este deberá tener comunicación con todas las cámaras que se instalen en los SITES de comunicaciones y el licitante deberá considerar todo lo necesario para la adecuada interconexión entre sitios de esta y todas las soluciones objetos del presente anexo técnico, así como todos los componentes, servicios y herramientas para mantener la integridad de los equipos de los SITES de comunicaciones como UPS, tierras y adecuaciones necesarias de acuerdo con la solución propuesta.

2.9.1 Cableado Estructurado

El mantenimiento consiste en ajustar, reparar y/o remplazar los componentes del cableado de la red de voz y datos que se relacionan en el presente Anexo Técnico, hasta 30 servicios al año y la instalación de hasta 40 nodos nuevos que cumplan con las mejores prácticas y categorías al menos UTP Cat5e o superior.
Para los servicios de cableados estructurado podrán ser utilizadas Las verticales del instituto, pero el licitante deberá considerar la ducteria, escalerillas y todo lo necesario para la prestación del servicio de acuerdo con lo especificado en el anexo técnico.
El cableado que deberá cubrir se ubica en la Ciudad de México, en los domicilios siguientes:

- Presidente Masaryk 172, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580.
- Schiller 138, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580.
- Viaducto Miguel Alemán 81, Colonia Escandón, Miguel Hidalgo, C.P. 11800.

2.9.1.1 Funcionalidades

Los nodos de datos que integran la red de voz y datos son alrededor de 1,200, con cable UTP de categoría 5e o superior. Cuando se efectué una reparación, se deberá hacer con materiales de las mismas características y colores que se encuentran instalados, si estos tienen números de parte se deberá observar que su cambio se apegue al mismo, respetando el estándar siguiente:

- TIA/EIA-568-B.
- En todo servicio de instalación de nodos de cableado estructurado, el proveedor deberá realizar el etiquetado de los componentes del cableado. Los extremos de los cables que llegan al sistema de paneles de parcheo y en el área de trabajo deberán quedar completamente identificados mediante etiquetas.

Lo anterior a efecto de conservar la homogeneidad y calidad en la red, por lo que el Licitante deberá presentar un escrito mediante el cual manifieste que cumple con el estándar antes mencionado.

Los daños o modificaciones en la estructura de la red que se hubiesen registrado a causa de negligencias, ausencia de aviso a la empresa, manipulación del cableado por parte de usuarios y, nodos ausentes de canalización, no formarán parte de este contrato y con solo acreditar que se trata de estas acciones no podrá ser exigible su atención. El licitante tendrá la obligación de no otorgar el servicio de red a este tipo de tramos.
El licitante ganador será responsable de la limpieza de las áreas donde labore, así como de los resanes, pintura, reparación de techos y espacios que se dañen como consecuencia de los trabajos que realice.
El mantenimiento correctivo del cableado de la red deberá otorgarse cuando:
· Falle la continuidad en un nodo ubicado en las áreas de trabajo, para lo cual deberá escasearse el patch cord ubicado en el área de trabajo; en seguida el tramo del cable desde el jack a su acometida en el rack, y en tercer lugar el match cord desde el patch panel hasta el switch. El licitante ganador deberá acreditar con el pentascanner la existencia de esa continuidad.
En el caso de que se tenga que sustituir un patch cord en el área de trabajo, el licitante ganador deberá sujetarlo al equipo mediante los mecanismos de sujeción establecidos y conectarlo al nodo. Cuando la reparación implique cambios en los tramos ubicados entre el jack y el rack se deberá etiquetar debidamente al cable con la falla y al nuevo, además a este último sujetarlo e identificarlo con la nomenclatura del anterior. Si la reparación implica una sustitución del match

conectado al switch este deberá ordenarse y sujetarse de la manera en que está establecido el esquema actual, cuidando estrictamente el orden debido a que se tiene una administración central de la red y a que cada nodo está ligado a un puerto especifico del switch.

Si el cambio implica ocupar una nueva posición en la regleta, se deberán identificar debidamente los puertos dañado y nuevo, cuidando de actualizar la numeración del nodo en las áreas de trabajo.
El licitante contará con un máximo de 48 horas hábiles para reparar satisfactoriamente un problema de continuidad en el nodo, en caso de no tener una respuesta satisfactoria la SECTUR podrá contratar un servicio externo y descontar el monto del mismo, del contrato pactado originalmente.
Cuando se presente una falla en la continuidad de los elementos de fibra óptica tales como:

- Falla en un patch cord de fibra óptica, en cuyo caso deberá sustituirse por otro igual etiquetando sus extremos.
- Cuando falle la continuidad de la fibra óptica que comunica los IDF's hasta el MDF's, se deberá suministrar todos los recursos necesarios para que los tres canales queden en servicio incluyendo la sustitución del tramo de fibra y la conectorización únicamente por el método epóxico o de calor.
- El tiempo en que debe ser atendida una falla en la fibra óptica es de 4 horas y resuelta en lapso de 20 horas hábiles a partir de la atención de la misma, o en su caso la SECTUR buscará la reparación a través de otra empresa descontando el costo del monto del contrato.

2.9.1.2 Características Técnicas

Los elementos que la SECTUR considera como parte de su sistema de cableado son los siguientes:

No.	Elemento
1	Cableado UTP de los MDF e IDF's a las áreas de trabajo
2	Escalerilla
3	Elementos de canalización desde la escalerilla o registros de crecimiento al nodo
4	Elementos de sujeción del cableado entre los que se encuentran cinchos de plástico y velcro
5	Cajas de nodos
6	Face plate
7	Jack's
8	Patch cords ubicados en las áreas de trabajo tanto de voz como de datos
9	Registros de crecimiento (Es decir el crecimiento que la secretaria puede considerar para los nodos y servicios de cableado, de acuerdo con las cantidades solicitadas en los servicios del presente anexo)
10	Regletas de los registros de crecimiento
11	Gabinetes de IDF's
12	Ventiladores para los equipos del Site y Cuartos de Comunicaciones
13	Regletas de energía eléctrica
14	Racks
15	Organizadores horizontales y verticales
16	Regletas para el cableado de voz
17	Cross Conect

18	Regletas para el cableado de datos
19	Patch cords para conectar al equipo activo de datos
20	Etiquetas de los nodos, patch cord de UTP y fibra óptica, cableado, patch panels, regletas, registros, gabinetes y equipo.
21	Patch cord de fibra
22	Patch panel de fibra
23	Espirales para el soporte de fibra
24	Fibra óptica multimodo del back bone de tres canales
25	Tubería externa de pared gruesa
26	Registros externos
27	El cross conect del conmutador hacia la vertical

2.9.1.3 Manuales y Documentación

Cuando la SECTUR requiera la reparación de nodos de datos, en algún sitio, lo solicitará por escrito al licitante ganador y este deberá efectuar la instalación con los estándares indicados en el presente Anexo Técnico, con sus respectivas puestas a punto y actualizaciones de planos. El licitante deberá considerar que la SECTUR podrá solicitar reportes de control de acceso de las herramientas.

Los servicios de cableados deberán ser cubiertos a solicitud de la SECTUR en las siguientes direcciones:

ID	Inmueble	Dirección física	Referencia
1	Masaryk	Presidente Masaryk 172, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580, Ciudad de México.	Esquina con Hegel.
2	Schiller	Schiller 138, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580, Ciudad de México.	Entre Homero y Ejército Nacional.
3	Viaducto	Viaducto Miguel Alemán 81, Colonia Escandón, Miguel Hidalgo, C.P. 11800, Ciudad de México.	Esquina con General Salvador Alvarado y casi esquina con Patriotismo.

3. Capacitación

El Licitante ganador está comprometido a realizar la trasferencia de conocimientos de las tecnologías implementadas con cupo para máximo 5 personas designadas por la SECTUR. Y deberá ser provista durante los siguientes tres meses después de terminada la implementación.

4. Entregables

Entrega reportes que servirán como elementos de análisis y mejora a las funciones de mesa de servicio y soporte técnico que se realiza, entre los reportes que deberán generarse se encuentran:

4.1 Entregables Iniciales.

El licitante deberá de entregar como versión final la siguiente documentación dentro de los primeros cinco días hábiles de iniciado del servicio:

a) Matriz de escalamiento, donde se detallarán los nombres completos del personal del licitante, roles, números de teléfonos fijos, números de teléfonos móviles, correos electrónicos, horario de disponibilidad de cada uno de ellos.
b) El licitante deberá proporcionar el procedimiento a través del cual resolverá cualquier falla presentada en la prestación del servicio.

Por su parte, la Secretaría de Turismo proporcionará el documento de la matriz de escalamiento del personal interno a fin de coordinar las actividades propias del servicio, en los siguientes 5 días hábiles de la adjudicación del contrato.

c) Implementación y puesta en operación:
   - Memoria técnica de implementación del servicio.

Los documentos anteriores se entregarán dentro de los treinta días naturales a partir de la fecha de inicio del servicio.

4.2 Entregables Mensuales

Los reportes mensuales se deberán entregar a más tardar 5 días hábiles posteriores a la terminación del mes que corresponda.

Reporte de Análisis estadístico, consistente en un análisis estadístico de los incidentes y solicitudes levantados y atendidos en la mesa de servicio, mismo que deberá presentarse agrupados por tipo de servicio, prioridad, causa o diagnóstico, grupo o personal de atención, entre otros,

Inventario de equipos que conforman la base instalada del servicio, detallando entre otras cosas localización, número de serie, condiciones especiales de operación y fecha de implementación, destacando las altas y bajas de equipo y configuraciones que tuvieron lugar durante el mes.

Se podrán solicitar reportes bajo demanda los cuales solo podrán ser solicitados por el administrador del contrato por escrito o el mecanismo que se acuerde con el licitante, estos reportes deberán ser integrados en los entregables mensuales en el caso de que exista alguna solicitud.

Actualización de la memoria técnica en caso de ser necesario.

5. Niveles de Servicio

El licitante deberá cumplir con los siguientes niveles de servicio, de acuerdo a la severidad de los eventos:

Nivel de Severidad	Descripción	Tipo de Solicitud	Tiempo de Atención	Tiempo de Solución
Severidad 1	Pérdida Total de la plataforma o equipo que forma parte del inventario cubierto y que origine un problema grave que interrumpa todas las funciones críticas del cliente.	Notificación del cliente vía telefónica o generación de ticket	Menor a 10 min	12 hrs
Severidad 2	Pérdida parcial de la plataforma o equipo que forma parte del inventario cubierto, el funcionamiento no está al 100%, y que origine una degradación del Servicio.	Notificación del cliente vía telefónica o generación de ticket	Menor a 10 min	18 hrs
Severidad 3	Todas las funciones de la plataforma o equipo que forme parte del Inventario cubierto opera al 100%, sin embargo, el rendimiento esta degradado o muy limitado	Notificación del cliente vía telefónica o generación de ticket	Menor a 10 min	24 hrs
Severidad 4	Se refiere al grupo de cambios, consultas de características y otras preguntas de uso común y que no se consideran	Notificación del cliente vía telefónica o generación de ticket	Menor a 10 min	36 hrs

Nivel de Severidad	Descripción	Tipo de Solicitud	Tiempo de Atención	Tiempo de Solución
	críticas para el desempeño de las funciones del cliente.			

El licitante deberá considerar 3 Ingenieros en sitio de lunes a viernes de 9 a 19 horas los días hábiles de la SECTUR, para efectuar el soporte técnico a todos los servicios solicitados en el anexo técnico y será responsabilidad del licitante entregar todo el equipamiento, herramientas, papelería, equipos de comunicación que considere necesarios para que los Ingenieros puedan llevar a cabo las tareas operativas encomendadas.

Adicionalmente el Licitante será responsable de proveer a los Ingenieros todo el equipo de protección necesario para salvaguardar su integridad y salud ante las problemáticas de salud por el SAR-COV-2. Es importante mencionar que la secretaria cuenta con todos los protocolos sanitarios necesarios para la operación diaria de manera segura.

6. Lugar de Entrega

El lugar de entrega de los servicios por el licitante se muestra en la siguiente tabla:

ID	Inmueble	Dirección física	Referencia
1	Masaryk	Presidente Masaryk 172, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580, Ciudad de México.	Esquina con Hegel.
2	Schiller	Schiller 138, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580, Ciudad de México.	Entre Homero y Ejército Nacional.
3	Viaducto	Viaducto Miguel Alemán 81, Colonia Escandón, Miguel Hidalgo, C.P. 11800, Ciudad de México.	Esquina con General Salvador Alvarado y casi esquina con Patriotismo.

7. Transición del servicio

Treinta días naturales previos al término del contrato, el Proveedor y la Dependencia acordaran el proceso de transición para la prestación del servicio, con la finalidad de que no se afecte la operación y los niveles de servicio requeridos por la Dependencia correspondiente en el presente anexo técnico. Derivado de lo anterior, el Proveedor se obliga a:

a) Participar en las reuniones que soliciten las Dependencias o Entidades para realizar la transición con el Proveedor adjudicado al final del contrato.

b) Durante este proceso de transición el Proveedor deberá seguir prestando el servicio por un periodo máximo de treinta (30) días naturales sin costo para la Dependencia o Entidad a partir de la conclusión del contrato, el que podrá ser reducido en la medida

que el nuevo Proveedor que resulte adjudicado implemente el servicio.

c) En caso de rescisión del contrato del servicio objeto del presente anexo técnico, este no podrá ser suspendido hasta que se asegure la transición en los términos previstos en el párrafo que antecede.

8. Condiciones y Forma de pago

Pagos a mes vencido, (a partir de marzo) de acuerdo con la normatividad vigente y con el visto bueno de la Dirección de Control y Soporte Técnico. El importe será pagado en moneda nacional. Conforme al último párrafo del artículo 51 de la LAASSP.
La factura de los servicios realmente devengados se hará a mes vencido. Dicha factura se elaborará conforme a las disposiciones fiscales vigentes y lo señalado en las cláusulas del contrato. Se dará por recibida la factura cuando sea aceptada la totalidad de los documentos del servicio del mes que corresponda según lo especificado en el procedimiento de recepción y revisión de entregables.

El cobro de las penas convencionales y de las deducciones, se llevarán a cabo observando las disposiciones correspondientes en la materia.

En caso de detectar algún cobro indebido posterior a la aceptación del detalle del servicio respectivo, la Secretaría presentarán su inconformidad por correo electrónico o escrito al Proveedor quien deberá reintegrar la cantidad pagada en exceso conforme a lo especificado en el contrato y la normatividad que resulte aplicable.

Las aclaraciones y/o modificaciones a los detalles de los documentos del servicio y factura no impedirán que se continúe prestando el servicio.

Es requisito indispensable contar con toda la documentación solicitada para autorizar y tramitar el pago. Dicha documentación consiste en: La documentación mensual soporte del servicio, factura, nota de crédito en su caso.

La no entrega oportuna de cualquiera de los documentos anteriormente mencionados impedirá al administrador del contrato autorizar y tramitar antes las instancias correspondientes de la Secretaría el pago en los términos de la cláusula correspondiente del contrato, independientemente de aplicación de las penas convencionales y deducciones que correspondan.

9. Penas y Deductivas

Durante la vigencia del contrato, la SECTUR podrá imponer penas convencionales al proveedor, por atraso en la prestación del servicio o deducciones por incumplimiento parcial o deficiente en que pudiera incurrir el proveedor respectivamente La SECTUR podrá optar entre promover su rescisión o exigir el cumplimiento del mismo, sin necesidad de intervención judicial al efecto.

Viaducto Presidente Miguel Alemán Valdés No. 81, Colonia Escandón 1 Sección, CP. 11800, Alcaldía Miguel Hidalgo, CDMX.
Tel: (55) 3002 6300 www.gob.mx/sectur

3. Las penas convencionales se aplicarán por la SECTUR, cuando el proveedor incurra en retraso en el cumplimiento oportuno de la prestación del servicio en cuyo caso se aplicará un porcentaje del 1% por cada día natural de retraso y hasta por el 10% del monto total de los servicios no prestados oportunamente.

4. Las deducciones se aplicarán cuando el proveedor incurra en incumplimiento parcial o deficiente en la prestación del servicio conforme a los requerimientos de calidad, contenidos y especificaciones técnicas señaladas en el contrato y su Anexo Técnico. Dicha deductiva corresponde al 1% de los servicios proporcionados parcial o deficiente por cada día natural, hasta el 10% del monto total del contrato.

Los montos a deducir se deberán aplicar en la factura que el proveedor presente para su cobro, una vez que el área usuaria haya cuantificado la deducción correspondiente.

Las penas convencionales se aplicarán con base en la parte proporcional de la garantía de cumplimiento del monto total del presente contrato.

La aplicación de las penas convencionales y deducciones no son excluyentes la una de la otra, esto es. Pueden aplicarse simultáneamente y no excederán en su conjunto al monto de la fianza de garantía de cumplimiento, por lo tanto, no serán acumulativas, para los efectos de la rescisión administrativa prevista por el artículo 54 de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público y el artículo 98 de su Reglamento

Las penas convencionales serán determinadas por la SECTUR por conducto del ENLACE designado por el área usuaria en función de los servicios no prestados.

10. Perfil del licitante.

El licitante deberá demostrar su especialidad, capacidad y experiencia a través de la siguiente documentación:

- Currículo de la empresa y personal calificado que acredite al menos un año de experiencia en la prestación de servicios similares a los solicitados en el presente Anexo Técnico y que contenga la lista de sus principales clientes.
- Presentar copia simple de al menos un contrato celebrado en los últimos tres años, cuyo objeto sea igual o similar a los servicios objeto del presente ANEXO, para acreditar al menos un año de experiencia en la prestación del servicio.

El licitante deberá entregar los documentos siguientes:

- Matriz de escalamiento, donde se detallarán los nombres completos del personal del proveedor, roles, números de teléfonos fijos, números de teléfonos móviles, correos electrónicos, horario de disponibilidad de cada uno de ellos.
- Procedimiento a través del cual resolverá cualquier falla presentada en la prestación del servicio.
- Proporcionar un plan de trabajo de implementación de todos los equipos que compongan las soluciones de seguridad informática. Este puede ser implementado en fases, las cuales

podrán ser actividades paralelas o secuenciales considerando la complejidad de la infraestructura en operación. El plan de trabajo debe ejecutarse para proporcionar los servicios el 16 de marzo de 2023.

- Incluir para el servicio de Seguridad Perimetral una carta de fabricante membretada en la cual señale que cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante, firmada por la persona autorizada por el fabricante de la solución propuesta.
- Incluir para el servicio de Seguridad Perimetral al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada.
- Para el servicio de Antispam, el licitante deberá especificar por escrito, que su solución ofrecerá la garantía de poder detectar correctamente el correo que sea spam, combinaciones spam, virus, exploits o contenido grafico de spam.
- Incluir para la solución de Antivirus una carta de fabricante membretada en la cual señale que cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante, firmada por la persona autorizada por el fabricante de la solución propuesta.
- Incluir para la solución de Antivirus al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada.
- Incluir para esta solución una carta en papel membretado firmada por el representante legal del fabricante del software de respaldos en la que manifieste que el proveedor es un distribuidor o partner de la marca.
- La mesa de servicios deberá operar siguiendo el marco de referencia ITIL versión 4, para lo cual el licitante deberá presentar el certificado de al menos 6 ingenieros certificados.
- Incluir copia de certificación NMX-|-27001 NYCE 2015 |ISO/ IEC 27001:2013: En su proceso de incidentes, problemas y niveles de servicio para la operación del servicio.
- Incluir copia de certificación NMX-|-20000-1 NYCE 2019 | ISO/IEC 20000-1:2018: En sus procesos de cambios, solicitudes de servicio y niveles de servicio con los que opera la Mesa de Ayuda.

Nota: Estos documentos se presentarán de acuerdo con lo solicitado en el procedimiento de contratación.

11. Anticipos.

No aplica.

12. Prórrogas.

No aplica

13. Garantía de cumplimiento.

El proveedor deberá garantizar el cumplimiento de sus obligaciones a través de una fianza por el 10 % del monto total del contrato/pedido sin considerar el IVA.

La garantía será divisible.

14. Suspensión de la prestación.

Cuando en la prestación del servicio se presente caso fortuito o fuerza mayor, o bien por causas atribuibles a la SECTUR, ésta bajo su responsabilidad podrá suspender la prestación del mismo, sin que ello implique la terminación del contrato, en cuyo caso únicamente se pagarán aquellos servicios que hubiesen sido efectivamente prestados.

Asimismo, las PARTES convienen en apego a lo consagrado en el artículo 91 del Reglamento, una vez que se acrediten los supuestos establecidos en el párrafo que antecede, las PARTES podrán modificar la vigencia del Contrato, en este supuesto se deberá formalizar a través del convenio modificatorio respectivo, no dando lugar a la aplicación de las penas convencionales por atraso del proveedor.

Cuando la suspensión obedezca a causas imputables a la SECTUR, previa petición y justificación del proveedor, ésta reembolsará al proveedor los gastos no recuperables que se originen durante el tiempo que dure esta suspensión, siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con el Contrato, de conformidad con lo dispuesto por el artículo 55 Bis de la Ley.

En cualquiera de los casos previstos en esta cláusula, las PARTES pactarán el plazo de suspensión, a cuyo término podrá iniciarse la terminación anticipada del Contrato, o bien, una vez que haya desaparecido la causa que motivó la suspensión, el Contrato podrá volver a producir sus efectos legales.

La suspensión de la prestación de servicios se sustentará mediante dictamen que precise las razones o las causas justificadas que den origen a las mismas, de conformidad con lo dispuesto con el artículo 102 del Reglamento.

15. Servidor Público del área responsable de administrar y verificar el cumplimiento del contrato.

El titular en funciones de la Dirección de Control y Soporte Técnico, fungirá como responsable de administrar y verificar el cumplimiento de los servicios descritos en el presente documento.

16. Normas Oficiales Mexicanas, las Normas Mexicanas y a falta de éstas, las Normas Internacionales que aplican al bien o servicio solicitado.

La mesa de servicios deberá operar siguiendo el marco de referencia ITIL, para lo cual el licitante deberá presentar el certificado de al menos 6 ingenieros certificados en ITIL Foundations v4.

La mesa de ayuda deberá operar en sus procesos de cambios, solicitudes de servicio y niveles de servicio el estándar NMX – I – 20000-1:2019 / ISO/IEC 20000-1:2018, para lo cual el licitante debe presentar copia del certificado vigente.

El servicio de monitoreo de red deberá operar en sus procesos de incidentes, problemas y niveles de servicio bajo el estándar NMX – I – 27001:2015 / ISO/IEC 27001:2013 , para lo cual el licitantes deberá presentar copia del certificado vigente.

17. Señalar si se entrega, en su caso, muestras y/o catálogos respectivos (fotografías, folletos, diseños, planos, entre otros.)

Se deberán entregar las hojas técnicas del fabricante donde especifique las características de los equipos propuestos, para lo cual los licitantes deberán entregar una relación de las especificaciones técnicas contenidas en el anexo técnico con la traducción simple de las especificaciones contenidas en la documentación oficial del fabricante y adjuntar los documentos del fabricante en su idioma original señalando las especificaciones técnicas referidas en español. No se aceptaran cartas de fabricante señalando especificaciones no soportadas contenidas en el presente anexo técnico.

Los certificados que avalan la capacidad de los recursos humanos podrán ser presentados en su idioma original identificando claramente el nombre del recurso propuesto.

********** **FIN DEL ANEXO TÉCNICO** **********

Viaducto Presidente Miguel Alemán Valdés No. 81, Colonia Escandón 1 Sección, CP. 11800, Alcaldía Miguel Hidalgo, CDMX.
Tel: (55) 3002 6300 www.gob.mx/sectur

SayNet

LICITACIÓN PUBLICA
LA-21-510-021000999-N-6-2023
"Solución de infraestructura de red (LAN, WIFI), seguridad perimetral y servidores"

1. PROPUESTA TÉCNICA

Propuesta Técnica Desarrollando todos los puntos del anexo técnico

Aviso de Privacidad y Derechos de Autor

ANEXO UNO: ESPECIFICACIONES TÉCNICAS

1. Descripción del Bien y/o Servicio

1.1 Identificación del proyecto

Solución de infraestructura de red (LAN, WiFi) seguridad perimetral y servidores

1.2 Objetivo

Soluciones Integrales SayNet S.A. de C.V. brindará el servicio de suministro y equipamiento mediante soluciones integradas de red alámbrica e inalámbrica, seguridad informática y computo en los inmuebles de la Secretaría de Turismo (SECTUR) derivado de las funciones sustantivas y adjetivas que se realizan en ellos y contribuir a la misión de la SECTUR.

1.3 Vigencia

Fecha de inicio del servicio

16 de marzo de 2023

Soluciones Integrales SayNet S.A. de C.V. entregará el servicio funcionando y operado al 100 % a partir del 16 de marzo de 2022.

Para este efecto **Soluciones Integrales SayNet S.A. de C.V.** contará para su implementación, con el plazo comprendido a partir de la firma de contrato y hasta el 16 de marzo de 2023, el equipo puede ser no nuevo y encontrarse en óptimas condiciones de operación.

Fecha de fin de servicio

31 de diciembre de 2023

Soluciones Integrales SayNet S.A. de C.V. tiene presente que
La etapa de cierre del servicio, aplicable a la infraestructura de cómputo Institucional, iniciará 45 días naturales previos a la conclusión de la vigencia.

1.4 Relación de los Servicios a Contratar

- Servicio de infraestructura de red.
- Servicio de Seguridad perimetral.
- Servicio de Antivirus
- Servicio de Respaldos
- Servicio de Infraestructura de Servidores

- Servicio de Monitoreo de red y Mesa de Ayuda
- Escaneo de Vulnerabilidades y certificados digitales
- Soporte a SITE, cuartos de comunicaciones y cableado estructurado

1.4.1. Requerimientos de recuperación de bienes al término del contrato:

a) **Soluciones Integrales SayNet S.A. de C.V.** en un término no mayor a 30 días naturales posteriores al término del contrato retirará la infraestructura activa de las instalaciones de la SECTUR previa demostración de que los equipos son de su propiedad.
b) Los equipos de infraestructura activa que no sean retirados en un plazo de 90 días naturales posteriores al término del contrato atribuible a **Soluciones Integrales SayNet S.A. de C.V.**, la SECTUR tomará las medidas legales y administrativas correspondientes para que dichos bienes pasen a ser parte del inventario de la SECTUR.

1.4.2. Requerimiento de migración de servicios al término del contrato

Al término de la vigencia del contrato, **Soluciones Integrales SayNet S.A. de C.V.** se obliga a realizar las actividades propias de transferencia y migración de los servicios hacia un nuevo Prestador de servicios.

1.4.3 Otros requerimientos que deberá cumplir Soluciones Integrales SayNet S.A. de C.V., para la prestación del servicio.

a) Todos los requerimientos y especificaciones son mínimos.
b) Toda la solución se debe proporcionar como un servicio integral, por tanto, **Soluciones Integrales SayNet S.A. de C.V.** considero que todos los requerimientos, especificaciones técnicas y servicios expresados en este anexo técnico, así como lo necesario para llevar a cabo la implantación, la operación, el soporte técnico, contar con los recursos humanos y materiales para cumplir con lo solicitado por la SECTUR.
c) Toda la infraestructura suministrada y empleada para la prestación del servicio integral por parte de **Soluciones Integrales SayNet S.A. de C.V.** será de su propiedad y entera responsabilidad.
d) Toda la infraestructura pasiva suministrada para la prestación del servicio integral por parte de **Soluciones Integrales SayNet S.A. de C.V.** pasará a ser propiedad de la SECTUR al término del contrato. Entiéndase como infraestructura pasiva como los elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de las dependencias o entidades, que sean necesarios

para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión .

e) **Soluciones Integrales SayNet S.A. de C.V.** será responsable de la legalidad y autenticidad de los derechos de autor, derechos de propiedad industrial o patentes del software y/o hardware utilizados para brindar el servicio integral.

f) **Soluciones Integrales SayNet S.A. de C.V.** sólo exigirá el pago de los conceptos que específicamente se encuentren detallados en la propuesta económica. Cualquier otro concepto que no aparezca en dicha propuesta no será exigible. Por lo anterior, **Soluciones Integrales SayNet S.A. de C.V.** considero todos los costos inherentes de los servicios, requerimientos, especificaciones técnicas, niveles de servicio, documentos, recursos humanos, materiales, equipos, infraestructuras entre otros en el precio final de los servicios que son parte de su propuesta económica.

g) Es responsabilidad de **Soluciones Integrales SayNet S.A. de C.V.** el diseño de la arquitectura tecnológica de cada una de las soluciones de servicio que proponga y en la que deberá considerar cada uno de los requerimientos, especificaciones técnicas y servicios de cada solución. Si durante el proceso de implementación, pruebas y operación de cada solución se detecta que esta no cubre adecuadamente algún requerimiento, especificación técnica y servicio expresado en este anexo técnico o existan problemas de compatibilidad e integración entre los componentes de cada solución, **Soluciones Integrales SayNet S.A. de C.V.** realizará los cambios de arquitectura tecnológica, componentes, equipos, accesorios, software, licenciamiento y cualquier otro elemento que sean necesarios para solucionar esta deficiencia sin costo adicional para la Secretaría de Turismo.

h) **Soluciones Integrales SayNet S.A. de C.V.** entiende que las características, capacidades y funcionalidades que no sean específicamente detalladas en este anexo técnico y que sean incluidas en cualquiera de las soluciones ya sea que estás estén integradas en el hardware, software o que se encuentren amparadas por el uso de la licencia serán puestas en operación y usados como parte integral del servicio.

1.5 Requerimientos del Servicio / Consideraciones para todos los componentes

Requerimientos funcionales:

Soluciones Integrales SayNet S.A. de C.V. realizará el suministro, distribución, instalación, configuración, puesta a punto y entrada en operación de equipos y componentes físicos especializados que provean:

- Servicio de infraestructura dered.
- Servicio de Seguridad perimetral.
- Servicio de Antivirus
- Servicio de Respaldo
- Servicio de Infraestructura deServidores
- Servicio de Monitoreo de red y Mesa de Ayuda
- Escaneo De Vulnerabilidades y certificados digitales
- Soporte a SITE, cuartos de comunicaciones y cableado estructurado

Requerimientos no funcionales:

- **Soluciones Integrales SayNet S.A. de C.V.** cumplirá con los Niveles de servicio conforme a lo detallado en la sección 5 "Niveles de Servicio".
- **Soluciones Integrales SayNet S.A. de C.V.** proveerá el Soporte documental del servicio.

Requerimientos y controles de seguridad:

- **Soluciones Integrales SayNet S.A. de C.V** Efectuará el borrado seguro de cualquier dispositivo de almacenamiento que sea retirado durante la vigencia del servicio.
- **Soluciones Integrales SayNet S.A. de C.V** Efectuará el borrado seguro de cualquier dispositivo de almacenamiento antes de retirarlo al finalizar la vigencia del servicio.

Requerimientos de implementación y puesta en operación:

- **Soluciones Integrales SayNet S.A. de C.V.** contemplo toda la logística necesaria para realizar el reemplazo de los equipos que componen la solución que proponga en cada uno de los inmuebles de la SECTUR.

Soluciones Integrales SayNet S.A. de C.V contempla las siguientes consideraciones generales para todos los componentes:

- Todos los equipos suministrados durante la vigencia del servicio son de características iguales o superiores a los solicitados en las especificaciones técnicas de este documento.
- **Soluciones Integrales SayNet S.A. de C.V.** contempla en su propuesta todos los accesorios, cables de alimentación, cables de red, cables de fibra, rieles, herrajes y todo lo necesario para la adecuada instalación e integración entre sí y en condiciones seguras de operación para todos los componentes de la solución que propone.
- **Soluciones Integrales SayNet S.A. de C.V.** contempla en su propuesta toda la canalización, ductos y herrajes para interconectar los racks que proponga hacia el rack de

comunicaciones existente en el centro de datos de Masaryk, así como también, las adecuaciones al piso falso que requiere la implementación de su solución de seguridad informática.

- **Soluciones Integrales SayNet S.A. de C.V.** contempla en la solución de seguridad informática la adecuada integración con la infraestructura existente en el centro de datos de la SECTUR.
- **Soluciones Integrales SayNet S.A. de C.V.** contempla la instalación de los circuitos y protección eléctrica (aterrizaje de los equipos de las soluciones que sean instalados hacia el sistema de tierra existente) en el centro de datos de Masaryk planta baja para los equipos de las soluciones que sean instalados en el mismo. La SECTUR cuenta con un tablero de distribución trifásico localizado en el centro de datos. La distancia máxima de los circuitos eléctricos es de 12 metros.
- **Soluciones Integrales SayNet S.A. de C.V.** contempla la instalación física de todos los equipos, rack's, componentes, cableados, accesorios y cualquier dispositivo de la solución de seguridad informática usado para el proceso de implementación estará correctamente ensamblado, adecuadamente colocado y ser seguro bajo los criterios que marque el supervisor del servicio.
- La operación de la solución de seguridad informática propuesta por **Soluciones Integrales SayNet S.A. de C.V.** está garantizada conforme a los niveles de servicio solicitados en este anexo técnico durante toda la vigencia delcontrato.
- **Soluciones Integrales SayNet S.A. de C.V.** tendrá actualizado el inventario y resguardos de los equipos de lasolución propuesta, incluyendo altas, bajas, cambios y reubicación.
- El personal "**Soluciones Integrales SayNet S.A. de C.V**" que labore durante la vigencia del contrato y efectúe trabajos relacionados con el servicio de este anexo técnico firmaran el documento de acuerdo de confidencialidad suministrado por el administrador del contrato.

Soluciones Integrales SayNet S.A. de C.V realizará la implementación y puesta en operación de acuerdo con lo siguiente:

- **Soluciones Integrales SayNet S.A. de C.V** proporcionará un plan de trabajo de implementación de todos los equipos que compongan las soluciones de seguridad informática. Este puede ser implementado en fases, las cuales podrán ser actividades paralelas o secuenciales considerando la complejidad de la infraestructura en operación. El plan de trabajo será aprobado por el administrador del contrato. El plan de trabajo se ejecutará para proporcionar los servicios el 16 de marzo 2023.
- **Soluciones Integrales SayNet S.A. de C.V.** iniciara la etapa de operación el 16 de marzo 2023 hasta la vigencia del contrato que corresponda y

consistirá en la administración, mantenimiento y soporte de los recursos que se encuentren instalados y operando de toda la solución.

- **Soluciones Integrales SayNet S.A. de C.V.** realizará la instalación de los circuitos eléctricos en el centro de datos de Masaryk con la capacidad suficiente para soportar los rack's con su respectivo equipamiento.
- **Soluciones Integrales SayNet S.A. de C.V.** realizará las adecuaciones y/o reposiciones de galletas del piso falso derivado de la instalación de los equipos.
- **Soluciones Integrales SayNet S.A. de C.V.** realizará la instalación de los rack's de la solución.
- **Soluciones Integrales SayNet S.A. de C.V.** Realizará la instalación, configuración y puesta a punto de todos los equipos de la solución, su software y componentes.

En cada una de las actividades de implementación pueden realizarse actividades de validación, verificación y pruebas del hardware y software para ser aprobadas antes de su puesta en operación y paso a producción las cuales serán autorizadas por el supervisor del servicio.

2. Características Técnicas y Funcionalidades

Soluciones Integrales SayNet S.A. de C.V. entiende que SECTUR tiene alojados en su centro de datos buzones de correo electrónico para 1500 cuentas habilitadas, la operación de los sistemas administrativos y sustantivos da servicios de Internet a alrededor de 900 usuarios activos, los cuáles son usados para desempeñar funciones orientadas a los objetivos institucionales y cuyas actividades requieren, entre otros los servicios de navegación segura, conexiones seguras y protección a la información que se genera.

Soluciones Integrales SayNet S.A. de C.V. comprende que para preservar la operatividad de los servicios que SECTUR otorga a las áreas responsables para su adecuado funcionamiento, requiere contar con las soluciones y/o herramientas tecnológicas.

Soluciones Integrales SayNet S.A. de C.V. comprende que SECTUR requiere de cada una de las soluciones tecnológicas de acuerdo con lo siguiente:

Seguridad Perimetral para usuario y datacenter: Las soluciones de seguridad perimetral protegen a las redes institucionales de la entrada de código malicioso o malware, permiten filtrar el tráfico del exterior hacia la red institucional. Además, se han presentado ataques de ransomware ante los cuales no se puede reaccionar de manera preventiva, para lo anterior se requiere de la protección a al centro de datos y de los usuarios desde el perímetro y en sus estaciones de trabajo, para garantizar la disponibilidad, autenticidad e integridad de la información, previniendo también de posibles secuestros de la información.

Soluciones Integrales SayNet S.A. de C.V. cumplirá con los siguientes servicios administrados:

- Servicio de infraestructura de red.
- Servicio de Seguridad perimetral.
- Servicio de Antivirus
- Servicio de Respaldos
- Servicio de Infraestructura de Servidores
- Servicio de Monitoreo de red y Mesa de Ayuda
- Escaneo De Vulnerabilidades y certificados digitales
- Soporte a SITE, cuartos de comunicaciones y cableado estructurado

2.1 Servicio de Infraestructura de Red

La solución de switches Core propuesta por **Soluciones Integrales SayNet S.A. de C.V.** es de alta disponibilidad, alto rendimiento y seguridad.
Soluciones Integrales SayNet S.A. de C.V tiene considerado proveer una red de datos de dos niveles, Núcleo (CORE) y Acceso además de un controlador de Red LAN inalámbrica (WLAN) igualando el número de Puntos de Acceso (Access Points), que se encuentran actualmente operando, por lo que se consideran 65 AP´s.

La solución propuesta por Soluciones Integrales SayNet S.A. de C.V, proporcionará una red capaz de soportar la convergencia de tráfico de datos, voz, video y de la red inalámbrica, es considerada como prioridad en la propuesta presentada por **Soluciones Integrales SayNet S.A. de C.V,** para ello el **Soluciones Integrales SayNet S.A. de C.V** propondrá el equipamiento y sistemas necesarios para lograr tal propósito, entre ellos se destacan:

- Análisis del equipamiento actual de red LAN y la red WLAN
- Proporcionará equipo igual o elevando sus características y funcionalidades a las requeridas en el presente anexo técnico.

Solución requerida

La red actual de la SECTUR está conformada por redes LAN en los tres sitios principales, donde hay un equipo operando como unidad de Núcleo (CORE TIPO 2) en cada edificio y diferentes equipos de acceso.

Los equipos propuestos por **Soluciones Integrales SayNet S.A. de C.V** son **Marca: Extreme Networks, Modelo: BlackDiamond 8806 para el CORE Tipo 2 y Marca: Extreme Networks, Modelo: Summit X450e-48P para el SWITCH DE ACCESO 48 PUERTOS POE CAPA 2** los cuales igualan o mejorarán estas características. En la Tabla 1, se muestra la distribución de los equipos a remplazar por Edificio y por IDF.

ÁREA	TIPO	CANTIDAD	NÚMERO DE PUERTOS COBRE	TOTAL DE PUERTOS COBRE	NÚMERO DE PUERTOS FIBRA	CONTROLADORAS / PROCESADORAS	FUENTES DE PODER
MASARIK							
Centro de Datos	CORE TIPO 2	1	48	48	24	2	3
MDF-PB	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	7	48	336	0	DEFAULT	DEFAULT
IDF-P2	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	5	48	240	5	DEFAULT	DEFAULT
IDF-P5	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	4	48	192	4	DEFAULT	DEFAULT
IDF-P8	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	3	48	144	4	DEFAULT	DEFAULT
IDF-P11	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	3	48	144	2	DEFAULT	DEFAULT
Red DMZ	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	1	48	48	0	DEFAULT	DEFAULT
SCHILLER							
IDF	CORE TIPO 2	1	48	48	16	2	3
MDF-PB	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	3	48	144	3	DEFAULT	DEFAULT
MDF-P3	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	3	48	144	3	DEFAULT	DEFAULT
MDF-P6	SWITCH DE ACCESO 48 PUERTOS POE APA 2	3	48	144	3	DEFAULT	DEFAULT
MDF-P9	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	3	48	144	3	DEFAULT	DEFAULT

MDF-PH	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	2	48	96	2	DEFAULT	DEFAULT
VIADUCTO							
IDF	CORE TIPO 2	1	48	48	16	2	3
MDF-PB	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	4	48	192	4	DEFAULT	DEFAULT
IDF-P1	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	5	48	240	4	DEFAULT	DEFAULT
IDF-Capacitación	SWITCH DE ACCESO 48 PUERTOS POE CAPA 2	1	48	48	0	DEFAULT	DEFAULT
AIFA							
AIFA	SWITCH DE ACCESO 4 PUERTOS POE CAPA 2	1	24	24	0	DEFAULT	DEFAULT

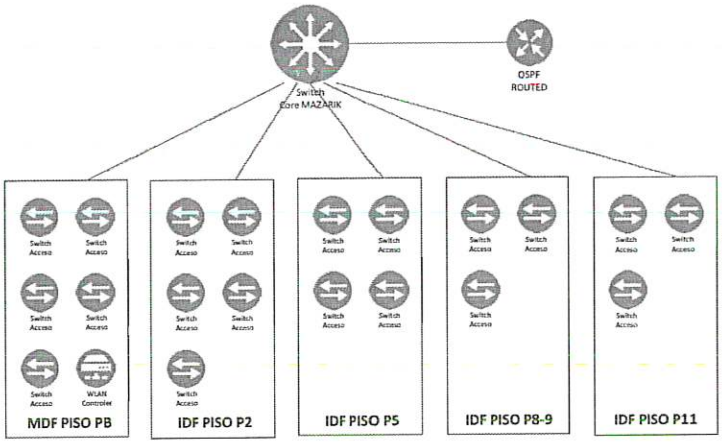
Tabla 1. Distribución de los equipos a reemplazar por inmueble e IDF.

Adicionalmente **Soluciones Integrales SayNet S.A. de C.V.**, considera que deberá proporcionar el soporte, mantenimiento y administración de un Switch de 48 puertos de la SECTUR, con las siguientes características:
Modelo: Summit X460
Marca: Extreme Networks

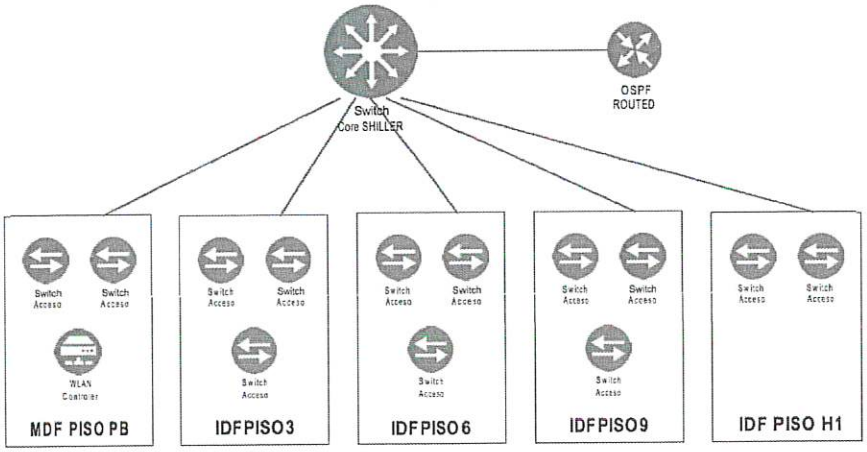
En cuanto a la red inalámbrica WLAN, **Soluciones Integrales SayNet S.A. de C.V.** propone una arquitectura centralizada donde un switch/controlador (CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1) **con equipos Marca: Extreme Networks, modelo: XCC VE6120 para Mazaryk y modelos: C35 para Schiller y Viaducto**, que administra, monitorea, controla y valida la operación de la red inalámbrica como un todo superpuesto a la red cableada.

La solución **propuesta por Soluciones Integrales SayNet S.A. de C.V.** es en modo de arrendamiento, contiene el equipamiento, instalación y administración de la solución que considera el equipamiento de la tabla 1.

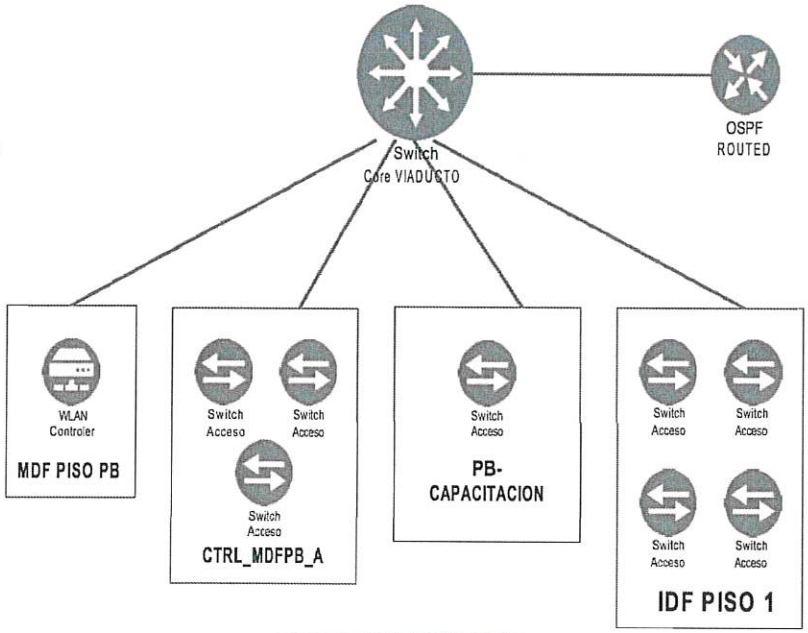
Diagramas Conceptuales de red



Red del Edificio de Presidente Masaryk



Red del Edificio de Schiller



Red del Edificio de Viaducto

Cada uno de los equipos Centrales (CORE TIPO 2) **Marca: Extreme Networks modelo: BlackDiamond 8806** y de los equipos de acceso **Marca: Extreme Networks modelo: Summit X450-48P** propuestos por **Soluciones Integrales SayNet S.A. de C.V.** cubren las características señaladas en este anexo.

Red Inalámbrica

La Red inalámbrica WLAN de la SECTUR está formada por 65 Access Points (PUNTO DE ACCESO PARA INTERIORES TIPO 1) simplemente proporcionando entrada a la red LAN Institucional.

La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V** es centralizada que controla la función, operación y seguridad en la red inalámbrica (CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1) **con equipos Marca: Extreme Networks, modelo: XCC VE6120 para Mazaryk y modelos: C35 para Schiller y Viaducto**. La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V** utilizara las mismas ubicaciones de cobertura existente y reforzar en la cobertura en caso de necesitarse.

Para garantizar un mayor grado de seguridad los AP actuales fueron requeridos para su operación en modo centralizado.

2.1.1 Funcionalidades de los equipos

Los equipos propuestos en la solución de **Soluciones Integrales SayNet S.A. de**

C.V., independientemente si éstos son para el Núcleo (CORE TIPO 2) **Marca: Extreme Networks Modelo: BlackDiamond 8806 de la red o el Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2) Marca: Extreme Networks Modelo: Summit X45048P** a la misma cuentan con las siguientes características:

- Arquitectura no-bloqueable: Necesaria para soportar aplicaciones de tiempo real, tales como, la voz y el video que requieren obligatoriamente de esta característica de arquitectura interna que le permite manejar todos los puertos de red al 100% de su capacidad sin pérdida de paquetes.
- Alta Disponibilidad: Poder tener una disponibilidad de 99.999% para el Núcleo de la Red (CORE TIPO 2) **Marca: Extreme Networks Modelo: BlackDiamond 8806** y 99.99% para el Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2) **Marca: Extreme Networks Modelo: Summit X45048P**, para lo cual todos los sistemas proveen mecanismos redundantes tales como procesamiento y control, fuentes de poder, ventiladores y sistema operativo en los equipos para el Núcleo (CORE TIPO 2) **Marca: Extreme Networks Modelo: BlackDiamond 8806**, y por lo menos una fuente de poder y un sistema operativo para los equipos de Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2) **Marca: Extreme Networks Modelo: Summit X45048P**.
- Calidad de Servicio: Para poder diferenciar y tratar de manera adecuada todas las aplicaciones que corren en la red, todos los equipos propuestos deberán soportar las mismas características técnicas y así proveer Calidad de Servicio.
- Altos niveles Seguridad: Todas las unidades propuestas cuentan con sistemas de seguridad de alto nivel tales como protección contra ataques de Negación de Servicio, Seguridad Avanzada para el Protocolo IP, monitoreo de flujos de IP en todos los puertos de red de los equipos. Capacidades para el despliegue de sistemas de control de acceso de red, así como el soporte para sistemas de autenticación de usuario. Los equipos deberán contar con un motor de seguridad que les permita reaccionar ante amenazas de seguridad, ataques, o comportamientos maliciosos e iniciar algún mecanismo de remediación.
- Fácil Administración: Todos los sistemas propuestos deberán contar con el mismo sistema operativo y línea de comandos. Esto aplica para los equipos para el Núcleo de la red, así como para los de Acceso. Si Soluciones Integrales SayNet S.A. De C.V, sustituye equipos que actualmente se encuentran en la red de la SECTUR, los equipos propuestos deberán soportar algún tipo de emulación de la línea de comandos de los equipos existentes. **Soluciones Integrales SayNet S.A. de C.V.** considera proveer un Sistema de Administración de Redes compatible **Marca: Extreme Networks, modelo: Ridgeline Network and Service Management Software** con los equipos propuestos, y permitir la administración, monitoreo, configuración y aprovisionamiento automatizado de los equipos de manera fácil y lógica.
- Red Convergente: La solución propuesta deberá ser capaz de soportar aplicaciones propias de una red convergente, para poder ser el medio de

conducción de tráfico dedicado a datos, VoIP, video encapsulado en IP, y el tráfico proveniente de la red WLAN. Como parte de la propuesta técnica **Soluciones Integrales SayNet S.A. de C.V.** presenta un **"Plan de Ingeniería de Tráfico"** que describe la forma en cómo la red propuesta tratará cada uno de estos escenarios de tráfico, de manera eficiente y de fácil administración.

Cada uno de estos requerimientos generales, son mínimos e imprescindibles, por lo que están respaldadas mediante el soporte y manejo de protocolos y arquitecturas abiertas. Más adelante en la presente propuesta técnica, se presentan las especificaciones técnicas a detalle para cada uno de los tipos de nodos de red, solicitados en la presente convocatoria.

Niveles de Redundancia para Alta Disponibilidad del Servicio

- La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V** proveerá todos los niveles de redundancia necesarios para asegurar la alta disponibilidad y contempla los siguientes niveles de redundancia:

Redundancia en Hardware

- Redundancia en los tipos de nodos para el Núcleo (CORE TIPO 2) **Marca: Extreme Networks Modelo: BlackDiamond 8806** de la red. Los equipos propuestos cuentan con:
    - Redundancia en tarjetas procesadoras (Switch Fabric) y de control/administración.
    - Redundancia en Fuentes de Poder, que permite la agregación sobre demanda de mayor potencia, con la adición de Fuentes de acuerdo con la carga presente o agregada a la unidad. Por esta razón se requiere de equipos que cuenten con Fuentes de Poder en arreglo N+1.

- Redundancia en los tipos de nodos para el Acceso de la red **Marca Extreme Networks, Modelo Summit X45048P**. Los equipos propuestos cuentan con:
    - Redundancia en Fuentes de Poder
    - Redundancia en Software

- Los equipos propuestos para el Núcleo de la red son **Marca Extreme Networks, Modelo BlackDiamond 8806**, cuentan para la redundancia en software con las siguientesfuncionalidades:
    - Doble almacenamiento en memoria FLASH para imágenes del S.O. y archivos de configuración en la procesadora primaria.
    - Doble almacenamiento en memoria FLASH para imágenes del S.O. y archivos de configuración en la procesadora secundaria.
    - Sistema Operativo Modular compatible con la arquitectura POSIX,

con procesamiento independiente para todas las tareas que controlen los diferentes algoritmos y protocolos soportados por la unidad. Cada proceso del S.O. se ejecuta independiente, para que, en caso de falla de alguno, los demás sigan operando sin interrupción. Esto debe extenderse no solo a fallos sino también a ataques dirigidos a un protocolo en particular.

- Redundancia a Nivel de Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2) **Marca: Extreme Networks, Modelo: Summit X45048P.**
    - Los equipos requeridos para el Nivel de Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2) **Marca: Extreme Networks Modelo: Summit X45048P**, son principalmente equipos de arquitectura apilable y con enlaces de alta velocidad hacia el Nivel de Núcleo (CORE TIPO 2) **Marca: Extreme Networks Modelo: BlackDiamond 8806**. Por lo que cuentan con funcionalidades para aprovechar por lo menos dos enlaces de alta velocidad mediante la agregación.

- Descripción de los enlaces
    - Los enlaces entre los equipos de Núcleo (CORE TIPO 2) **Marca: Extreme Networks Modelo: BlackDiamond 8806** y Acceso (SWITCH DE ACCESO 48 PUERTOS POE CAPA 2) **Marca: Extreme Networks Modelo: Summit X45048P**, se entregarán con conexiones de Gigabit Ethernet en Fibra Óptica.
    - Los enlaces hacia los usuarios de la red incluyendo equipos periféricos, deberán entregarse con conexiones 100/1000BaseT.

- Calidad de Servicio
    - Las redes de la SECTUR están concebidas para tener un ambiente de red, donde varias aplicaciones vitales y servicios deben corren indistintamente por los diferentes medios de transmisión. Por lo mismo se considera una jerarquía de los mismos. Las aplicaciones de importancia crítica sensibles a retardos, como la voz (VoIP) y la transmisión de video, deben garantizarse mediante la implementación de mecanismos de Calidad de Servicio. Por lo que todos los equipos propuestos soportan al menos 8 niveles de QoS en Capa 2 definidos por el estándar IEEE 802.1p que son mapeados a los niveles en Capa 3 soportados por los esquemas el estándar DiffServ.

- Los criterios para la clasificación de tráfico son los siguientes:
    - Tráfico Explícitamente Etiquetado - (i.e. los paquetes contienen información o etiquetas que indican al equipo de red el nivel de servicio requerido)
    - Capa 2: 802.1p - De acuerdo del estándar de la evolución de Ethernet que añade distintos campos, entre ellos tres bits de prioridad, lo que permite formar una diferenciación con 8 niveles de prioridad.

Operando en Capa 2.

- Capa 3: ToS y DiffServ – ToS (Tipo de Servicio) Que dentro del paquete IP (Capa 3), que junto con la definición del estándar DiffServ, en donde se especifica la calidad de servicio requerida.
- Tráfico Implícitamente marcado, tráfico que no contiene información de QoS pero que debe ser inferida por el equipamiento de red.
- Capa 1: Por puerto físico origen.
- Capa 2: Por dirección MAC origen o destino – De la misma manera que en el rubro anterior, la dirección física de capa 2 puede proporcionar el parámetro de clasificación de tráfico.
- Capa 3: Por dirección IP origen o destino – La dirección IP es el parámetro suficiente para su clasificación por parte de los equipos de red.
- Capa 4: Por socket UDP o TCP – Análisis de los paquetes a mayor profundidad, ya que pudiera ser tráfico crítico o sin importancia y demandante en cuanto a ancho de banda, para lo cual el socket UDP o TCP proporcionan la información de la naturaleza del tráfico para su clasificación y tratada así por parte del equipamiento de red.

- Administración

Los equipos propuestos por **Soluciones Integrales SayNet S.A. de C.V** son administrados por varias vías, mismas que se describen a continuación:

- CLI, Línea de Comandos:
- La línea de comandos (command line interface) Los comandos y el lenguaje son consistentes en todos los equipos de red, presentados de una manera estructurada y amigable, además de contar con ayudas para terminación de comandos y posibles parámetros.
- De manera adicional, los equipos propuestos soportan una manera de emular la línea de comandos de los equipos actualmente instalados con excepción de los encontrados en menor cantidad en la red.
- La línea de comandos es accesada directamente mediante puerto serial, Telnet o Secure Shell para conexiones remotas seguras.

- Interface Web:
  - Los equipos también cuentan con acceso mediante una interface Web para su administración, monitoreo y configuración de manera gráfica y remota. Y cuentan con el soporte para http o https.

- Sistema de Administración de Redes

La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V.** para la Administración de Redes es de la **Marca: Extreme Networks, modelo: Ridgeline Network and Service Management Software**, esta instalada en un servidor Windows XP, Vista W7, Solaris o Linux. Además de correr como una plataforma independiente, cuenta con herramientas para:

- Administración e Inventario de dispositivos: Que puede descubrir los dispositivos ygenerar una base de datos central de los mismos. Los dispositivos son monitoreados continuamente para mantener actualizada la información.
- Administrador de Configuraciones: Que posibilite la actualización automatizada ys encilla de sistemas operativos de los equipos. Que contiene un directorio local con las distintas versiones utilizadas. Que archiva las configuraciones de los dispositivos de red periódicamente, con el fin de contar con un respaldo actualizado de manera automática. Que automatiza la descarga de nuevas versiones del sistema operativo.
- Administrador de Alarmas: Que administra las alarmas generadas por los equipos. Que cuenta con una lista de alarmas previamente configuradas que reflejan los eventos más comunes. Que pueden configurarse alarmas personalizadas para eventos específicos con sus respectivos umbrales para cubrir necesidades específicas. Genera una bitácora de los eventos registrando parámetros particulares como hora, criticidad, etc. y se maneja un código de colores para su rápida revisión. Las alarmas también pueden provocar respuestas automáticamente como envió de correos electrónicos, alarmas sonoras, o ejecución de un script para su ejecución en los equipos de la red.
- Sesiones de Administración Remota: Desde esta herramienta se pueden abrir sesiones de telnet, SSH o web. Adicionalmente, la plataforma de administración de red permite la invocación de una sesión de administración remota mediante un navegador web.
- Gestionador de Scripts de Configuración. Se cuenta con un editor de scripts de configuración, y desde esta plataforma de administración despliega hacia los equipos de la red y programar o disparar su ejecución.
- Presentación Gráfica: La plataforma presenta gráficamente imágenes de los equipos y sus componentes como módulos de interfaz, tarjetas centrales, fuentes de poder, ventiladores, puertos físicos, etc. Al seleccionar los distintos elementos, presenta información y estado de los mismos. Adicionalmente se genera una representación topológica de la red física.
- Generador de Reportes: Mismo que puede generar reportes, como: listados de vlans, historiales de alarmas, errores de transmisión, etc. Estos reportes pueden ser presentados de manera gráfica, en tablas, o exportados en distintos formatos para su uso en otras aplicaciones.
- Estadísticas en Tiempo Real: Cuenta con un sistema que genera histogramas que reflejen estadísticas en tiempo real, sobre puertos y dispositivos que reflejen la utilización de los mismos.
- Visualizador de Topología de Red: Servicio que muestra de manera gráfica la topología de la red, en la que se pueden identificar las VLANs configuradas en la red, mostrando los puertos, enlaces y dispositivos de la

VLAN seleccionada en el visualizador.

El Sistema de Administración de Redes propuesto por **Soluciones Integrales SayNet S.A. de C.V.** es **Marca: Extreme Networks, Ridgeline Network and Management center** es repositorio de TRAPS vía SNMP; administra la red LAN y la red WLAN vía SNMP. Adicionalmente puede monitorear cualquier dispositivo compatible con MIB II.

El Sistema de Administración de Redes propuesto por **Soluciones Integrales SayNet S.A. de C.V. Marca: Extreme Networks, modelo: Ridgeline Network and Service Management Center** actúa como syslog server, para almacenar los event logs de todos los dispositivos que apunten al servidor de administración.

El Sistema soporta los protocolos RMON, SNMPv1/v2 y SNMPv3 Vía RMON se deben graficar tasas de errores de tx, errores de rx, errores de fragmentación, errores de colisión o CRC.

El ahorro de energía contempla:

- Ahorro de energía en los equipos tipo chasís con fuentes en arreglo N+1 para garantizar consumo de energía sobre demanda. Los equipos de Núcleo (Core), cuentan con un mecanismo de hibernación que se activa cuando no haya tráfico en algún puerto de red. Al detectarse tráfico, los puertos de manera automática e imperceptible por los usuarios y aplicaciones.

2.1.2 Características Técnicas

EQUIPOS A NIVEL DE NÚCLEO DE LA RED (CORE TIPO 2) de Marca: Extreme Networks Modelo: BlackDiamond 8806, PROPUESTOS POR SOLUCIONES INTEGRALES SAYNET S.A. DE C.V. cuentan con las siguientes características:

ARQUITECTURA Y CAPACIDADES:

- Equipo modular de al menos cuatro ranuras para interfaces de servicio.
- Cuenta con desempeño de al menos 1.9 Tbps de conmutación.
- Soporta una capacidad de reenvío de paquetes de al menos 1400 Mpps.
- Ofrece al menos 250 Gbps por ranura.
- Arquitectura sin bloqueos (Non-blocking)
- Soporte de interfaces 1, 10 GE.
- Soporte de tarjetas de procesamiento redundantes.
- Soporte de fuentes de poder y ventiladores redundantes.
- Soporta protocolos de enrutamiento RIP, OSPF, BGP, ruteo estático, en sus versiones más recientes estables liberadas, tanto en IPv4 como en IPv6.
- Soporte de al menos 512 mil direcciones MAC.
- Soporte de 4 mil VLANs

FUNCIONALIDADES:

- Opere con protocolos IPv4/IPv6.
- Soporte de IGMPv2/v3 y IGMPv2/v3 Snooping.
- Soporte de PIM-DM, PIM-SM y PIM-SSM.
- Capacidad instalada de VRRP o HSRP.
- Administración por Interface de línea de comandos (CLI), SNMPv2/v3.
- Soporte incluido de sFlow o similar.
- Soporte de múltiples niveles de privilegios de acceso por consola para administrador.
- Soporte de ACLs por puerto, en capas 2, 3 y 4.
- Soporte de Port Mirroring.
- Soportar encapsulamiento de VLANs Q-in-Q.
- Soporte de calidad de servicio (QoS) incluyendo:
- Clasificación de tráfico en capa 2, 3 y 4.
- Temperatura de operación de 0 a 40 °C.

SEGURIDAD:

- Soporte de autenticación 802.1X, dirección MAC y Portal.
- Soporte de RADIUS.
- Soportar defensa contra ataques de DoS.

ADMINISTRACIÓN Y MANTENIMIENTO

- Soporte de SNMP v1, v2c y v3.
- Soporte de servidor externo de NTP.
- Soporte de gestión a través de línea de comando (CLI) o vía web.
- Soporte de administración por puerto de consola, Telnet y SSH
- Soporte de FTP y TFTP
- Soporte de registros de operaciones de usuarios.

EQUIPOS SWITCH DE ACCESO 48 PUERTOS POE CAPA 2, PROPUESTOS POR SOLUCIONES INTEGRALES SAYNET S.A. DE C.V., SON MARCA: EXTREME NETWORKS MODELO: SUMMIT X450-48P Y X460-48P, cuentan con las siguientes características:

ARQUITECTURA Y CAPACIDADES

- Están equipados con 48 puertos 10/100/1000 BaseT.
- Cuentan con desempeño de al menos 250 Gbps de conmutación.
- Soportan una capacidad de reenvío de paquetes de al menos 130 Mpps.
- Soporte de 48 puertos PoE de manera simultánea.
- Soporte al menos cuatro puertos SFP compartidos
- Soportan protocolos de enrutamiento RIP y ruteo estático.
- Soporte de al menos 8 mil direcciones MAC.
- Soporte de 4 mil VLANs
- Soporte de apilamiento o Stacking de 8 unidades, con velocidad de al menos 40 Gbps.

FUNCIONALIDADES

- Opere con protocolos IPv4/IPv6.
- Soporte de IGMPv2/v3 y IGMPv2/v3 Snooping.
- Soporte de PIM-SM y PIM-SSM.
- Capacidad instalada de VRRP o HSRP.
- Administración por Interface de línea de comandos (CLI), SNMPv2/v3.
- Soporte incluido de sFlow o similar.
- Soporte de múltiples niveles de privilegios de acceso por consola para administrador.
- Soporte de ACLs por puerto, en capas 2.
- Soporte de Port Mirror.
- Soporte de calidad de servicio (QoS) incluyendo:
- o Clasificación de tráfico en capa 2.
- Soporte de ITU-Y.1731, y 802.1ag para detención de fallas.
- Temperatura de operación de 0 a 40 °C.

SEGURIDAD

- Soporte de autenticación 802.1X, dirección MAC y Portal.
- Soporte de RADIUS.
- Soportan defensa contra ataques de DoS.

ADMINISTRACIÓN Y MANTENIMIENTO

- Soporte de SNMP v1, v2c y v3.
- Soporte de servidor externo de NTP.
- Soporte de gestión a través de línea de comando (CLI) o vía web.
- Soporte de administración por puerto de consola, Telnet y SSH
- Soporte de FTP o TFTP
- Soporte de registros de operaciones de usuarios.

2.1.3 Normas, Estándares y Protocolos

Normas, Estándares y Protocolos para todos los Switches:

- IEEE 802.1D Media Access Control (MAC) Bridges
- IEEE 802.1p Virtual Bridged Local Area Networks
- IEEE 802.1Q Virtual Bridged Local Area Networks
- IEEE 802.1ad Provider Bridges
- IEEE Std 802.3ab 1000BASE-T specification
- IEEE Std 802.3ad Aggregation of Multiple Link Segments
- IEEE Std 802.3ae 10GE
- IEEE Std 802.3z Gigabit Ethernet Standard
- IEEE 802.1ag Connectivity Fault Management
- IEEE 802.1ab Link Layer Discovery Protocol

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol
- IEEE802.1X Port based network access control protocol
- IEC 60950-1
- UL 60950-1
- CSA C22.2 No 60950-1

ESPECIFICACIONES TÉCNICAS DE LA SOLUCIÓN WLAN.
Equipo CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1

propuestas por **Soluciones Integrales SayNet S.A. de C.V.** son **Marca: Extreme Networks, modelo: XCC VE6120 para Mazaryk y Marca: Extreme Networks, modelo: C35 para Schiller y Viaducto**, realiza las funciones de control centralizados por sede, sin embargo, el tráfico de los usuarios no pasa por las controladoras y cumple con las siguientes características:

CAPACIDADES

- Soportan al menos 245 Puntos de Acceso.
- Soportan la gestión de al menos 4,000 usuarios conectados.
- Desempeño del dispositivo de al menos 3.6 Gbps
- Cuenta con al menos 6 puertos 10/100/1000 Base-T y 2 x USB Port.
- Cuenta con un puerto de consola del tipo RJ-45
- Soportar al menos 16 SSID o VNS, para las sedes de Schiller y Viaducto.
- Soportar al menos 30 SSID o VNS, para Mazaryk.

FUNCIONALIDADES

- Maneja los estándares 802.11 a/b/g/n/ac.
- Soporta balanceo de carga entre las diferentes redes.
- Soporte de un portal básico para autenticación.
- Soportar asignación dinámica de canales para optimizar la cobertura y desempeño.
- Soporte de detección, y capacidad de evitar, interferencia mediante la re-calibración de la red
- Soporta los siguientes métodos de autenticación: 802.1x, MAC, Portal Web.
- Cuenta con tecnología para el control dinámico de la radio frecuencia (RF) y reaccionar automáticamente ante eventos de ruido e interferencia.
- Cuenta con un tablero centralizado de estado de la red inalámbrica.
- Soporte de calidad de servicio QoS.
- Cuenta con políticas diferenciadas por SSID.

SEGURIDAD

- Soportar los siguientes métodos de autenticación: WEP, WPA/WPA2–PSK, WPA/WPA2 con 802.1x, WPA/WPA2.
- Soporte de RADIUS.
- Soporte de EAP-TLS, EAP-TTLS, EAP-SIM, EAP-FAST, PEAP
- Soporte para detección y prevención de intrusiones de nueva generación estable.

ADMINISTRACIÓN Y MANTENIMIENTO

- Soporte de SNMPv1/v2/v3
- Soporte de CLI e interfaz gráfica.

Equipo PUNTOS DE ACCESO TIPO 1

La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V.** son **Marca: Extreme Networks, modelo: AP3935i-ROW** son equipos con desempeño para cubrir escenarios típicos de oficinas o espacios con menos de 30 usuarios concurrentes y cumplen con las siguientes características:

CAPACIDADES

- Soporte de 802.11a/b/g/n/ac.
- Soporte de MIMO de al menos 4x4
- Soportar al menos 16 SSID.
- Soportar alimentación PoE o PoE+.
- Pueden operar en la banda de 2.4 GHz y en la banda de 5.0 GHz.
- Soportan dos puertos GE BaseT 10/100/1000.

FUNCIONALIDADES

- Cuenta con mecanismos de optimización de la interfaz aire, para mejorar la experiencia de los usuarios.

SEGURIDAD

- Soporta los siguientes métodos de autenticación: WPA, WPA2 (AES), 802.11i, 802.1x, IPSec, IKEv2, PKCS #10, X509 DER / PKCS#12, SSL, WPA/WPA2 Empresarial.
- Soporte para detección y prevención de intrusiones de nueva generación estable.

ADMINISTRACIÓN Y MANTENIMIENTO

- Soporte de gestión a través de línea de comando (CLI) o vía web.

2.1.3 Normas, Estándares y Protocolos

Normas, Estándares y Protocolos para la controladora y los Puntos de Acceso:

- Exclusivo para Puntos de acceso: IEEE 802.11a, 802.11ac, 802.11b, 802.11g, 802.11n.
- IEEE 802.11a, 802.11ac, 802.11b, 802.11e, 802.11g, 802.11i, 802.11n, para la controladora.
- UL 60950–1, para la controladora.
- FCC Part 15, para la controladora.
- EN 55022, para la controladora.
- CISPR 24, para la controladora.

2.1.4 Manuales y Documentación

Soluciones Integrales SayNet S.A. de C.V. incluye copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada.

2.2 Servicio de Seguridad Perimetral

El servicio incluye como mínimo los elementos de hardware, software y funcionalidades requeridas en el presente anexo técnico. Como referencia y para garantizar la operación del servicio de seguridad de red, **Soluciones Integrales SayNet S.A. de C.V.** ofrece en su propuesta, soluciones en donde el fabricante **FORCEPOINT** esta ubicado y reconocido dentro del cuadrantes de Gartner o en algún otro reporte reconocido por la industria a nivel internacional.

Soluciones Integrales SayNet S.A. de C.V. incluye para el Servicio Administrado de Seguridad Perimetral una carta **de fabricante membretada** en la cual señale que cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante, firmada por la persona autorizada por el fabricante de la solución de **FORCEPOINT** propuesta.

2.2.1 Servicio de Firewall/IPS/Filtrado de Contenido.

Soluciones Integrales SAYNET S.A. de C.V. incluye en su propuesta, todo el Licenciamiento, Hardware y Software necesario, para proporcionar de inicio, la totalidad de Servicios de Seguridad con funcionalidades asociadas de IPS, Filtrado de Contenido WEB que se requieran, conforme a los perfiles y cantidades indicadas para cada tipo de Firewall. Soporta configuraciones en alta disponibilidad solo para el sitio de Mazaryk.

2.2.1.1 Funcionalidades de los equipos

La solución propuesta por Soluciones Integrales SayNet S.A. de C.V se compone de **2 Equipos Marca: FORCEPOINT Next Generation Firewall (NGFW), modelo: NGFW 1065 en clúster para Mazaryk y 2 equipos Marca: FORCEPOINT Next Generation Firewall (NGFW), modelo: NGFW 1035 en standalone, uno para Schiller y otro Viaducto,** que cumplen con las siguientes características:

I. Control de políticas

a) Permite a los usuarios configurar políticas de seguridad en función del tiempo, usuario / grupo de usuarios / grupo de seguridad, protocolo de capa de aplicación, ubicación geográfica, dirección IP, puerto, grupo de nombre de dominio, categoría de URL, tipo de acceso.
b) Son capaces de manejar protocolos tales como RADIUS o KERBEROS.

II. Enrutamiento

a) Admite rutas estáticas, enrutamiento basado en políticas y protocolos de enrutamiento dinámicos como OSPF, BGP en sus últimas versiones estables.
b) El enrutamiento basado en políticas admite las siguientes condiciones coincidentes: dirección IP de origen, dirección IP de destino, tipo de servicio, tipo de aplicación, usuario/grupo de usuarios/grupo de seguridad, interfaz de entrada y prioridad DSCP.
c) Opera con protocolos IPv4/IPv6.

III. Protocolos Avanzados de VPN

a) Especificaciones IKE
   i. Versión 1, Versión 2
   ii. Modo de Negociación: Main, Aggressive
   iii. Encriptación: AES-256, AES-128, 3DES, DES
   iv. Autenticación: vía clave compartida o por certificado.
   v. Integridad Hash: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5.
   vi. vi. Grupo DH: 1,2,5,14,15,16,18,19,20,21

b) Especificaciones IPSec:
   i. Modo de encapsulación: Transport, Tunnel
   ii. Protocolo de seguridad: ESP, AH.
   iii. ESP Encriptación: AES-GCM-128, AES-GCM-256, AES-256, AES-128, 3DES, DES
   iv. ESP Autenticación: DES, 3DES, AES-GCM-128 , AES-GCM-256.
c) GRE
d) VPN SSL

i. Portal Web para acceso a servicios basados en HTTP y HTTPS a través de formas predefinidas y formas libres de URL
ii. Plataformas soportadas con cliente:
   a. Android
   b. Mac OS X
   c. Windows

IV. Identificación de aplicaciones

a) El sistema identificará, categorizará, controlará y visualizará tráfico de más de 7000 aplicaciones de manera granular por usuario, grupos de usuarios y, horarios.
b) La identificación de la aplicación será independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.

V. IPv6

a). Soporta el protocolo IPv6.

VI. Control de tráfico

a) Admite políticas de control de tráfico basadas en el protocolo de la capa de aplicación, incluida la configuración del ancho de banda máximo, el ancho de banda garantizado y la prioridad del tráfico del protocolo.
b) Admite garantía de ancho de banda basada en usuarios y direcciones IP.
c) Admite el tráfico basado en la ubicación geográfica y el análisis de amenazas.

VII. Gestión de políticas

a) Admite el filtrado de URL.
b) Es compatible con SafeSearch para filtrar el contenido no saludable devuelto por los motores de búsqueda como Google.
c) Las reglas de firewall tendrán vigencia con base a fechas (incluyendo día, mes y año).

VIII. NAT

a) Admite funciones NAT completas.
b) Permite hacer traslación de direcciones estático, uno a uno. Hacer traslación de direcciones dinámico, muchos a uno.

IX. Prevención de intrusiones y antivirus.

a) Admite la personalización de plantillas de políticas de prevención de intrusiones basadas en escenarios.
b) Admite el filtrado basado en nombres de dominio malintencionados para bloquear C&C.
c) Admite protección contra malware para protocolos como HTTP/HTTPS, FTP, SMTP, POP3, IMAP.
d) Soporte de detección y bloqueo de ataques.
e) Cuenta con la funcionalidad de detección de anomalías y evasiones (AET - Técnicas Avanzadas de evasión) validadas como mínimo por NSS Labs
f) Tiene la capacidad de identificar como mínimo 800 millones de técnicas avanzadas de evasión

X. Protección de seguridad de tráfico cifrado.

a) Descifra el tráfico HTTPS, POP3S e IMAPS y realiza filtrado de datos, auditoría y protección de seguridad en el tráfico descifrado.
b) Descifra el tráfico y lo refleja en dispositivos de terceros para auditoría y detección de seguridad.

XI. Gestión Centralizada.

a. Admite la actualización mediante una unidad flash USB para reducir los costos de O&M.
b. Soporta los protocolos SNMP, SNMPv2c o SNMPv3

XII. Selección de enlace ascendente inteligente

a) Selecciona de forma inteligente los enlaces del operador en función de las direcciones IP de destino, admite la configuración de la interfaz activa / en espera y el equilibrio de carga por porcentaje.
b) Soportar QoS basada en colas inteligentes.
c) Cuenta con conceptos de Alta Disponibilidad y Balanceo de Enlaces, y no deberá tener restricciones con respecto a la tecnología usada en la misma
d) Cuenta con mínimo 2 métodos de balanceo, tipo RTT y Ratio
e) Cuenta con conceptos de QoS (Calidad de Servicio) integrados al ambiente de SD-WAN
f) Cuenta con conceptos de priorización y clasificación de tráfico integrados al ambiente de SD-WAN
g) Tiene la capacidad de creación de gateways tanto standalone, así como en clúster, e insertarlos en el ambiente de SD-WAN

XIII. IPS

a) Proveerá control de acceso e inspección profunda del tráfico.
b) Será capaz de detectar técnicas de evasión (Fragmentación de paquetes, segmentación TCP, etc).
c) Es capaz de reducir el número de falsos positivos.
d) Es capaz de realizar análisis de protocolos.
e) Es capaz de realizar la detección de anomalías estadísticas. (Ej. Basado en la secuencia de los eventos).
f) Es capaz de almacenar la captura de los paquetes para análisis posterior.

XIV. Filtrado de Contenido.

a) El acceso de los usuarios será comparado con listas o categorías de URL´s.
b) Es capaz de notificar al usuario por mensaje en el navegador.
c) Es capaz de configurar la opción de PROXY HTTP, permitiendo declarar el PROXY HTTP dentro del EndPoint y puede ser capaz de configurar la opción de PROXY HTTP de forma transparente y mediante PROXY explicito.
d) La categorización de URL es capaz de funcionar en IPv4 o IPv6.

2.2.1.2 Características Técnicas

La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V.** cumple con las funcionalidades y características antes descritas y aplican para cada uno de los tipos de Firewall tipo 1 requeridos para los inmuebles de Viaducto y Schiller, **se proveerán 2 equipos Marca: FORCEPOINT Next Generation Firewall (NGFW), modelo: NGFW 1035 en modo standalone**, y tipo 2 para Mazaryk, **se proveerán 2 Equipos Marca: FORCEPOINT Next Generation Firewall (NGFW), modelo: NGFW 1065 en modo clúster.**

FIREWALL TIPO 1: Sitio Schiller y Viaducto

Las especificaciones son las mínimas más no limitativas.

La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V.** está integrada por **2 Equipos (unos para cada sitio) Marca: FORCEPOINT Next Generation Firewall (NGFW), modelo: NGFW 1035 en Standalone,** cumple con:

INDICADOR	REQUISITO DE ESPECIFICACIÓN TÉCNICA
Requisitos de configuración física.	18,000 túneles de VPN IPSec.
Requisitos de interfaces	12 número máximo de puertos 4 Puertos 10/100/1000 base T GE.
Requisitos de desempeño	10 Gb Rendimiento Maximo de Firewall (Throughput). 1 Gb Rendimiento en inspección (UDP 1518 bytes) 150 Mbps Rendimiento inspección SSL. 5,000,0000 Número de conexiones simultáneas. 35,000 número de conexiones nuevas por segundo. 1 Gbps IPsec VPN Throughput (AES-GCM-256). 18,000 número máximo de IPSec túneles (site to site). 5,000 número máximo de IPSec túneles (client to site).
VLANs	1024

FIREWALL TIPO 2: Sitio Central Mazarik (en HA)

Las especificaciones solicitadas, son mínimas más no limitativas en modo clúster (HA) para el sitio de Mazaryk.

La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V.** está integrada por **2 Equipos Marca: FORCEPOINT Next Generation Firewall (NGFW), modelo: NGFW 1065 en clúster,** cumple con:

INDICADOR	REQUISITO DE ESPECIFICACIÓN TÉCNICA
Requisitos de configuración física.	18,000 túneles de VPN IPSec.
Requisitos de interfaces	12 número máximo de puertos 4 Puertos 10/100/1000 base T GE.
Requisitos de desempeño	20 Gbps Rendimiento Maximo de Firewall (Throughput) 3 Gbps Rendimiento en inspección (UDP 1518 bytes) 350 Mbps Rendimiento inspección SSL. 8,000,0000 Número de conexiones simultáneas. 100,000 número de conexiones nuevas por segundo. 2.5 Gbps IPsec VPN Throughput (AES-GCM-256). ≥ 18,000 Número máximo de IPSec túneles (site to site). ≥ 5,000 Número máximo de IPSec túneles (client to site).
VLANs	1024

2.2.1.4 Manuales y Documentación

Soluciones Integrales SayNet S.A. de C.V. incluye para el servicio de Protección Perimetral una carta de fabricante membretada en la cual señale que **Soluciones Integrales SayNet S.A. de**

C.V. cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante **FORCEPOINT**, firmada por la persona autorizada por el fabricante de la solucion propuesta.

Soluciones Integrales SayNet S.A. de C.V. incluirá para el servicio de Firewall al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada **marca FORCEPOINT**.

2.2.2 Servicio de AntiSpam

La SECTUR cuenta con el servicio de correo electrónico para 1600 usuarios, con 2 servidores centralizados, en los que se concentra la entrada de todos los correos. El servicio consta de 2 sistemas de Filtrado de Contenido vía SMTP CON ANTISPAM y Antivirus para el sistema de correo de forma perimetral en appliance en esquema Activo - Activo. Incluyendo el mantenimiento del hardware y licenciamiento que se alojaran en el sitio de Mazaryk.

Se contempla que el Sistema con Antispam y Antivirus para el Sistema de Correo de forma perimetral realizara el análisis de todo el correo entrante y saliente de la organización. Es obligación de **Soluciones Integrales SayNet S.A. de C.V.** dimensionar todos los elementos requeridos para cumplir con las capacidades operativas de la secretaria a partir de la información contenida en el presente anexo técnico.

Sera responsabilidad de **Soluciones Integrales SayNet S.A. de C.V.** migrar las cuentas de correo en caso de ser necesario, a la solución de ANTISPAM propuesta.

2.2.2.1 Funcionalidades de los equipos

Soluciones Integrales SayNet S.A. de C.V. considera que para prestar el servicio proporcionará 2 equipos **Marca: Barracuda, modelo: Barracuda Email Security Gateway 600,** así como la instalación, configuración, puesta en marcha; así como el mantenimiento de los mismos durante la vigencia del contrato, en el entendido de que todos los equipos o equipo requeridos formarán parte del servicio ofrecido por parte de **Soluciones Integrales SayNet S.A. de C.V.** y que la convocante no adquirirá ninguno de los mismos.

La solución anti-spam propuesta por **Soluciones Integrales SayNet S.A. de C.V.** integrada por 2 equipos **Marca: Barracuda, modelo: Barracuda Email Security Gateway 600** está basada en un servicio usando un dispositivo de hardware, totalmente administrable de forma remota por **Soluciones Integrales SayNet S.A. de C.V.** y que radicará físicamente en las instalaciones de la SECTUR, el cual estará configurado en Alta Disponibilidad.

2.2.2.2 Características Técnicas

La solución propuesta por Soluciones Integrales SayNet S.A. de C.V. cumple las siguientes funciones sobre las cuales trabaja la solución:

- Filtrado de Anti-Spam en correo.
- Filtrado de Anti-Virus en correo.

- Hacer reglas por IP, dominio, usuarios y extensión de anexos o cualquier cadena de texto en un mensaje de correo.
- Reglas basadas en formato MIME.
- Reglas basadas en listas de bloqueo o de no-bloqueo, por IP, dominio, o remitente.
- Creación de cuarentenas o carpetas de auditoría de correo en base a reglas del Antispam de correo. Mismas que deberán ser reciclables a intervalos de tiempo determinado por la SECTUR.
- Creación de listas negras o blancas independientes por usuario, accesibles por los mismos vía Web.
- Creación de políticas a nivel global por grupos o por usuario.
- Envío de mensajes de aviso de correo en cuarentena, personalizado a los usuarios, donde éstos puedan decidir qué hacer con su propia cuarentena.
- Sistema de respaldo de configuración de la solución.
- Protección anti-relay para correo de entrada o de salida.
- Sistema de revisión de mensajes en cuarentena basada en queries, por remitente, asunto, destinatario o IP, para su consulta, que permita revisar adjuntos y cuerpos de mensaje, en formato texto y html.
- Sistema de revisión de log´s de entrada y salida de tráfico de correo que permita realizar búsqueda de palabras, para su rápida consulta.
- Sistema de análisis de correo no entregado temporalmente o en cola de salida.
- Sistema de análisis de tipos de archivos para uso y creación de formatos MIME.
- Sistema de calificación de spam, que permita determinar que calificación corresponde al correo spam y cual al correo no-spam.
- Administración vía Web con manejo de contraseñas que puedan determinar el nivel o jerarquía de acceso para administración y/o consulta para diversos tipos de usuarios.

2.2.2.4 Manuales y Documentación

Se incluye para la solución de Antispam al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solucion ofertada por **Soluciones Integrales SayNet S.A. de C.V., marca Barracuda.**

2.3 Servicio de Protección de Usuario Final

Debido al avance de los ataques informáticos y de las mejores prácticas de seguridad, es necesario contar con una herramienta de detección, contención y respuesta de los puntos finales, recolectando, inspeccionando y centralizando la información importante que sucede en tiempo real, de tal forma que en el momento o incluso posterior a un ataque informático se pueda investigar, prevenir, contener y responder con la mayor información posible, por lo que "LA SECTUR", tiene la necesidad de proteger la información y fortalecer las zonas de riesgo de la infraestructura conectada en red que utilice servicios educativos. A la fecha se han venido incrementando los ataques de red, los cuales afectan vulnerabilidades de sistemas operativos, plataformas de desarrollo, versiones de sistemas, de negación de servicio o sobre escaneo de puertos y debilidades de sistemas y aplicaciones, fueron contenidos por la seguridad perimetral.

2.3.1 Funcionalidades de los equipos

Así mismo, la solución propuesta por **Soluciones Integrales SayNet S.A. de C.V.** es de **Marca: Kaspersky, modelo: Kaspersky Endpoint Security for Business** contempla una solución de software antivirus para un número de máquinas de 1150 equipos.

2.3.2 Características Técnicas

La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V.,** es Marca: Kaspersky, modelo: Kaspersky Endpoint Security for Business y cumple con las siguientes características:

- Protección para estaciones, dispositivos móviles y servidores contra todo tipo de amenazas de Internet: virus, gusanos, troyanos, phishing y spam en todas capas de la red.
- Análisis de todos los mensajes transmitidos a través de los servidores de correo.
- Procesamiento de mensajes, bases de datos y otros objetos en los servidores de correo / Domino
- Protección contra ataques phishing y spam.
- Bloqueo de correo masivo (spam) y epidemias virales
- Escalabilidad
- Instalación y administración centralizadas
- Protección proactiva contra programas desconocidos
- Seguridad al trabajar en redes WiFi
- Escaneado al vuelo de tráfico del correo e Internet.
- Reversión de cualquier cambio malicioso realizado en el sistema
- Redistribución inteligente de recursos durante el escaneado completo del sistema
- Puesta en cuarentena de objetos infectados y sospechosos
- Sistema para informes sobre el estado del sistema
- Actualización automática de las bases de datos.
- Compatible con cualquier sistema operativo, Estaciones de trabajo: (incluyendo 64bit) y Linux, Dispositivos móviles, Servidores de archivos: Microsoft Windows (incluyendo 64bit), y Linux, Servidores de correo y servidores para grupos: Microsoft Domino, Linux (Sendmail, Qmail, PostfixyExim).

2.3.4 Manuales y Documentación

La solución propuesta incluye para la solución de Antivirus una carta del fabricante membretada en la cual señala que **Soluciones Integrales SayNet S.A. de C.V.** cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante **BARRACUDA**, firmada por la persona autorizada por el fabricante.

Soluciones Integrales SayNet S.A. de C.V incluye para la solución de Antivirus al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada **marca BARRACUDA**.

2.4 Servicio Administrado de Respaldos

Los servidores y equipos de cómputo de los cuales se requiere el respaldo de información se encuentran ubicados en diferentes redes sin ningún dominio **Soluciones Integrales SayNet S.A. de C.V. propone su solución de Marca: ArcServe, modelo: Arcserve® Unified Data Protection que** suministrará todos los elementos físicos y lógicos para la implementación de un sistema de respaldo central que realice sus actividades de manera desatendida y programada.

2.4.1 Funcionalidades de los equipos

La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V,** cumple con las siguientes funcionalidades:

Los servidores de los cuales se requiere el respaldo de información se encuentran ubicados en diferentes redes sin ningún dominio por lo que la solución propuesta por **Soluciones Integrales SayNet S.A. de C.V. Marca: ArcServe, modelo: Arcserve® Unified Data Protection** suministra todos los elementos físicos y lógicos para la implementación de un sistema de respaldo central que realice sus actividades de manera desatendida y programada.

La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V. Marca: ArcServe, modelo: Arcserve® Unified Data Protection cumple las siguientes Generalidades de los respaldos:**

Permite respaldo de sistemas operativos Windows Server 2008 en adelante y Linux Server de las distribuciones de CentOS, Debian, Ubuntu y RedHat en entorno físico y virtual sobre Hyper-V y Vmware.
Soporta respaldos/recuperación en unidades de cinta Overland y NAS.
Opera con de duplicación y compresión.
Opera con catálogo y base de datos central.
Opera con consola central de administración.
Opera con integración a Directorio Activo de Microsoft.
Permite recuperación de sistemas de archivos completos basados en fecha de respaldo.
Permite la recuperación granular de archivos basados en fecha de respaldo.
Opera mediante esquemas de políticas de respaldo.
Opera realizando respaldos completos, incrementales o diferenciales.
Opera en base a agentes de respaldos/recuperación.
Cuenta con licencia para respaldar 20 TB comprimidos.
Soportar tamaños de bloque mínimos de 4 kb y deberá permitir seleccionar el tamaño de bloque deseado.
Respalda simultáneamente servidores en operación sin afectar la operación de las aplicaciones y servicios del servidor.

La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V, Marca: ArcServe, modelo: Arcserve® Unified Data Protection** se configurará para qué los sábados a las 20:00 horas o cuando se acuerde con la SECTUR se programe la realización de respaldos, del total de la información contenida en los servidores relacionados en este inciso cuyo volumen aproximado es de 20 TB comprimidos, sin la intervención manual de un administrador a menos que ocurra alguna contingencia extraordinaria. La información se respaldará simultáneamente de todos los servidores sin bajar ninguno de los servicios (on-line) y con usuarios haciendo uso de aplicaciones durante el proceso de respaldo. **Soluciones Integrales SayNet S.A. de C.V.** suministrará, instalará y pondrá a punto todos los agentes necesarios para que el respaldo se efectúe satisfactoriamente.

Todos los días a partir de las 23:00 horas o cuando se acuerde con la SECTUR se efectuarán respaldos incrementales o diferenciales, comprimidos, de manera automática sin la intervención manual de un administrador, a menos que ocurra alguna contingencia y la solución deberá soportar una capacidad ilimitada de agentes. La información se respaldará simultáneamente de todos los servidores sin bajar ninguno de los servicios (on-line) y con usuarios haciendo uso de aplicaciones durante el proceso de respaldo.
El agente permite al administrador la recuperación de un archivo ubicado en la unidad de respaldo del mismo equipo por fecha de respaldo.

Entre la información que al menos se reportará al administrador a través de las vías de la consola de alertamiento, se informará el resultado del respaldo, si fue realizado satisfactoriamente y el tiempo en que fue realizado o en su caso los problemas que se presentaron, la cantidad de bytes que se transmitieron y el servidor o equipo del usuario que lo efectúo.
En la consola de administración instalada en el servidor de respaldo suministrado se habilitará un servicio de Web para la administración del respaldo y restauración de la información vía html, para que el administrador de la red pueda administrar sus respaldos y recuperar su información vía internet.
Soluciones Integrales SayNet S.A. de C.V. suministrara, instalara y pondrá a punto todos los agentes necesarios para que el respaldo se efectúe satisfactoriamente.

Además del respaldo a los servidores descritos, **Soluciones Integrales SayNet S.A. de C.V.** dará respaldo a los servidores que le indique la SECTUR, siempre que en su conjunto no rebase la cantidad de 20 TB de respaldo de diferentes sistemas operativos y plataformas.

Adicional y tal como o solicita la SECTUR, en nuestra propuesta **Soluciones Integrales SayNet S.A. de C.V.** incluimos **una unidad de almacenamiento Marca: Synology**, exclusiva para los respaldos.

2.4.2 Características Técnicas

El sistema de Respaldos propuesto por Soluciones Integrales SayNet S.A. de C.V., Marca: ArcServe, modelo: Arcserve® Unified Data Protection cumple con las

capacidades siguientes:

- Proteger diversos tipos de nodos de origen, incluyendo el nodo basado en el agente, el nodo sin agentes, CIFS, Exchange Online, SharePoint Online, OneDrive, etc.
- Realiza la copia de seguridad de datos en servidores de punto de recuperación.
- Replica datos de copia de seguridad en servidores de puntos de recuperación remotos y locales.
- Archiva datos.

- **Copia:**
  - Archivos de origen seleccionados a una ubicación de la copia de seguridad secundaria.
  - Puntos de recuperación a ubicaciones locales como la carpeta de recursos compartidos.

- **Crea**
  - Máquinas de Virtual Standby a partir de datos de copia de seguridad en el hipervisor local (Hyper-V, y Vsphere
  - Máquina virtual instantánea en el hipervisor local (Hyper-V o Vsphere

- **Restaura**
  - Datos de copia de seguridad y realiza una reconstrucción completa.
  - Objetos de correo electrónico y objetos que no lo son de Microsoft Exchange mediante la utilidad Restauración Granular de Exchange.

- **Es compatible con**
  - La administración basadaen roles
  - La instantánea de hardware
  - Prueba de recuperación asegurada para los puntos de recuperación.

Para la Unidad de respaldo **Soluciones Integrales SayNet S.A. de C.V.** contemplo una unidad de almacenamiento **NAS, Marca: Synology,** como dispositivo de almacenamiento conectado a la red LAN, con las siguientes características:

- En este sistema de almacenamiento NAS se hará el respaldo de todos los servidores físicos o virtuales de la SECTUR, Las características técnicas mínimas de la unidad de almacenamiento NAS son:

  I. Capacidad de 64 TB útiles en Raid 5 para el inmueble de Masaryk.
  II. Memoria interna de 2 GB DDR3L, con posibilidad de expansión hasta 16 GB.
  III. Al menos 2 interfaces de red de 1 Gbps conector RJ-45.
  IV. Al menos 1 Puerto USB 3.0.

V. Soporte de hasta 4 discos internos de SSD/HDD SATA de 2.5" o 3.5 ".
VI. RAID 0, 1, 5, 6 y 10.
VII. Protocolos de servicio: CIFS/SMB, AFP, NFS, HTTP y HTTPS y FTPS.
VIII. Integración con Directorio Activo
IX. Soporte de virtualización con VMware Sphere, Hyper-V, Citrix, OpenStack
X. Consola de administración en idioma español
XI. Gestión de Almacenamiento:
   a. Tamaño máximo de volumen individual: 108TB
   b. Número máximo de volúmenes internos: 512
   c. Máximo de iSCSI Target: 32
   d. Máximo de iSCSI LUN: 256
   e. Compatibilidad con clon/instantánea de iSCSI LUN
XII. Software y licencia de administración y operación integrada al hardware.

2.4.4 Manuales y Documentación

Se incluye para la solución de respaldos una carta de fabricante membretada en la cual señale que **Soluciones Integrales SayNet S.A. de C.V.** cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante **ARCSERVE**, firmada por la persona autorizada por el fabricante.
Soluciones Integrales SayNet S.A. de C.V. incluye para la solución de respaldos al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada **ARCSERVE**.

2.5 Servicio de Infraestructura de Servidores

La SECTUR tiene la necesidad de la adquisición o arrendamiento de servidores tipo gabinete o enclosure de servidores (Blade), para dar soporte a los distintos servidores de aplicaciones internas y externas de la SECTUR

Servidor tipo Blade

La solución de servidores tipo Blade propuesta, **Soluciones Integrales SayNet S.A. de C.V.** incluye 10 servidores tipo blade **Marca: HP, modelo: HPE BladeSystem c7000 Enclosure,** con las siguientes características:

DESCRIPCIÓN	GABINETE O ENCLOSURE DE SERVIDORES TIPO BLADE
Características mínimas	**Soluciones Integrales SayNet S.A. de C.V.** proporcionará la infraestructura de servidores tipo blade deberá de considerar el gabinete o enclosure para este tipo de servidores con las siguientes características mínimas: Gabinete o enclosure que soporte o aloje servidores tipo navaja o blade con mínimo 16 bahías para el alojamiento de 10 de los servidores. Para montaje en rack standard de 19" Sistema de chasis de al menos 10 unidades de rack

	Incluiye mínimo 1 módulos de administración de todos los elementos incluidos en el gabinete o enclosure. Incluye al menos 1 puerto de video que permita la conexión de un monitor para la administración local y remota del gabinete o enclosure. Incluye bahías o slots para la instalación de elementos de conexión a red de datos redundantes con mínimo 2 puertos de conectividad Ethernet 10GB Ethernet.
Bahías o slots	Mínimo 10 bahías para servidores blade o nodos utilizables. Capacidad de integración hot swap de los servidores o nodos. Soportar procesadores E5-2697 v3. Se debe considerar que los Slots deben contar con la siguiente capacidad en memorias RAM como mínimo: Slot 1: 192Gb Slot 2: 512 Gb Slot 3: 512 Gb Slot 4: 256 Gb Slot 5: 256 Gb Slot 6: 192 Gb Slot 7: 512 Gb Slot 8: 512 Gb Slot 9: 256 Gb Slot 10: 64 Gb Soporta virtualización con Hiper-V y VSphere. Soporta al menos 500 GB de disco duro en configuración RAID de preferencia con almacenamiento en SAN.
Fuentes de poder	Incluye la mínima cantidad de fuentes de poder soportadas con redundancia, necesarias para que el chasis opere en su carga de trabajo total, es decir, todos los servidores y opciones de conectividad instaladas. Redundancia de fuentes de poder N+1. Tecnología Hot Swap.
Módulo de gestión y administración	Botón de encendido. Gestión centralizada de todos los servidores Blade o nodos. Herramientas de gestión y administración centralizada con interfaz gráfica y acceso remoto. Cuenta con software de administración remota embebido y con un puerto de red dedicado que permita contar con el monitoreo de los elementos de hardware, firmware; así como el manejo de alertas que emita el sistema.
Ventiladores	Incluye la mínima cantidad de ventiladores soportada con redundancia que permita que el chasis opere en su carga total de trabajo y enfriamiento para todos los servidores Blade o nodos. Redundancia de fuentes de poder N+1. Tecnología Hot Swap.
Módulos o slots para conectividad LAN	Incluye dos módulos o slots exclusivos para la interconexión LAN del chasis Cada módulo es escalable, de alto desempeño y baja latencia 1/10GB Ethernet. Todos los puertos internos y externos están licenciados y habilitados para su uso. Desempeño de al menos 110 Tbps. Incluye la instalación y configuración de los equipos en el chasis.

Módulos de interconexión para conectividad de almacenamiento SAN	Incluye mínimo 2 módulos exclusivos para la interconexión SAN del chasis. Los puertos operan entre 8 Gbps a 16 Gbps. Todos los puertos internos y externos estan licenciados y habilitados para su uso. Incluiye la instalación y configuración de los equipos en el chasis.
Sistema de almacenamiento.	Incluiye sistema de almacenamiento con capacidad de: 60 TB usables configurados en RAID 6. La conectividad es mediante cables de fibra óptica redundante. Soporte comunicación por canal de fibra e iSCSI. Ventiladores redundantes HotSwap. Permite operar esquemas de Thin y Think provisioning. Es compatible con sistemas operativos Windows Server 2008 en adelante. Es compatible con sistemas operativos Linux Centos, Debiam, Ubuntu y RedHat. Todos los puertos internos y externos estan licenciados y habilitados para su uso. Incluye la instalación y configuración de los equipos. Incluye todos los insumos de instalación necesarios y para la interconexión del sistema NAS vía Red.

Soluciones Integrales SayNet S.A. de C.V. considera licenciamiento para hipervisor VMware VSphere 7X y el VCenter correspondiente para 4 servidores blade como parte del servicio para la solución de Blades y el servidor donde se albergara dicha licencia de virtualización..

Servidores Tipo Microserver

La solucion propuesta por **Soluciones Integrales SayNet S.A. de C.V., incluye 4 equipos Marca: HP, modelo: HPE ProLiant MicroServer Gen10 Plus**, los cuales cuentan con las siguientes características:

- Procesador: Xeon Quad Core 3.40 GHz o superior
- Memoria RAM: 16 GB
- Disco Duro: 1 TB

Soluciones Integrales SayNet S.A. de C.V., incluye 3 servidores tipo Torre **marca DELL PowerEdge T350** con las siguientes características:

- Procesamiento: Un procesador físico con 8 núcleos y 3 GHz. no mayor a dos años de liberación de la serie por parte del fabricante.
- Memoria RAM física: 64 GB.
- Sistema de disco en RAID 5 con capacidad 2 TB.
- Red: 2 tarjetas para RJ-45 de 1 GB de ancho de banda.
- Alimentación eléctrica: Una fuente para voltajes 110/220 autosence con nema estándar nacional.

Así mismo, **Soluciones Integrales SayNet S.A. de C.V** proveerá el soporte y mantenimiento correctivo a los servidores propiedad de la SECTUR siguientes:

1. Servidor marca DELL propiedad de la SECTUR:

- Marca: DELL
- Modelo: PowerEdge R640
- Etiqueta de servicio: HGDW8N2.

2. Servidor marca HP propiedad de la SECTUR:

Marca: HP
Modelo: Proliant 360 Gen10.

Soluciones Integrales SayNet S.A. de C.V. tendrá la solución de servidores tipo Blade lista y funcionando a partir del 16 de marzo 2023.

2.5.4 Manuales y Documentación

La solución propuesta por **Soluciones Integrales SayNet S.A. de C.V.** incluye: la instalación, configuración, puesta a punto e integración con los equipos de las otras partidas, realizando lo siguiente: armado de opciones y montaje en el chassis, actualización de Firmware de todos los componentes de hardware, definición de puertos de SAN y LAN, configuración del módulo de administración remota.

2.7 Servicio de Monitoreo de red y Mesa de Ayuda

2.7.1 Monitoreo de red

Soluciones Integrales SayNet S.A. de C.V. proporcionará la solución de monitoreo que permita alertar en tiempo real los dispositivos, tanto aplicaciones como recursos de la red de la SECTUR. Este monitoreo lo operará e instalará en la red de la institución con la finalidad de mantener la operación 7x24. El monitoreo comprenderá ese horario de servicio a través de un centro de monitoreo de **Soluciones Integrales SayNet S.A. de C.V.**, enlazándose mediante un método seguro, VPN sitio a sitio o enlace dedicado.

La SECTUR entregará durante los primeros 10 días, después de la firma del contrato, un inventario de aplicaciones, servidores, switches, ruteadores y dispositivos que necesiten ser monitoreados, a partir de esta entrega **Soluciones Integrales SayNet S.A. de C.V.** contará con 5 días naturales para la implementación de la solución de monitoreo.

2.7.1.1 Funcionalidad:

- La solución de monitoreo considera al menos 200 monitores, donde los monitores o probes, son los servidores, switches, routers y aplicaciones de la institución.
- Se entregará la administración del rendimiento o performance o detección 7x24.
- **Soluciones Integrales SayNet S.A. de C.V.** desarrollará al menos 3 tableros ejecutivos que proporcionaran una vista de negocio ejecutivo, una vista operativa y una de capacidad.
- Se detectarán eventos de seguridad en la red

2.7.1.2 Infraestructura necesaria

- **Soluciones Integrales SayNet S.A. de C.V.** proporcionará el sistema de monitoreo tanto de software y hardware para que se aloje en SECTUR en el sitio de Mazaryk.
- **Soluciones Integrales SayNet S.A. de C.V.** cuenta con un centro de monitoreo formalmente establecido y con certificaciones: **NMX-I-20000-1-NYCE-2019 | ISO/IEC 20000-1:2018** y **NMX-I-27001-NYCE-2015 | ISO/IEC27001:2013**, el centro monitorea, detecta, valida y notifica los eventos de red que sucedan en un horario 7x24 en la institución.
- **Soluciones Integrales SayNet S.A. de C.V.** proporcionará al menos 2 pantallas planas de plasma o LCD con el servicio y su respectiva tarjeta controladora con el dispositivo que emita la señal.
- **Soluciones Integrales SayNet S.A. de C.V.** cuenta con línea de atención telefónica con atención 7x24 durante la vigencia del contrato
- **Soluciones Integrales SayNet S.A. de C.V.** cuenta con un área exclusiva para el SOC la cual es independiente de las demás áreas que integran las instalaciones del licitante.
- **Soluciones Integrales SayNet S.A. de C.V.** cuenta con controles de acceso biométrico.
- **Soluciones Integrales SayNet S.A. de C.V.** cuenta con sistemas de respaldo de energía, sistemas contra incendios, sistemas de video vigilancia y CCTV.
- **Soluciones Integrales SayNet S.A. de C.V.** cuenta con enlaces redundantes de internet para garantizar la continuidad del servicio.

2.7.1.3 Notificación y Escalamiento

- **Soluciones Integrales SayNet S.A. de C.V.** notificará las alertas del sistema de monitoreo a través de alguno de los siguientes medios: correo electrónico, teléfono celular, oficina o envío de SMS durante el presente contrato.
- El escalamiento se revisará al menos cada 3 meses.

2.7.1.4 Especificaciones Técnicas

El sistema de monitoreo propuesto por **Soluciones Integrales SayNet S.A. de C.V.** está basado en una arquitectura inteligente y se compone de visualizaciones interactivas que tienen como objetivo proyectar el estatus en tiempo real de la

infraestructura de la red y de las aplicaciones críticas y cumple con las siguientes características:

- Sistema de información en base a tableros de control (DashBoard).
- Tableros de control operativos que muestran la comunicación visual efectiva y precisa de los datos de las aplicaciones en tiempo real.
- Tableros de control ejecutivos que muestran la disponibilidad de las aplicaciones de la organización en tiempo real.
- Los tableros de control almacenan y despliegan la información histórica para conocer las tendencias e indicadores para la toma de decisiones.
- El sistema debe estar desarrollado en Web 2.0 o Superior
- La extracción de información de los dispositivos y aplicaciones que se despliega en los tableros de control se realiza a través de SNMP, trap de SNMP, XML, HTML o bases de datos SQL, MySQL u Oracle.
- La extracción de información de dispositivos y aplicaciones no es intrusiva, es decir no debe instalarse algún agente.
- La agrupación de Tableros de control debe ser de acuerdo con las aplicaciones o cadenas de servicios en base a la infraestructura.
- El Monitoreo de aplicaciones a través de transacciones
- Realiza asociaciones de dispositivos de red
- Realización de guías de aplicativo de los servicios.
- Despliega la disponibilidad de servicios (el tiempo en el que está disponible el sistema o dispositivo).
- Despliega el tiempo de respuesta del sistema o dispositivo hacia el usuario final.
- Despliega el tiempo de respuesta de una transacción de punta a punta.
- Despliega la capacidad del sistema o dispositivo para ejecutar los procesos o las tareas programadas, considerando parámetros como la utilización de disco duro, memoria física, procesador o CPU.
- Despliega el porcentaje de utilización de ancho de banda de enlaces principales dentro de la red como son: Switch Core, Router, Puertos de Switch, Wireless.
- El tablero principal está diseñado estructuralmente para que despliegue los elementos productivos de la red desde las aplicaciones, telecomunicaciones y hasta el usuario final.
- Interactúa con los indicadores de niveles de servicio en tiempo real.
- Procesamiento analítico en línea de los indicadores de niveles de servicio.
- Presenta tableros sobre actividad sobre la red de acuerdo con puertos, categoría, direcciones IP orígenes y destinos, país.
- Detecta actividades sospechas sobre la red y alertar sobre las mismas.
- Cuenta con listas de amenazas que se integren al monitoreo para poder realizar análisis y detección, debe incluir al menos las siguientes listas de amenazas: direcciones IP, malware, botnet, dominios, spam, hash, URL´s y redes TOR.
- Prioriza eventos de red en base a criticidad
- Analiza bitácoras de los dispositivos de seguridad en tiempo real

- Monitoreo 7x24
  - El Centro de operaciones realizará las notificaciones de las incidencias que afectan a la infraestructura (Seguridad, Aplicativos, Telecomunicaciones) en base a un escalamiento operativo e informativo
  - El Sistema de ticket para el registro de control de cambios o mantenimiento a los sistemas y dispositivos.
  - Notificación de incidencias vía telefónica, correo electrónico y vía SMS
  - Reportes de disponibilidad de servicios semanales, mensuales y bimestrales.
  - Monitoreo de disponibilidad de servicios desde internet
  - Monitoreo de disponibilidad de servicios vía VPN

2.7.2 MESA DE AYUDA

Soluciones Integrales SayNet S.A. de C.V. proporciona un servicio de mesa de ayuda para recibir, dar seguimiento, resolver y cerrar tickets de las solicitudes de servicio, incidentes, monitoreo de seguridad y monitoreo de red que se contemplan en el servicio. Este servicio operará en modalidad 7x24 durante la vigencia del contrato.

La SECTUR entregará durante los primeros 10 días, después de la firma del contrato, una lista de personal autorizado para el contacto con la mesa de ayuda de **Soluciones Integrales SayNet S.A. de C.V.**

2.7.2.1 Funcionalidad:

- **Soluciones Integrales SayNet S.A. de C.V** garantiza la disponibilidad de la mesa de ayuda que es de 7 x 24 (las 24 horas del día, los 7 días de la semana, durante la vigencia del contrato).
- **Soluciones Integrales SayNet S.A. de C.V.** realizará el soporte técnico a través de su Mesa de ayuda para la atención de reportes y fallas, en sitio o remoto conforme a su estrategia, para cumplir con los requerimientos de Nivel de Servicio.
- **Soluciones Integrales SayNet S.A. de C.V.** generará un número de ticket o número de reporte único por cada reporte que se reciba en la mesa de servicio con la finalidad de llevar un control adecuado de los tiempos de solución.
- **Soluciones Integrales SayNet S.A. de C.V** Gestionará el control de cambios, atendiendo un proceso certificado por NMX-I-20000-1-NYCE-2019 | ISO/IEC 20000-1:2018 y todos los ingenieros de la mesa de ayuda están certificados en ITIL Foundation v4.
- **Soluciones Integrales SayNet S.A. de C.V** realizará la gestión de los tickets mediante en la mesa de servicios certificada en NMX-I-20000-1-NYCE-2019 | ISO/IEC 20000-1:2018 y todos los ingenieros de la mesa de ayuda están certificados en ITIL Foundation v4, para atender las solicitudes realizadas por el personal autorizado por la SECTUR.

2.7.2.2 Infraestructura necesaria

- **Soluciones Integrales SayNet S.A. de C.V.** contará con un sistema de recepción y seguimiento de tickets
- **Soluciones Integrales SayNet S.A. de C.V** cuenta con línea de atención telefónica con atención 7x24 durante la vigencia del contrato
- **Soluciones Integrales SayNet S.A. de C.V.** cuenta con medios de comunicación para reportar fallas de equipo (Mesa de ayuda). Los medios para reportar fallas, al menos deberán ser un número convencional, un celular y un correo electrónico.

2.7.2.3 Notificación y Escalamiento

- **Soluciones Integrales SayNet S.A. de C.V.** notificará el seguimiento de los tickets mediante correo electrónico a los contactos involucrados.
- El escalamiento se revisar al menos cada 3 meses.

2.7.2.4 Especificaciones Técnicas

- **Soluciones Integrales SayNet S.A. de C.V.** realizará el soporte técnico a través de su Mesa de ayuda para la atención de reportes y fallas, en sitio o remoto conforme a su estrategia, para cumplir con los requerimientos de Nivel de Servicio.
- **Soluciones Integrales SayNet S.A. de C.V** proporcionará la administración y operación de una mesa de servicios que proporcione servicios de soporte de primer, segundo y tercer nivel para los servicios
- La mesa de servicios opera siguiendo el marco de referencia ITIL, para lo cual **Soluciones Integrales SayNet S.A. de C.V.** presentará el certificado de al menos 6 ingenieros certificados en ITIL Foundation versión 4.
- **Soluciones Integrales SayNet S.A. de C.V** entiende que los problemas que se cataloguen como de primer nivel serán resueltos directamente con el personal de la mesa de servicios con apoyo de la base de conocimientos con que cuenta.
- **Soluciones Integrales SayNet S.A. de C.V** comprende que en la atención del primer nivel de soporte si no tiene registro en su base de conocimiento, invariablemente canalizará el soporte a un técnico especializado en el tipo de problema o falla presentada.
- **Soluciones Integrales SayNet S.A. de C.V** comprende que los problemas que se cataloguen como de segundo nivel serán atendidos por personal especializado de **Soluciones Integrales SayNet S.A. de C.V.** y directamente del fabricante del hardware o software dependiendo de la naturaleza del problema reportado.
- **Soluciones Integrales SayNet S.A. de C.V** comprende que las tareas mínimas que realizará la mesa de servicio son: Recibir solicitud, abrir el ticket, registrar detalle del incidente, analizar la falla o evento, canalizar al soporte técnico

interno, escalar en su caso el incidente, dar seguimiento, informar de la solución empleada y cerrar el ticket del incidente.

- La información que contendra una solicitud de falla o evento es:
  - Número de ticket.
  - Fecha y hora de apertura del ticket.
  - Fecha y hora de inicio de reporte de la falla.
  - Nombre completo de quien levanta el reporte.
  - Nombre completo de la persona que atienda el ticket.
  - Vía de notificación de la falla o evento (correo electrónico o telefónico).
  - Datos del equipo o servicio afectado.
  - Detalle de la falla reportada.
  - Diagnóstico de la falla.
  - Solución empleada o implementada.
  - Fecha y hora de cierre del ticket.

- La mesa de servicios de **Soluciones Integrales SayNet S.A. de C.V** invariablemente por cada ticket abierto, enviará un correo electrónico a las cuentas especificadas por el administrador del contrato detallando la apertura del ticket y los correos posteriores necesarios para el seguimiento y cierre del mismo.
- **Soluciones Integrales SayNet S.A. de C.V.** generará un número de ticket o número de reporte único por cada reporte que se reciba en la mesa de servicio con la finalidad de llevar un control adecuado de los tiempos de solución.
- De manera mensual, **Soluciones Integrales SayNet S.A. de C.V.** entregará estadísticas de desempeño de servicio comparadas con los Niveles de Servicio y Niveles de Disponibilidad especificados. Las diferencias significativas serán registradas e informadas, indicando las causas de los desvíos. El reporte especificará acciones correctivas para restaurar el desempeño del servicio a los niveles comprometidos.

Escaneo de Vulnerabilidades y certificados digitales

Soluciones Integrales SayNet S.A. de C.V. a través del Centro de Operaciones de Seguridad ejecutará los escaneos de vulnerabilidades delos sitios web públicos de la SECTUR, para el cumplimiento con los estatutos del Gobierno Digital de acuerdo a lo requerido por SECTUR.
Soluciones Integrales SayNet S.A. de C.V. realizará 5 escaneos de vulnerabilidades semestralmente para 5 FQDN´s, SECTUR decidirá a que aplicaciones se deberá aplicar dicho escaneo

La solución de escaneó de vulnerabilidades de**Soluciones Integrales SayNet S.A. de C.V.** ayudará a Sectur a identificar, evaluar y emitir las posibles acciones de mitigación de los riesgos de seguridad de las aplicaciones web, incluidos los categorizados por el Proyecto de seguridad de aplicaciones web abiertas (OWASP), como Inyección de SQL, Secuencias de comandos entre sitios (XSS), Falsificación de

solicitudes entre sitios (CSRF) y otros.
La solución de escaneo de vulnerabilidades de **Soluciones Integrales SayNet S.A. de C.V.** es una herramienta no invasiva, basada en la nube, sin impacto en las operaciones de los sitios Web de Sectur.
La solución de escaneo de vulnerabilidades de **Soluciones Integrales SayNet S.A. de C.V.** escanea cualquier aplicación web que sea de acceso público, independientemente de dónde esté alojada, ubicación conjunta o en un servidor de nube pública. Las aplicaciones web pueden analizarse independientemente de si están detrás de un firewall o un equilibrador de carga.
La solución de escaneo de vulnerabilidades de **Soluciones Integrales SayNet S.A. de C.V.** no recopila ninguna información de identificación personal (PII) o registros de la base de datos de la aplicación, independientemente de si esta información es de acceso público. La solución de escaneo de vulnerabilidades de **Soluciones Integrales SayNet S.A. de C.V.** no recoge ningún dato que pueda verse comprometido. Solo emite el reporte del problema.
La solución de escaneo de vulnerabilidades de **Soluciones Integrales SayNet S.A. de C.V.** al detectar vulnerabilidades, genera automáticamente un informe detallado que permite identificar, evaluar y emitir las opciones de mitigación de las vulnerabilidades de las aplicaciones web. Durante el análisis, recopila la información sobre la aplicación para aumentar la precisión y encontrar vulnerabilidades, incluidos datos sobre las tecnologías y los componentes que utiliza la aplicación, la estructura de la aplicación, así como listas de formularios, campos y cookies de páginas.
La solución de escaneo de vulnerabilidades de **Soluciones Integrales SayNet S.A. de C.V.** realiza los escaneos a una velocidad razonable, para no sobrecargar el servidor web o infraestructura de red.
Los reportes de la solución de escaneo de vulnerabilidades de **Soluciones Integrales SayNet S.A. de C.V.** presenta un resumen ejecutivo, donde presente un vistazo rápido a su nivel de riesgo basado en las vulnerabilidades descubiertas en el sitio web de su aplicación, incluido un desglose por nivel de gravedad.
La solución de escaneo de vulnerabilidades de **Soluciones Integrales SayNet S.A. de C.V.** cuenta con el cumplimiento de Normas, esta sección del reporte mostrará si cumple con los requisitos para cumplir con varias medidas de cumplimiento con al menos uno de los estándares de la industria, que incluyen:

- OWASP Top 10 – Open Web Application Security
- PCI DSS – Payment Card Industry Data Security Standard
- HIPAA – The Health Insurance Portability and Accountability Act of 1996

El reporte de la solución de escaneo de vulnerabilidades de **Soluciones Integrales SayNet S.A. de C.V.** contiene a detalle lo siguiente:

- Nombre de la vulnerabilidad: el nombre oficial de cada vulnerabilidad se lista para cada sección numerada
- CVSS: puntuación y vector del sistema de puntuación de vulnerabilidad común de la base de datos de vulnerabilidad nacional.

- Recomendaciones de remediación: describe brevemente los métodos mediante los cuales puede mitigar esta vulnerabilidad en su sistema
- La ruta en su servidor web donde se localizó la vulnerabilidad.
- La severidad de la vulnerabilidad. Se podrá cambiar este valor, según la percepción que tenga Sectur de la gravedad.
- Confianza, probabilidad de que su sitio web tenga esta vulnerabilidad
- Detalle del problema, descripción de cómo el escáner detectó la vulnerabilidad.

2.8.1 CERTIFICADOS DIGITALES

Soluciones Integrales SayNet S.A. de C.V. entregará a través de su Centro de Operaciones de seguridad los certificados digitales SSL que SECTUR requiere para sus sitios web Certificados digitales SSL, **Soluciones Integrales SayNet S.A. de C.V.** entregará al menos 10 certificados SSL, los dominios de dichos certificados serán provistos por SECTUR de acuerdo a sus necesidades y el tamaño mínimo de clave pública tendrá que ser de acuerdo a la recomendación emitida por el ente certificador.

Adicionalmente **Soluciones Integrales SayNet S.A. de C.V.** entregará 1 certificado wildcard para el dominio sectur.gob.mx.

Dichos certificados brindan seguridad a los visitantes de las páginas web de Sectur, es una manera de decirles a nuestros usuarios que el sitio es auténtico, real y confiable para ingresar datos personales. Las siglas SSL responden a los términos en inglés (Secure Socket Layer), el cual es un protocolo de seguridad que hace que sus datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario web, y en retroalimentación, es totalmente cifrada o encriptada.

Al tener un certificado SSL confiable, nuestros datos están encriptados, con lo que podremos asegurar que nadie puede leer su contenido. Todo esto nos lleva a entender que la tecnología que brinda un certificado SSL es la transmisión segura de información a través de internet, y así confirmar que los datos están libres de personas no deseadas.
Dichos certificados SSL deben consistir en una clave pública y una clave privada. La clave pública se utilizará para cifrar la información y la privada para descifrarla. Cuando un navegador Web se dirige a uno de nuestros dominios asegurado, una presentación SSL autentica al servidor (sitio Web) y al cliente (navegador Web). Con este método de cifrado se establece una clave de sesión exclusiva y posibilita el inicio de una transmisión segura.

2.9 Soporte a SITE, cuartos de comunicaciones y Cableado Estructurado

Soluciones Integrales SayNet S.A. de C.V. otorgará a la SECTUR el servicio de protección al SITE y a dos cuartos de comunicaciones de la SECTUR, implementando las chapas electrónicas y cámaras de video en el SITE y cuartos

de comunicaciones. El sistema de control de acceso para el SITE y cuartos de comunicaciones será biométrico con teclado, lector de huellas digitales y una cámara de video vigilancia que cuenta con las siguientes características:
Sistema de vigilancia con capacidad de conexión IP y capacidad de almacenamiento de las grabaciones de por lo menos 30 días para el SITE, para lo cual el almacenamiento no podrá ser considerado mediante un medio extraíble. Búsqueda rápida de registro y verificación de usuarios que entran al sistema. Nueve modos de operaciones para controlar la operación de la puerta. Comunicación TCP/IP y comunicación Ethernet Software PLA-64 usando un PC como Anfitrión para el registro centralizado, monitoreo en red y control. Contraseña para proteger el acceso no autorizado a la red mediante un sistema de administración con acceso protegido por contraseña. Se deberá considerar un Teclado de Funciones Múltiples para poder ingresar una contraseña de acceso manual en caso de falla de lector biométrico. **La solucion propuesta es marca: NITGEN, modelo: NAC-2500 PLUS**, con teclado, lector de huellas digitales y una cámara de video vigilancia **marca: GrandStream modelo: GXV3601LL** que cumple con las características solicitadas.

Las cámaras IP de video vigilancia propuestas por **Soluciones Integrales SayNet S.A. de C.V.,** son **marca: GrandStream modelo: GXV3601LL,** cuentan con una resolución de 720x480 (NTSC D1) y de 720x576 (PAL D1)

Soluciones Integrales SayNet S.A. de C.V., proporcionará al menos 8 cámaras IP con resolución mínima 720 x 480, 5 lectores biométricos y las chapas electromagnéticas necesarias que garanticen la seguridad del SITE y los cuartos de comunicaciones. Así mismo se consideran 2 cámaras adicionales con resolución mínima 720 x 480 y las cuales podrán contar con una unidad de almacenamiento externa y alimentación POE.

Adicional, la SECTUR requiere una solución para la vigilancia exterior de los edificios de sus tres sedes Schiller, Mazarik y Viaducto, la solución propuesta por **Soluciones Integrales SayNet S.A. de C.V marca Hikvison modelo DS-2CD3356G2-ISU/SL,** cuenta con al menos 11 cámaras para exterior turret IP de 5 Megapixel con Lente 2.8 mm, 40 mts IR, protección contra agua y polvo IP67, micrófono y bocina integrados, tecnología contra falsas alarmas, rango dinámico (WDR) de 120 dB, **Soluciones Integrales SayNet S.A. de C.V,** incluye 3 cámaras para exterior turret IP de 4 Megapixel, imagen a color 24/7 para alimentación POE, con Lente 2.8 mm, luz blanca 30 mts, protección contra agua y polvo IP67, rango dinámico (WDR) de 120 dB que soporte H.265+/ONVIF, **marca Hikvison modelo DS-2CD2347G2-LSU/SL, Soluciones Integrales SayNet S.A. de C.V** considera 3 NVR con 8 canales IP con 8 Puertos POE+, que soporte cámaras con tecnología contra falsas alarmas, 2 bahías para disco duro con capacidad de almacenamiento de las grabaciones de por lo menos 30 días (debe ser interno, no se aceptan medios extraibles), switch POE hasta 250 mts, salida a través de puerto HDMI en HD y 4K. **marca Hikvison modelo DS-7608NI-K2/8P NVR, Soluciones Integrales SayNet S.A. de C.V** incluye todos los insumos, cableados, habilitadores y servicios necesarios para que la solución que proponga, quede correctamente instalada, configurada y en operación.

Soluciones Integrales SayNet S.A. de C.V., considera que el enrolamiento de los trabajadores de la SECTUR para los controles de acceso deberá ser de forma manual y total responsabilidades de **Soluciones Integrales SayNet S.A. de C.V.**

La administración centralizada de todos los componentes del SITE se llevará a cabo desde el sitio Mazaryk y este deberá tener comunicación con todas las cámaras que se instalen en los SITES de comunicaciones, por lo que **Soluciones Integrales SayNet S.A. de C.V.,** consideró todo lo necesario para la adecuada interconexión entre sitios de esta y todas las soluciones objetos del presente anexo técnico, así como todos los componentes, servicios y herramientas para mantener la integridad de los equipos de los SITES de comunicaciones como UPS, tierras y adecuaciones necesarias de acuerdo con la solución propuesta.

2.9.1 Cableado Estructurado

Soluciones Integrales SayNet S.A. de C.V. asume y entiende que el mantenimiento consiste en ajustar, reparar y/o remplazar los componentes del cableado de la red de voz y datos que se relacionan en el presente Anexo Técnico, **Soluciones Integrales SayNet S.A. de C.V.** realizará hasta 30 servicios al año y la instalación de hasta 40 nodos nuevos. que cumplan con las mejores prácticas y categorías al menos UTP Cat5e o superior.
Para los servicios de cableados estructurado podrá utilizar las verticales del instituto, pero el licitante deberá considerar la ducteria, escalerillas y todo lo necesario para la prestación del servicio de acuerdo con lo especificado en el anexo técnico.

Soluciones Integrales SayNet S.A. de C.V. realizará el servicio de cableado en la Ciudad de México, en los domicilios siguientes:

- Presidente Masaryk 172, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580.
- Schiller 138, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580.
- Viaducto Miguel Alemán 81, Colonia Escandón, Miguel Hidalgo, C.P. 11800.

2.9.1.1 Funcionalidades

Los nodos de datos que integran la red de voz y datos son alrededor de 1,200, con cable UTP de categoría 5e o superior. Cuando **Soluciones Integrales SayNet S.A. de C.V.** efectué una reparación, lo hará con materiales de las mismas características y colores que se encuentran instalados, si estos tienen números de parte hará que su cambio se apegue al mismo, respetando todos los estándares:

- TIA/EIA-568-B.
- En todo servicio de instalación de nodos de cableado estructurado, **Soluciones Integrales SayNet S.A. de C.V.** realizará el etiquetado de los componentes del cableado. Los extremos de los cables que llegan al sistema de paneles de parcheo y en el área de trabajo deberán quedar completamente identificados mediante

etiquetas.

Lo anterior a efecto de conservar la homogeneidad y calidad en la red, por lo que **Soluciones Integrales SayNet S.A. de C.V.,** deberá presentar un escrito mediante el cual manifieste que cumple con el estándar antes mencionado

Los daños o modificaciones en la estructura de la red que se hubiesen registrado a causa de negligencias, ausencia de aviso a **Soluciones Integrales SayNet S.A. de C.V.**, manipulación del cableado por parte de usuarios y nodos ausentes de canalización, no formarán parte de este contrato y con solo acreditar que se trata de estas acciones no podrá ser exigible su atención. **Soluciones Integrales SayNet S.A. de C.V.** tiene la obligación de no otorgar el servicio de red a este tipo de tramos.
Soluciones Integrales SayNet S.A. de C.V. será responsable de la limpieza de las áreas donde labore, así como de los resanes, pintura, reparación de techos y espacios que se dañen como consecuencia de los trabajos que realice.
El mantenimiento correctivo del cableado de la red deberá otorgarse cuando:

- Falle la continuidad en un nodo ubicado en las áreas de trabajo, para lo cual deberá escanearse el patch cord ubicado en el área de trabajo; en seguida el tramo del cable desde el jack a su acometida en el rack, y en tercer lugar el patch cord desde el patch panel hasta el switch. **Soluciones Integrales SayNet S.A. de C.V.** acreditará con el pentascanner la existencia de esa continuidad.

En el caso de que se tenga que sustituir un patch cord en el área de trabajo, **Soluciones Integrales SayNet S.A. de C.V.** lo sujetará al equipo mediante los mecanismos de sujeción establecidos y lo conectará al nodo. Cuando la reparación implique cambios en los tramos ubicados entre el jack y el rack se etiquetará debidamente al cable con la falla y al nuevo, además a este último se sujetará e identificará con la nomenclatura del anterior. Si la reparación implica una sustitución del patch conectado al switch este se ordenará y sujetará de la manera en que está establecido el esquema actual, cuidando estrictamente el orden debido a que se tiene una administración central de la red y a que cada nodo está ligado a un puerto especifico del switch.

Si el cambio implica ocupar una nueva posición en la regleta, **Soluciones Integrales SayNet S.A. de C.V.,** identificará debidamente los puertos, dañado y nuevo, cuidando de actualizar la numeración del nodo en las áreas de trabajo.

Soluciones Integrales SayNet S.A. de C.V. cuenta con un máximo de 48 horas hábiles para reparar satisfactoriamente un problema de continuidad en el nodo, en caso de no tener una respuesta satisfactoria la SECTUR podrá contratar un servicio externo y descontar el monto del mismo, del contrato pactado originalmente.

Cuando se presente una falla en la continuidad de los elementos de fibra

óptica tales como:

- Falla en un patch cord de fibra óptica, en cuyo caso **Soluciones Integrales SayNet S.A. de C.V.** sustituirá por otro igual etiquetando sus extremos.
- Cuando falle la continuidad de la fibra óptica que comunica los IDF's hasta el MDF's, **Soluciones Integrales SayNet S.A. de C.V.** suministrará todos los recursos necesarios para que los tres canales queden en servicio incluyendo la sustitución del tramo de fibra y la conectorización únicamente por el método epóxico o de calor.
- El tiempo en que **Soluciones Integrales SayNet S.A. de C.V.** atenderá una falla en la fibra óptica es de 4 horas y será resuelta en lapso de 20 horas hábiles a partir de la atención de la misma, o en su caso la SECTUR buscará la reparación a través de otra empresa descontando el costo del monto del contrato.

2.9.1.2 Características Técnicas

Los elementos que la SECTUR considera como parte de su sistema de cableado son los siguientes:

No.	Elemento
1	Cableado UTP de los MDF e IDF's a las áreas de trabajo
2	Escalerilla
3	Elementos de canalización desde la escalerilla o registros de crecimiento al nodo
4	Elementos de sujeción del cableado entre los que se encuentran cinchos de plástico y velcro
5	Cajas de nodos
6	Face plate
7	Jack's
8	Patch cords ubicados en las áreas de trabajo tanto de voz como de datos
9	Registros de crecimiento (es decir el crecimiento que la secretaria puede considerar para los nodos y servicios de cableado, de acuerdo con las cantidades solicitadas en los servicios del presente anexo)
10	Regletas de los registros de crecimiento
11	Gabinetes de IDF's
12	Ventiladores para los equipos del Site y Cuartos de Comunicaciones
13	Regletas de energía eléctrica
14	Racks
15	Organizadores horizontales y verticales
16	Regletas para el cableado de voz
17	Cross Conect
18	Regletas para el cableado de datos
19	Patch cords para conectar al equipo activo de datos
20	Etiquetas de los nodos, patch cord de UTP y fibra óptica, cableado, patch panels, regletas, registros, gabinetes y equipo.
21	Patch cord de fibra
22	Patch panel de fibra
23	Espirales para el soporte de fibra
24	Fibra óptica mutimodo del back bone de tres canales
25	Tubería externa de pared gruesa
26	Registros externos
27	El cross conect del conmutador hacia la vertical

2.9.1.3 Manuales y Documentación

Cuando la SECTUR requiera la reparación de nodos de datos, en algún sitio, lo solicitará por escrito a **Soluciones Integrales SayNet S.A. de C.V** y **Soluciones Integrales SayNet S.A. de C.V.** efectuará la instalación con los estándares indicados en el presente Anexo Técnico, con sus respectivas puestas a punto y actualizaciones de planos.

Los servicios de cableados serán cubiertos a solicitud de la SECTUR en las siguientes direcciones:

ID	Inmueble	Dirección física	Referencia
1	Masaryk	Presidente Masaryk 172, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580, Ciudad de México.	Esquina con Hegel.
2	Schiller	Schiller 138, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580, Ciudad de México.	Entre Homero y Ejército Nacional.
3	Viaducto	Viaducto Miguel Alemán 81, Colonia Escandón, Miguel Hidalgo, C.P. 11800, Ciudad de México.	Esquina con General Salvador Alvarado y casi esquina con Patriotismo.

3. Capacitación

Soluciones Integrales SayNet S.A. de C.V. está comprometido a realizar la trasferencia de conocimientos de las tecnologías implementadas con cupo para máximo 5 personas designadas por la SECTUR. Y será provista durante los siguientes tres meses después de terminada la implementación.

4. Entregables

Soluciones Integrales SayNet S.A. de C.V. entregará reportes que servirán como elementos de análisis y mejora a las funciones de mesa de servicio y soporte técnico que se realiza, entre los reportes que deberán generarse se encuentran:

4.1 Entregables Iniciales.

Soluciones Integrales SayNet S.A. de C.V. entregará como versión final la siguiente documentación dentro de los primeros cinco días hábiles de iniciado del servicio:

a) **Soluciones Integrales SayNet S.A. de C.V.** incluye la matriz de escalamiento, especificando los nombres completos del personal, roles, números de teléfonos fijos, números de teléfonos móviles, correos electrónicos, horario de disponibilidad de cada uno de ellos.

b) **Soluciones Integrales SayNet S.A. de C.V.** proporciona el procedimiento a través del cual resolverá cualquier falla presentada en la prestación del servicio.

Por su parte, la Secretaría de Turismo proporcionará el documento de la matriz de escalamiento del personal interno a fin de coordinar las actividades propias del servicio, en los siguientes 5 días hábiles de la adjudicación del contrato.

c) Implementación y puesta en operación:
   - **Soluciones Integrales SayNet S.A. de C.V.** entregará la memoria técnica de implementación del servicio.

Los documentos anteriores **Soluciones Integrales SayNet S.A. de C.V.** los entregará dentro de los treinta días naturales a partir de la fecha de inicio del servicio.

4.2 Entregables Mensuales

Soluciones Integrales SayNet S.A. de C.V. entregará los reportes mensuales a más tardar 5 días hábiles posteriores a la terminación del mes que corresponda.

Soluciones Integrales SayNet S.A. de C.V. entregará el reporte de Análisis estadístico, consistente en un análisis estadístico de los incidentes y solicitudes levantados y atendidos en la mesa de servicio, mismo que se presentarán agrupados por tipo de servicio, prioridad, causa o diagnóstico, grupo o personal de atención, entre otros,

Soluciones Integrales SayNet S.A. de C.V. entregará el inventario de equipos que conforman la base instalada del servicio, detallando entre otras cosas localización, número de serie, condiciones especiales de operación y fecha de implementación, destacando las altas y bajas de equipo y configuraciones que tuvieron lugar durante el mes.

Se podrán solicitar reportes bajo demanda los cuales solo podrán ser solicitados por el administrador del contrato por escrito o el mecanismo que se acuerde con **Soluciones Integrales SayNet S.A. de C.V.**, estos reportes serán integrados en los entregables mensuales en el caso de que exista alguna solicitud.

Soluciones Integrales SayNet S.A. de C.V. entregará la actualización de la memoria técnica en caso de ser necesario.

5. Niveles de Servicio

Soluciones Integrales SayNet S.A. de C.V. cumplirá con los siguientes niveles de servicio, de acuerdo a la severidad de los eventos

Nivel de Severidad	Descripción	Tipo de Solicitud	Tiempo de Atención	Tiempo de Solución
Severidad 1	Pérdida Total de la plataforma o equipo que forma parte del inventario cubierto y que origine un problema grave que interrumpa todas las funciones críticas del cliente.	Notificación del cliente vía telefónica o generación de ticket	Menor a 10 min	12 hrs
Severidad 2	Pérdida parcial de la plataforma o equipo que forma parte del inventario cubierto, el funcionamiento no está al 100%, y que origine una degradación del Servicio.	Notificación del cliente vía telefónica o generación de ticket	Menor a 10 min	18 hrs
Severidad 3	Todas las funciones de la plataforma o equipo que forme parte del Inventario cubierto opera al100%, sin embargo, el rendimiento esta degradado o muy limitado	Notificación del cliente vía telefónica o generación de ticket	Menor a 10 min	24 hrs
Severidad 4	Se refiere al grupo de cambios, consultas de características y otras preguntas de uso común y que no se consideran críticas para el desempeño de las funciones del cliente.	Notificación del cliente vía telefónica o generación de ticket	Menor a 10 min	36 hrs

Soluciones Integrales SayNet S.A. de C.V. considera 3 Ingenieros en sitio de lunes a viernes de 9 a 19 horas los días hábiles de la SECTUR, para efectuar el soporte técnico a todos los servicios solicitados en el anexo técnico y será responsabilidad entregar todo el equipamiento, herramientas , papelería, equipos de comunicación que consideren necesarios para que los ingenieros puedan llevar acabo las tareas operativas encomendadas.

Adicionalmente **Soluciones Integrales SayNet S.A. de C.V.** será responsable de proveer a los ingenieros todo el equipo de protección necesario para salvaguardar su integridad y salud ante las problemáticas de salud por el SAR-COV-2. Es importante mencionar que la secretaria cuenta con todos los protocolos sanitarios necesarios para la operación diaria de manera segura.

6. Lugar de Entrega

Los lugares de entrega de los servicios que oferta **Soluciones Integrales SayNet S.A. de C.V.** se muestra en la siguiente tabla:

ID	Inmueble	Dirección física	Referencia
1	Masaryk	Presidente Masaryk 172, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580, Ciudad de México.	Esquina con Hegel.

2	Schiller	Schiller 138, Colonia Bosques de Chapultepec, Miguel Hidalgo, C.P. 11580, Ciudad de México.	Entre Homero y Ejército Nacional.
3	Viaducto	Viaducto Miguel Alemán 81, Colonia Escandón, Miguel Hidalgo, C.P. 11800, Ciudad de México.	Esquina con General Salvador Alvarado y casi esquina con Patriotismo.

7. Transición del servicio

Treinta días naturales previos al término del contrato, **Soluciones Integrales SayNet S.A. de C.V.**y la Dependencia acordaran el proceso de transición para la prestación del servicio, con la finalidad de que no se afecte la operación y los niveles de servicio requeridos por la Dependencia correspondiente en el presente anexo técnico. Derivado de lo anterior, **Soluciones Integrales SayNet S.A. de C.V.**, se obliga a:

a) Participar en las reuniones que soliciten las Dependencias o Entidades para realizar la transición con el Proveedor adjudicado al final del contrato.

b) Durante este proceso de transición **Soluciones Integrales SayNet S.A. de C.V.**, deberá seguir prestando el servicio por un periodo máximo de treinta (30) días naturales sin costo para la Dependencia o Entidad a partir de la conclusión del contrato, el que podrá ser reducido en la medida que el nuevo Proveedor que resulte adjudicado implemente el servicio.

En caso de rescisión del contrato del servicio objeto del presente anexo técnico, este no podrá ser suspendido hasta que se asegure la transición en los términos previstos en el párrafo que antecede.

8. Condiciones y Forma de pago

Soluciones Integrales SayNet S.A. de C.V. acepta que la forma de pago será de acuerdo a lo siguiente:

Pagos a mes vencido, (en el caso del mes de febrero será por la fracción del mes) de acuerdo a la normatividad vigente y con el visto bueno de la Dirección de Control y Soporte Técnico. El importe será pagado en moneda nacional. Conforme al último párrafo del artículo 51 de la LAASSP.

La factura de los servicios realmente devengados se hará a mes vencido. Dicha factura se elaborará conforme a las disposiciones fiscales vigentes y lo señalado en las cláusulas del contrato. Se dará por recibida la factura cuando sea aceptada la totalidad de los documentos del servicio del mes que corresponda según lo especificado en el procedimiento de recepción y revisión de entregables.

El cobro de las penas convencionales y de las deducciones, se llevarán a cabo observando las disposiciones correspondientes en la materia.

En caso de detectar algún cobro indebido posterior a la aceptación del detalle del servicio respectivo, la Secretaría presentarán su inconformidad por correo electrónico o escrito a **Soluciones Integrales SayNet S.A. de C.V.**

quien deberá reintegrar la cantidad pagada en exceso conforme a lo especificado en el contrato y la normatividad que resulte aplicable.

Las aclaraciones y/o modificaciones a los detalles de los documentos del servicio y factura no impedirán que se continúe prestando el servicio.

Es requisito indispensable contar con toda la documentación solicitada para autorizar y tramitar el pago. Dicha documentación consiste en: La documentación mensual soporte del servicio, factura, nota de crédito en su caso.

La no entrega oportuna de cualquiera de los documentos anteriormente mencionados impedirá al administrador del contrato autorizar y tramitar antes las instancias correspondientes de la Secretaría el pago en los términos de la cláusula correspondiente del contrato, independientemente de aplicación de las penas convencionales y deducciones que correspondan.

9. Penas y Deductivas

Durante la vigencia del contrato, la SECTUR podrá imponer penas convencionales a **Soluciones Integrales SayNet S.A. de C.V.**, por atraso en la prestación del servicio o deducciones por incumplimiento parcial o deficiente en que pudiera incurrir **Soluciones Integrales SayNet S.A. de C.V.** respectivamente La SECTUR podrá optar entre promover su rescisión o exigir el cumplimiento del mismo, sin necesidad de intervención judicial al efecto.

1. Las penas convencionales se aplicarán por la SECTUR, a **Soluciones Integrales SayNet S.A. de C.V.** en caso de que incurra en retraso en el cumplimiento oportuno de la prestación del servicio en cuyo caso se aplicará un porcentaje del 1% por cada día natural de retraso y hasta por el 10% del monto total de los servicios no prestados oportunamente.

2. Las deducciones se aplicarán cuando a **Soluciones Integrales SayNet S.A. de C.V.** en caso de que incurra en incumplimiento parcial o deficiente en la prestación del servicio conforme a los requerimientos de calidad, contenidos y especificaciones técnicas señaladas en el contrato y su Anexo Técnico. Dicha deductiva corresponde al 1% de los servicios proporcionados parcial o deficiente por cada día natural, hasta el 10% del monto total del contrato.

Los montos a deducir se deberán aplicar en la factura que **Soluciones Integrales SayNet S.A. de C.V.** presente para su cobro, una vez que el área usuaria haya cuantificado la deducción correspondiente.

Las penas convencionales se aplicarán con base en la parte proporcional de la garantía de cumplimiento del monto total del presente contrato.

La aplicación de las penas convencionales y deducciones no son excluyentes la una de la otra, esto es. Pueden aplicarse simultáneamente y no excederán en su conjunto al monto de la fianza de garantía de cumplimiento, por lo tanto, no serán acumulativas, para los efectos de la rescisión administrativa prevista por el artículo 54 de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público y el artículo 98 de su Reglamento

Las penas convencionales serán determinadas por la SECTUR por conducto del ENLACE designado por el área usuaria en función de los servicios no prestados.

10. Perfil del licitante.

Soluciones Integrales SayNet S.A. de C.V. demostrará su especialidad, capacidad y experiencia a través de la siguiente documentación:

- Currículo de la empresa y personal calificado que acredite al menos un año de experiencia en la prestación de servicios similares a los solicitados en el presente Anexo Técnico y que contenga la lista de sus principales clientes.
- Presentamos copia simple de al menos un contrato celebrado en los últimos tres años, cuyo objeto sea igual o similar a los servicios objeto del presente ANEXO, para acreditar al menos un año de experiencia en la prestación del servicio.

Soluciones Integrales SayNet S.A. de C.V. entregará los documentos siguientes:

- Matriz de escalamiento, donde se detallarán los nombres completos del personal del proveedor, roles, números de teléfonos fijos, números de teléfonos móviles, correos electrónicos, horario de disponibilidad de cada uno de ellos.
- Procedimiento a través del cual resolverá cualquier falla presentada en la prestación del servicio.
- Plan de trabajo de implementación de todos los equipos que compongan las soluciones de seguridad informática. Este puede ser implementado en fases, las cuales podrán ser actividades paralelas o secuenciales considerando la complejidad de la infraestructura en operación. El plan de trabajo debe ejecutarse para proporcionar los servicios el 16 de marzo 2023.
- Incluirá para el servicio de Seguridad Perimetral una carta de

fabricante membretada en la cual señale que **Soluciones Integrales SayNet S.A. de C.V.** cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante **FORCEPOINT**, firmada por la persona autorizada por el fabricante de la solucion propuesta.

- Incluirá para el servicio de Seguridad Perimetral al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada.
- Para el servicio de Antispam, **Soluciones Integrales SayNet S.A. de C.V.** especificará por escrito, que su solución ofrecerá la garantía de poder detectar correctamente el correo que sea spam, combinaciones spam, virus, exploits o contenido grafico de spam.
- Incluirá para la solución de Antivirus una carta de fabricante membretada en la cual señale que **Soluciones Integrales SayNet S.A. de C.V.** cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante, firmada por la persona autorizada por el fabricante de la solución propuesta **marca KASPERSKY**.
- Incluirá para la solución de Antivirus al menos copia de los certificados de dos ingenieros calificados para implementar y soportar la solución ofertada **marca KASPERSKY**.
- Incluirá para la solución del software de respaldos una carta en papel membretado del fabricante en la cual señale que **Soluciones Integrales SayNet S.A. de C.V.** cuenta con la autorización de venta, reventa, distribución o comercialización de los productos del fabricante **ARCSERVE**, firmada por la persona autorizada por el fabricante.
- La mesa de servicios operará siguiendo el marco de referencia ITIL versión 4, para lo cual el licitante deberá presentar el certificado de al menos 6 ingenieros certificados
- Incluirá copia de certificación NMX-I-27001-NYCE-2015 / ISO/IEC 27001:2013 en su proceso de incidentes, problemas y niveles de servicio para la operación del servicio.
- Incluirá copia de certificación NMX-I-20000-1-NYCE-2019 | ISO/IEC 20000-1:2018 en sus procesos de cambios, solicitudes de servicio y niveles de servicio con los que opera la Mesa de Ayuda.

Nota: **Soluciones Integrales SayNet S.A. de C.V.** presentará estos documentos de acuerdo a lo solicitado en el procedimiento de contratación.

11. Anticipos.

No aplica.

12. Prórrogas.

No aplica

13. Garantía de cumplimiento.

Soluciones Integrales SayNet S.A. de C.V. garantizará el cumplimiento de sus obligaciones a través de una fianza por el 10 % del monto total del contrato/pedido sin considerar el IVA.

La garantía será divisible.

14. Suspensión de la prestación.

Cuando en la prestación del servicio se presente caso fortuito o fuerza mayor, o bien por causas atribuibles a la SECTUR, ésta bajo su responsabilidad podrá suspender la prestación del mismo, sin que ello implique la terminación del contrato, en cuyo caso únicamente se pagarán aquellos servicios que hubiesen sido efectivamente prestados.

Asimismo, las PARTES convienen en apego a lo consagrado en el artículo 91 del Reglamento, una vez que se acrediten los supuestos establecidos en el párrafo que antecede, las PARTES podrán modificar la vigencia del Contrato, en este supuesto se deberá formalizar a través del convenio modificatorio respectivo, no dando lugar a la aplicación de las penas convencionales por atraso de Soluciones Integrales SayNet S.A. de C.V.

Cuando la suspensión obedezca a causas imputables a la SECTUR, previa petición y justificación del proveedor, ésta reembolsará a Soluciones Integrales SayNet S.A. de C.V. los gastos no recuperables que se originen durante el tiempo que dure esta suspensión, siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con el Contrato, de conformidad con lo dispuesto por el artículo 55 Bis de la Ley.

En cualquiera de los casos previstos en esta cláusula, las PARTES pactarán el plazo de suspensión, a cuyo término podrá iniciarse la terminación anticipada del Contrato, o bien, una vez que haya desaparecido la causa que motivó la suspensión, el Contrato podrá volver a producir sus efectos legales.

La suspensión de la prestación de servicios se sustentará mediante dictamen que precise las razones o las causas justificadas que den origen a las mismas, de conformidad con lo dispuesto con el artículo 102 del Reglamento.

15. Servidor Público del área responsable de administrar y verificar el cumplimiento del contrato.

El titular en funciones de la Dirección de Control y Soporte Técnico fungirá como responsable de administrar y verificar el cumplimiento de los servicios descritos en el presente documento.

16. Normas Oficiales Mexicanas, las Normas Mexicanas y a falta de éstas, las Normas Internacionales que aplican al bien o servicio solicitado.

La mesa de ayuda de **Soluciones Integrales SayNet S.A. de C.V.** opera siguiendo el marco de referencia ITIL, para lo cual **Soluciones Integrales SayNet S.A. de C.V.** presentará el certificado de al menos 6 ingenieros certificados en ITIL Foundation v4.

La mesa de ayuda de **Soluciones Integrales SayNet S.A. de C.V.** opera en sus procesos de cambios, solicitudes de servicio y niveles de servicio el esstándar NMX-I-20000-1-NYCE-2019 | ISO/IEC 20000-1:2018, para lo cual se presentará el certificado NMX-I-20000-1-NYCE-2019 | ISO/IEC 20000-1:2018 vigente.

El servicio de monitoreo de red de **Soluciones Integrales SayNet S.A. de C.V.** opera en sus procesos de incidentes, problemas y niveles de servicio bajo el estándar NMX-I-27001-NYCE-2015 / ISO/IEC 27001:2013, para lo cual se presentará el certificado NMX-I-27001-NYCE-2015 / ISO/IEC 27001:2013 vigente.

17. Señalar si se entrega, en su caso, muestras y/o catálogos respectivos (fotografías, folletos, diseños, planos, entre otros.

Soluciones Integrales SayNet S.A. de C.V. entregará las hojas técnicas del fabricante donde especifique las características de los equipos propuestos, para lo cual se entregará una relación de las especificaciones técnicas contenidas en el anexo técnico con la traducción simple de las especificaciones contenidas en la documentación oficial del fabricante y se adjuntaran los documentos del fabricante en su idioma original señalando las especificaciones técnicas referidas en español. No se aceptarán cartas de fabricante señalando especificaciones no soportadas contenidas en el presente anexo técnico.
Los certificados que avalan la capacidad de los recursos humanos podrán ser presentados en su idioma original identificando claramente el nombre del recurso propuesto.

Diseño de la Solución.

Soluciones Integrales SayNet S.A. de C.V. propone el siguiente diseño de la solución distribuida en los tres sitios de la Secretaría de Turismo.

Mazaryk

Soluciones Integrales SayNet S.A. de C.V. proporcionará a la Sectur la herramienta de borrado seguro Blancco Drive Eraser es una sólida solución de borrado de datos para entornos de almacenamiento, servidores, portátiles y PC.

Para que la Sectur pueda crear y mantener políticas de seguridad sólidas y salvaguardar sus datos confidenciales dentro de la infraestructura de la solución

propuesta por Soluciones Integrales SayNet S.A. de C.V. Con Blancco Drive Eraser, la Sectur puede agregar un nivel adicional de protección a sus políticas de seguridad borrando permanentemente datos confidenciales de HDD y SSD, incluidas NVM, servidores. El proceso de sobrescritura seguro desinfecta los datos en una amplia variedad de dispositivos de almacenamiento para que Soluciones Integrales SayNet S.A. de C.V. pueda garantizar el borrado seguro de los datos activos de la solución propuesta por Soluciones Integrales SayNet S.A. de C.V.

La solución propuesta para el Núcleo de Core tipo 2 por Soluciones Integrales SayNet S.A. de C.V., propone el equipo Marca: Extreme Networks, modelo: BlackDiamond 8806, el cual cumple las características solicitadas en el Anexo Técnico, cuenta con una tarjeta de puertos Ethernet de 48 puertos PoE modelo: G48Tc(PoE), la cual será utilizada para la conexión de dispositivos mediante Ethernet y brinda energía sobre los puertos Ethernet (PoE), una tarjeta de puertos de 24 Puertos a fibra modelo: G24Xc incluye 24 transeivers SFP-based 1-gigabit, la cual será utilizada para la interconexión a fibra de los 5 IDF´s del sitio Mazaryk (MDF-PB, IDF-P2, IDF-P5, IDF-P8, IDF-P11) con el CORE tipo 2 formando un anillo con los 5 IDF´s para garantizar la redundancia hacia cada uno de los IDF´s del sitio de Mazaryk, dos tarjetas de administración o procesadoras modelo: MSM-48c, con lo que se garantiza la redundancia en la administración del Switch CORE Tipo 2, y tres fuentes de poder HOT SWAP modelo: PS-2431 con las tres fuentes se obtiene la redundancia en la alimentación del Switch de CORE tipo 2. En el Núcleo de Core tipo 2, se configurarán las VLANs y el direccionamiento IPv4, para que este Núcleo de Core tipo 2, sea el Gateway de las diferentes redes de la Secretaría en el sitio de Mazaryk.

La solución propuesta para el SWITCH DE ACCESO 48 PUERTOS POE CAPA 2 por Soluciones Integrales SayNet S.A. de C.V., propone 21 equipos Marca: Extreme Networks, modelo: Summit X450e-48p, el cual cumple las características solicitadas en el Anexo Técnico, la distribución de los switches será de la siguiente manera; para el MDF-PB se realizará una interconexión de 7 Switches Summit X450e-48p y 1 switch Summit X450e-48p (DMZ) , los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada en el primero y ultimo switch de la apilamiento de Switches Summit X450e-48p, para el IDF-P2 se realizará un apilamiento de 5 Switches Summit X450e-48p, los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada en el primero y ultimo switch de la apilamiento de Switches Summit X450e-48p, para el IDF-P5 se realizará un apilamiento de 4 Switches Summit X450e-48p, los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada en el primero y ultimo switch de la apilamiento de Switches Summit X450e-48p, para el IDF-P8 se realizará un apilamiento de 3 Switches Summit X450e-48p, los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada en el primero y ultimo switch de la apilamiento de Switches Summit X450e-48p, para el IDF-P11 se realizará un apilamiento de 3 Switches Summit X450e-48p, los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada en el primero y ultimo switch de la apilamiento de Switches Summit X450e-48p.

La solución propuesta para el Sistema de Administración de Redes por Soluciones Integrales SayNet S.A. de C.V., propone 1 software Marca: Extreme Networks, modelo: Ridgeline Network and Service Management Software y será implementado en un PC con las siguientes características: Procesador: Intel Core i5 a 2.0 GHz, Memoria RAM: 8 GB, Disco Duro: 1 Tb HDD, el cual cumple con las características solicitadas en el Anexo Técnico. Este sistema de administración de redes administrará los equipos de red de los tres sitios Mazaryk, Schiller y Viaducto.

La solución propuesta para la CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1 por Soluciones Integrales SayNet S.A. de C.V., propone 1 equipo Marca: Extreme Networks, modelo: WLAN XCC VE6120, la cual cumple las características solicitadas para la CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1.

La solución propuesta para los PUNTOS DE ACCESO TIPO 1 por Soluciones Integrales SayNet S.A. de C.V., la distribución se acoplará a las necesidades de ubicación de los PUNTOS DE ACCESO TIPO 1, conforme a las necesidades de la Sectur, los PUNTOS DE ACCESO TIPO 1, son 65 equipos Marca: Extreme Networks, modelo: AP3935i-ROW y serán implementados de acuerdo a las ubicaciones que la Sectur indique. Los AP3935i-ROW, serán conectados y alimentados por los switches Summit X450e-48p, y serán controlados por la CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1 Marca: Extreme Networks, modelo: XCC VE6120 en la sede de Mazaryk y la CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1 marca Extreme Networks modelo C35 en las sedes de Schiller y Viaducto.

La solución propuesta para el Servicio de Firewall/IPS/Filtrado de Contenido, FIREWALL TIPO 2 por Soluciones Integrales SayNet S.A. de C.V., para la sede de Mazaryk, propone 2 equipos Marca: FORCEPOINT Next Generation Firewall (NGFW), modelo: NGFW 1065, los cuales cumplen con las características solicitadas en el Anexo Técnico, el modo de operación del clúster de firewalls NGFW 1065, será en Activo-Pasivo, en este clúster de Firewalls NGFW 1065, se activaran las funcionalidades de IPS para la prevención de ataques informáticos y Filtrado de Contenido, para el control de acceso a sitios web y aplicaciones, así mismo será el concentrador de VPNs Site-to-Site y Client-To-Site, en el clúster de Firewalls NGFW 1065, se controlaran los enlaces de Internet, L2L, MPLS, etc, con los que cuenta la Secretaría y será el único punto de contacto entre las redes internas de la Secretaría y los enlaces de Internet de la Secretaría garantizando la seguridad de acceso de los usuarios hacia redes públicas y protegiendo los portales web de la Secretaria de los accesos desde el Internet, la Gestión Centralizada, se realizará con el software FORCEPOINT NGFW Security Management Center (SMC) y será instalado como un ambiente virtual controlado por VMWare ESXi 6.5, sobre un servidor con las siguientes características: marca: HP, Modelo: Proliant DL20 Gen9, Procesador: 4 CPUs Intel Xeon CPU E3-1220 v6 @ 3.00 Ghz, memoria ram: 8 Gb, disco duro 4.5 TB, este sistema de Gestión Centralizada, será el encargado de gestionar los firewalls de los sitios de Mazaryk, Schiller y Viaducto.

La solución propuesta para el Servicio de AntiSpam, por Soluciones Integrales SayNet S.A. de C.V., propone 2 equipos Marca: Barracuda, modelo: Barracuda Email Security Gateway 600, los cuales cumplen con las características solicitadas en el Anexo Técnico, el modo de operación del clúster de Appliance de AntiSpam

Barracuda Email Security Gateway 600, será en Activo-Activo este clúster AntiSpam protegerá el envío y recepción de correo electrónico vía SMTP del sistema de correo electrónico de la Sectur.

La solución propuesta para el Servicio de Antivirus, por Soluciones Integrales SayNet S.A. de C.V, propone 1150 licencias de Protección de EndPoint Marca: Kaspersky, modelo: Kaspersky Endpoint Security for Business, el cual cumple con las características solicitadas en el Anexo Técnico, el despliegue de los agentes de Antivirus Kaspersky Endpoint Security for Business, se realizará a través de la integración del directorio activo de la Secretaría, con apoyo del Administrador del Directorio Activo de la Sectur se realizará la distribución del agente a los endpoints, la consola de administración para los agentes Kaspersky Endpoint Security for Business será Kaspersky Security Center, y será instalado como un ambiente virtual controlado por VMWare ESXi 6.5, sobre un servidor con las siguientes características: marca: DELL, Modelo: Power Edge R730, Procesador: 10 CPUs Intel(R) Xeon(R) E5-2630 v4 @ 2.20 Ghz, memoria ram: 16 Gb, 2 discos duros 1 TB.

La solución propuesta para el Servicio de Respaldos, por Soluciones Integrales SayNet S.A. de C.V., propone el software de respaldos Marca: ArcServe, modelo: Arcserve® Unified Data Protection, el cual cumple con las características solicitadas en el Anexo Técnico, la solución de respaldos de Arcserve® Unified Data Protection, funciona con y sin agentes, la operación de respaldos se definirá en conjunto con el cliente para la opción que más le convenga con o sin agente, la solución de Arcserve® Unified Data Protection, cuenta con licenciamiento para respaldar 20Tb con compresión, la solución será instalada como un ambiente virtual controlado por VMWare ESXi 6.5, sobre un servidor con las siguientes características: marca: DELL, Modelo: Power Edge R730, Procesador: 10 CPUs Intel(R) Xeon(R) E5-2630 v4 @ 2.20 Ghz, memoria ram: 16 Gb, 2 discos duros 1 TB. Para garantizar el almacenamiento de los respaldos Soluciones Integrales SayNet S.A. de C.V, proporcionará una NAS con las siguientes características, Marca: Synology, Modelo: RS818+, con arreglo en disco en Raid5 quedará un espacio utilizable de 64 Tb, 2 GB DDR3L de memoria RAM (expandible a 16 GB), 4 puertos ethernet a 1GbE (RJ-45), esta unidad NAS será el repositorio exclusivo de los Respaldos que la herramienta de respaldos Arcserve® Unified Data Protection realizados para la Sectur.

La solución propuesta para el Servicio de Servidores Tipo Blade, por Soluciones Integrales SayNet S.A. de C.V., propone 1 equipo Marca: HP, modelo: HPE BladeSystem c7000 Enclosure, con 16 Bahías y con 10 Blades Modelo: HP Proliant BL460c Gen 9, con las siguientes características por Blade, Procesadores: 2 Intel(R) Xeon(R) E5-2697 v3 con 14 Cores a 2.6 Ghz, 6 fuentes de poder Hot Swap, Memoria RAM: 4 slots 512Gb, 3 slots hasta 256 Gb y los slots restantes al menos 64 Gb, el sistema de almacenamiento para este chasis serán: Marca: HP Modelo: Storage Virtual 4330 en Cluster(10 Unidades), el arreglo de discos en RAID 6 con espacio usable de 60Tb, con dos fuentes de poder Hot Swap por unidad, la interconexión entre el HPE BladeSystem c7000 Enclosure y el almacenamiento Storage Virtual 4330 en Clúster se realiza a través de tarjetas 10 Gb Fiber Channel.

La solución propuesta para el Servicio de Servidores Tipo Torre, por Soluciones Integrales SayNet S.A. de C.V., propone 3 equipos Marca: DELL PowerEdge T350

con las siguientes especificaciones: Procesamiento: Un procesador físico con 8 núcleos y 3 GHz. no mayor a dos años de liberación de la serie por parte del fabricante, Memoria RAM física: 64 GB, Sistema de disco en RAID 5 con capacidad 2 TB, Red: 2 tarjetas para RJ-45 de 1 GB de ancho de banda, Alimentación eléctrica: Una fuente para voltajes 110/220 autosence con nema estándar nacional.

La solución propuesta para el Servicio de Servidores Tipo MicroServer, por Soluciones Integrales SayNet S.A. de C.V., propone 4 equipos Marca: HP, modelo: HPE ProLiant MicroServer Gen10 Plus, con las siguientes características, Procesadores: 1 Xeon E-2224 @ 3.40 GHz con 4 Cores, Memoria RAM: 16 Gb, Disco Duro: 1 Tb.

La solución propuesta para el Servicio de Servidores, por Soluciones Integrales SayNet S.A. de C.V., proporcionará el soporte a los siguientes servidores propiedad de la Sectur:

1. Servidor marca DELL propiedad de la SECTUR:
   - Marca: DELL
   - Modelo: PowerEdge R640
   - Etiqueta de servicio: HGDW8N2.

2. Servidor marca HP propiedad de la SECTUR:
   - Marca: HP
   - Modelo: Proliant 360 Gen10.

Soluciones Integrales SayNet S.A. de C.V. considera una licencia para virtualización de servidores como parte del servicio para la solución de Blades que permitirá la virtualización de 4 hosts, para el servidor que la SECTUR destine.

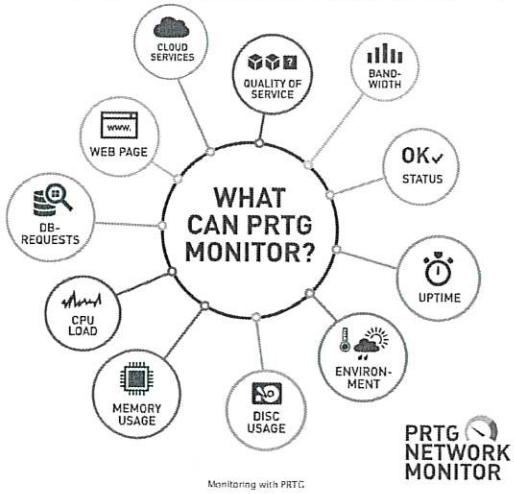
La solución propuesta para el Servicio de Monitoreo de red y Mesa de Ayuda, por Soluciones Integrales SayNet S.A. de C.V., propone el sistema de monitoreo Marca: Paessler AG, modelo: PRTG Network Monitor, con las siguientes características:

- PRTG Network Monitor sigue y analiza los flujos red y no requiere software de terceros
- Monitorea y alerta sobre tiempos de inactividad o servidores lentos
- Monitoreo del estado del sistema de sus diversos dispositivos de hardware
- Monitoreo de dispositivos de red, visibilidad de ancho de banda
- Monitoreo de aplicaciones
- Monitoreo de servidores virtuales
- Supervisión del acuerdo de nivel de servicio (SLA)
- Supervisión del uso del sistema (por ejemplo, cargas de CPU, memoria libre, espacio libre en disco)
- Monitoreo del rendimiento de la base de datos y valores de la tabla
- Monitoreo del servidor de correo electrónico y revisión de varias soluciones de respaldo
- Supervisión del entorno físico de su red
- Clasificación del tráfico de la red por origen o destino, así como por contenido
- Descubre actividad inusual, sospechosa o maliciosa con dispositivos o usuarios
- Medición de parámetros de calidad de servicio (QoS) y voz sobre IP (VoIP)
- Descubrimiento y evaluación de dispositivos de red

- Recopilación de información del sistema para varios tipos de hardware
- Encuentra relaciones inesperadas entre los componentes de su red para detectar posibles problemas de seguridad y evaluar el uso real de su red y hardware
- Monitoreo a prueba de fallas mediante una configuración de clúster de conmutación por error

Para la solución de monitoreo propuesta por por Soluciones Integrales SayNet S.A. de C.V, se instalará una PC en las instalaciones de Mazaryk, con un agente o sonda de PRTG Network Monitor en una PC con las siguientes características; CPU Intel Core i3 @ 2.6 Ghz, Ram: 32 Gb y disco duro de 500Gb, este agente mostrará las alertas en tiempo real de los dispositivos y aplicaciones de la Sectur este mismo agente tendrá comunicación directa con el sistema de monitoreo central del SOC de Soluciones Integrales SayNet S.A. de C.V, con esta configuración se tendrán dos Probes de Monitoreo el local en las instalaciones de la Sectur y el Remoto en el sistema de monitoreo central del SOC de Soluciones Integrales SayNet S.A. de C.V. La comunicación de la información del agente de monitoreo local en la Sectur será enviada al sistema de monitoreo central del SOC de Soluciones Integrales SayNet S.A. de C.V, vía VPN con lo que se garantiza la seguridad de la información de la Sectur.

Soluciones Integrales SayNet S.A. de C.V, proporcionará a la Sectur 2 Pantallas Marca: SONY Bravia de 32 pulgadas Modelo: KDL-32EX520 y Soluciones Integrales SayNet S.A. de C.V, realizará los trabajos de montaje de las pantallas en acuerdo con personal de la Sectur.



La resolución de cambios, altas y bajas en la configuración de la solución propuesta por Soluciones Integrales SayNet S.A. de C.V., así como el monitoreo se realizará a través del SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V. en un horario de atención 7x24x365 es decir de lunes a domingo las 24 horas del día, se proporcionará la capacitación al personal de Sectur sobre el proceso de generación de solicitudes de servicio (Altas, Bajas y Cambios) dentro del sistema de Mesa de Ayuda del SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V.

El SOC-NOC-HORUS ofrecido por Soluciones Integrales SayNet S.A. de C.V. cuenta con una amplia gama de certificaciones tecnológicas, que le permite abarcar prácticamente

cualquier solución en el mercado. Soluciones Integrales SayNet S.A. de C.V. cuenta con las certificaciones globales y nacionales NMX-I-20000-1-NYCE-2019 | ISO/IEC 20000-1:2018 para garantizar la entrega y operación de servicios de tecnologías de la información, NMX-I-27001-NYCE-2015 | ISO/IEC27001:2013 para garantizar la disponibilidad, integridad y confidencialidad de la información, CERT – Carnegie Mellon que certifica al SOC NOC Horus como una agencia de respuesta a incidentes a nivel global. Soluciones Integrales SayNet S.A. de C.V. cuenta con procesos y políticas apegadas a los marcos normativos más reconocidos a nivel internacional que garantizan las mejores prácticas en el dimensionamiento, implementación, operación y entrega de los servicios ofertados.

Para garantizar la disponibilidad del servicio Soluciones Integrales SayNet S.A. de C.V. cuenta con las siguientes características:

- Enlaces redundantes de Internet
- Redundancia en equipos de comunicaciones
- Planta de Emergencia
- UPS
- Sistema de enfriamiento para control de temperatura y extintores en caso de incendios
- Acceso Biométrico
- Sistema de CCTV
- Servicio de Mesa de Ayuda 7x24

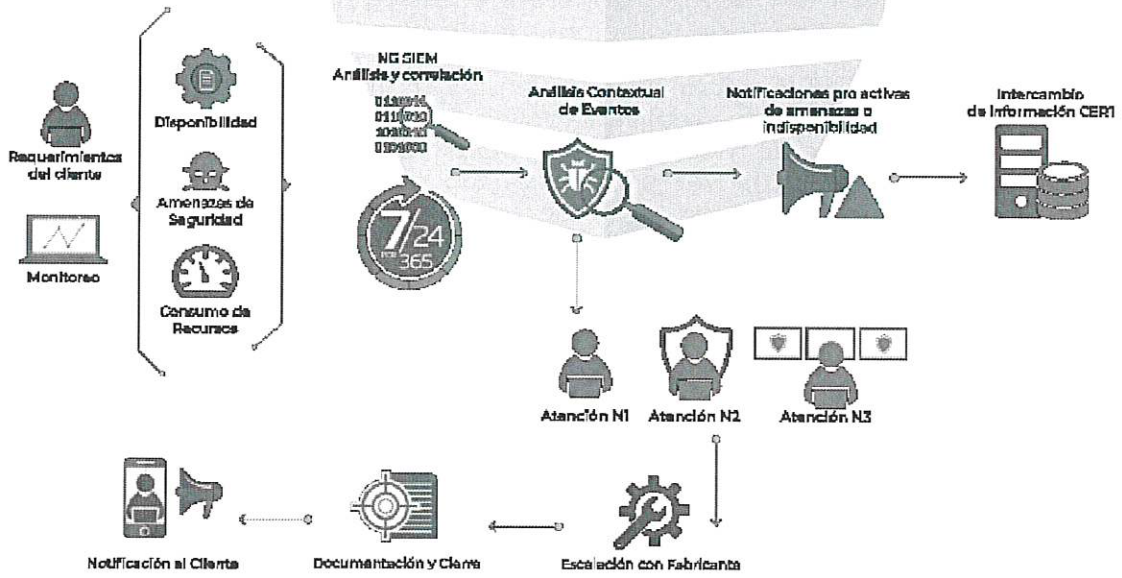
Como valor agregado a la Sectur, Soluciones Integrales SayNet S.A. de C.V, brindará e incorporará el servicio de monitoreo de Seguridad con la herramienta de correlación del SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V. con el cual se fortalecerá la seguridad de las operaciones de la Sectur, los elementos que se integraran al sistema de monitoreo de Seguridad son los firewalls de los 3 sitios, el sistema de AntiSpam y la Consola de Antivirus.

Matriz de escalamiento.

Niveles de Escalación	Responsable	Horario	Puesto
1er Nivel	**Ingenieros SOC/Mesa de Ayuda** [redacted] ncalderon@saynet.com.mx [redacted] emendieta@saynet.com.mx [redacted] drodas@saynet.com.mx [redacted] hflores@saynet.com.mx [redacted] emendoza@saynet.com.mx **Ingenieros Implementadores y Soporte SOC** Líneas Directas (Numero de Teléfonos Móviles): [redacted]	24 hrs	Analistas de Seguridad
	Ingenieros en Sitio [redacted] gromero@saynet.com.mx Cel: [redacted] [redacted] flicona@saynet.com.mx Cel: [redacted]	Lunes a Viernes 09:00 hrs a 19:00 hrs	Ingenieros de Soporte de Primer Nivel en Sitio

Niveles de Escalación	Responsable	Horario	Puesto
2do Nivel	**Ingenieros en Sitio 2do Nivel** [redacted] baranados@saynet.com.mx Cel: [redacted] atencion@noc-horus.com.mx 5871-6090 Ext. 1411, 1422 y 1511	24 hrs	Ingeniero de Segundo Nivel
3er Nivel	**Dirección de Ingeniería** [redacted] rgutierrez@saynet.com.mx [redacted] Raul Eleno Garcia releno@saynet.com.mx 5871-6090 Ext. 1411 [redacted]	24 Hrs.	Administrador de Plataforma / Director de Ingeniería
Ingeniero de Calidad	**Ingeniero Auditor Líder de ISO27001** [redacted] jpacheco@saynet.com.mx Ingeniero de apego a las mejores prácticas en la operación del servicio.	Lunes a viernes 09:00 hrs a 19:00 hrs	Ingeniero de Calidad

PROCESO DE ATENCIÓN



La solución propuesta para el Servicio de Escaneo De Vulnerabilidades y certificados digitales, por Soluciones Integrales SayNet S.A. de C.V, propone el sistema de Escaneo de Vulnerabilidades del SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V. La solución de escaneo de vulnerabilidades se ubica

en las instalaciones del SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V., ayudará a la Sectur a reducir su exposición a amenazas al permitirle evaluar y responder a los cambios en su entorno en tiempo real y priorizando el riesgo a través de vulnerabilidades, configuraciones y controles.

Las violaciones de datos están creciendo a un ritmo alarmante. Su superficie de ataque cambia constantemente, el adversario se vuelve más ágil que sus equipos de seguridad y su junta quiere saber qué está haciendo al respecto. Nexpose le brinda la confianza que necesita para comprender su superficie de ataque, concentrarse en lo que importa, y crear mejores resultados de seguridad.

No puede reducir el riesgo si no puede encontrarlo, validarlo y contextualizarlo. La solución de escaneo de vulnerabilidades ubicada en las instalaciones del SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V., descubre dinámicamente su superficie de ataque completa y encuentra las vulnerabilidades. Ayudará a la Sectur a que comprenda su exposición a amenazas determinando si sus vulnerabilidades pueden explotarse y si se implementan sus controles de compensación exitosamente.

La solución de escaneo de vulnerabilidades está ubicada en las instalaciones del SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V., se ejecutará bajo demanda siendo solicitada por el personal de la Sectur en la herramienta de mesa de ayuda del SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V.

Una vez terminado el escaneo de vulnerabilidades el SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V., generará y entregará el reporte vía la mesa de ayuda del SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V.

La solución propuesta para el Servicio de certificados digitales, por Soluciones Integrales SayNet S.A. de C.V, propone realizar la solicitud del o los certificados que requiera la Sectur en el sistema de mesa de ayuda SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V. una vez en un tiempo máximo de 12 Horas se generará el certificado digital solicitado por la Sectur mismo que será entregado vía el ticket en la mesa de ayuda del SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V.

Soluciones Integrales SayNet S.A. de C.V, entregará a la Sectur 10 certificados SSL y un certificado wildcard emitidos por la entidad certificadora.

La solución de Soporte a SITE, cuartos de comunicaciones y Cableado Estructurado, se realizará la solicitud del servicio de cableado a reparar, ajustar y/o reemplazar que requiera la Sectur en el sistema de mesa de ayuda SOC-NOC Horus de Soluciones Integrales SayNet S.A. de C.V. una vez generado el ticket en la mesa de ayuda Soluciones Integrales SayNet S.A. de C.V., coordinara con el personal de la Sectur y el personal en sitio de Soluciones Integrales SayNet S.A. de C.V, la asistencia a sitio del personal de cableado para ajustar, reparar y/o remplazar los componentes del cableado de la red de la Sectur que fueron reportados.

El personal de Sectur proporcionará los accesos necesarios para realizar los trabajos de ajuste, reparación y/o remplazo de los componentes del cableado de

la red de la Sectur. Este apartado se incluirán las solicitudes para los 3 sitios de la Sectur, Mazaryk, Schiller, Viaducto.

Biométricos, Chapas Electromagnéticas y Cámaras IP de Video Vigilancia.

Soluciones Integrales SayNet S.A. de C.V. instalará las cámaras de videovigilancia de la siguiente forma; una Cámara IP marca: GrandStream modelo: GXV3601LL en el SITE de Planta Baja, una Cámara IP marca: GrandStream modelo: GXV3601LL vigilando a la entrada de personal de area de soporte, una Cámara IP marca: GrandStream modelo: GXV3601LL vigilando la salida de emergencia, una Cámara IP marca: GrandStream modelo: GXV3601LL vigilando la entrada de la salida de emergencia, las 4 cámaras IP a instalar cuentan con al menos una resolución 720x480, de acuerdo con la respuesta de la convocante en la Junta de Aclaraciones.

Soluciones Integrales SayNet S.A. de C.V. instalará las chapas de acceso electromagnético de la siguiente forma; una chapa electromagnética en la entrada del personal del área de soporte de la planta baja con el botón de control de salida para la misma chapa electromagnética, la segunda chapa electromagnética en la entrada del Site de la planta baja con el botón de control de salida para la misma chapa electromagnética. Los Biométricos a instalar serán de la marca: NITGEN, modelo: NAC-2500 PLUS

El sistema de administración de las cámaras de Video Vigilancia de Mazaryk y control de acceso de los biométricos de los tres sitios Mazaryk se instará en una PC en el SITE con las siguientes características: Procesador: Intel CORE i7, 32 Gb de RAM y 6 TB de Disco Duro, , las 4 cámaras IP a instalar cuentan con al menos una resolución 720x480, de acuerdo con la respuesta de la convocante en la Junta de Aclaraciones.

Schiller.

Soluciones Integrales SayNet S.A. de C.V., propone que para la comunicación entre Mazaryk y Schiller se realizará vía un enlace que será controlado por los Firewalls Instalados en los sitios de Schiller y Mazaryk. La comunicación hacia el sitio de Viaducto se enviará a Mazaryk y de Mazaryk se enviará a Viaducto.

La solución propuesta para el Núcleo de Core tipo 2 por Soluciones Integrales SayNet S.A. de C.V , propone el equipo Marca: Extreme Networks, modelo: BlackDiamond 8806, el cual cumple las características solicitadas en el Anexo Técnico ,cuenta con una tarjeta de puertos Ethernet de 48 puertos PoE modelo: G48Tc(PoE), la cual será utilizada para la conexión de dispositivos mediante Ethernet y brinda energía sobre los puertos Ethernet (PoE), una tarjeta de puertos de 24 Puertos a fibra modelo: G24Xc incluye 24 tranceivers SFP-based 1-gigabit, la cual será utilizada para la interconexión a fibra de los 5 MDF´s del sitio Schiller (MDF-PB, MDF-P3, MDF-P6, MDF-P9, MDF-PH) con el CORE tipo 2 formando un anillo con los 5 MDF´s para garantizar la redundancia hacia cada uno de los IDF´s del sitio de Schiller, dos tarjetas de administración o procesadoras modelo: MSM-48c, con lo que se garantiza la redundancia en la administración del Switch CORE Tipo 2, y tres fuentes de poder HOT SWAP modelo: PS-2431 con las tres fuentes se obtiene la redundancia en la alimentación del Switch de CORE tipo 2. En el Nucleo

de Core tipo 2, se configurarán las VLANs y el direccionamiento IPv4, para que este Núcleo de Core tipo 2, sea el Gateway de las diferentes redes de la Secretaría en el sitio de Schiller.

La solución propuesta para el SWITCH DE ACCESO 48 PUERTOS POE CAPA 2 por Soluciones Integrales SayNet S.A. de C.V , propone 14 equipos Marca: Extreme Networks, modelo: Summit X450e-48p, el cual cumple las características solicitadas en el Anexo Técnico, la distribución de los switches será de la siguiente manera; para el MDF-PB se realizará un apilamiento de 3 Switches Summit X450e-48p, los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada en el primero y ultimo switch de apilamiento de Switches Summit X450e-48p, para el MDF-P3 se realizará un apilamiento de 3 Switches Summit X450e-48p, los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada en el primero y ultimo switch de la apilamiento de Switches Summit X450e-48p, para el MDF-P6 se realizará un apilamiento de 3 Switches Summit X450e-48p, los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada en el primero y ultimo switch de la apilamiento de Switches Summit X450e-48p, para el MDF-P9 se realizará un apilamiento de 3 Switches Summit X450e-48p, los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada en el primero y ultimo switch de la apilamiento de Switches Summit X450e-48p, para el MDF-PH se realizará un apilamiento de 2 Switches Summit X450e-48p, los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra optica conectada en el primero y ultimo switch del apilamiento de Switches Summit X450e-48p.

La solución propuesta para la CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1 por Soluciones Integrales SayNet S.A. de C.V, propone 1 equipos Marca: Extreme Networks, modelo: C35 appliance la cual cumple las características solicitadas en el Anexo Técnico.

La solución propuesta para los PUNTOS DE ACCESO TIPO 1 por Soluciones Integrales SayNet S.A. de C.V, propone de forma inicial para el diseño de la solución, la distribución se acoplará a las necesidades de ubicación de los PUNTOS DE ACCESO TIPO 1, conforme a las necesidades de la Sectur, los PUNTOS DE ACCESO TIPO 1, son 19 equipos Marca: Extreme Networks, modelo: AP3935i-ROW y serán implementados de la siguiente forma; 1 AP Marca: Extreme Networks, modelo: AP3935i-ROW, para la Planta Baja, 2 APs Marca: Extreme Networks, modelo: AP3935i-ROW, para el Piso 1, 2 APs Marca: Extreme Networks, modelo: AP3935i-ROW, para el piso 2, 2 APs Marca: Extreme Networks, modelo: AP3935i-ROW, para el Piso 3, 1 AP Marca: Extreme Networks, modelo: AP3935i-ROW, para el Piso 4, 1 AP Marca: Extreme Networks, modelo: AP3935i-ROW, para el Piso 5, 2 APs Marca: Extreme Networks, modelo: AP3935i-ROW, para el Piso 6, 2 APs Marca: Extreme Networks, modelo: AP3935i-ROW, para el Piso 7, 1 AP Marca: Extreme Networks, modelo: AP3935i-ROW, para el Piso 8, 2 APs Marca: Extreme Networks, modelo: AP3935i-ROW, para el Piso 9, 1 AP Marca: Extreme Networks, modelo: AP3935i-ROW, para el Piso 10 y 2 APs Marca: Extreme Networks, modelo: AP3935i-ROW, para la Piso H, las 19 APs Marca: Extreme Networks, modelo: AP3935i-ROW, serán conectadas y alimentadas por los switches Summit X450e-48p, y serán

controladas por la CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1 Marca: Extreme Networks, modelo: C35.

La solución propuesta para el Servicio de Firewall/IPS/Filtrado de Contenido, FIREWALL TIPO 1 por Soluciones Integrales SayNet S.A. de C.V, propone 1 equipo Marca: FORCEPOINT Next Generation Firewall (NGFW), modelo: NGFW 1035, el cual cumple con las características solicitadas en el Anexo Técnico, en el Firewall NGFW 1035, se activaran las funcionalidades de IPS para la prevención de ataques informáticos y Filtrado de Contenido, para el control de acceso a sitios web y aplicaciones, así mismo será el concentrador de VPNs Site-to-Site y Client-To-Site, se controlaran los enlaces de Internet, L2L, MPLS, etc, con los que cuente la Secretaría y será el único punto de contacto entre las redes internas de la Secretaría en Schiller y los enlaces de Internet de la Secretaría garantizando la seguridad de acceso de los usuarios hacia redes públicas y protegiendo los portales web de la Secretaria de los accesos desde el Internet, la Gestión Centralizada, se realizará con el software FORCEPOINT NGFW Security Management Center (SMC) y será instalado como un ambiente virtual controlado por VMWare ESXi 6.5, sobre un servidor con las siguientes características: marca: HP, Modelo: Proliant DL20 Gen9, Procesador: 4 CPUs Intel Xeon CPU E3-1220 v6 @ 3.00 Ghz, memoria ram: 8 Gb, disco duro 4.5 TB, este sistema de Gestión Centralizada instalado en el Site del sitio Mazaryk, será el encargado de gestionar los firewalls de los sitios de Mazaryk, Schiller y Viaducto.

Biométricos, Chapas Electromagnéticas y Camaras IP de Video Vigilancia.

Soluciones Integrales SayNet S.A. de C.V. instalará las cámaras de videovigilancia de la siguiente forma; una Cámara IP marca: GrandStream modelo: GXV3601LL en el SITE de Planta Baja, la cámara IP a instalar cuentan con al menos una resolución 720x480.

Soluciones Integrales SayNet S.A. de C.V. instalará las chapas de acceso electromagnético de la siguiente forma; una chapa electromagnética en la entrada del Site de la planta baja con el botón de control de salida para la misma chapa electromagnética. Los Biométricos con teclado a instalar serán de la marca: NITGEN, modelo: NAC-2500 PLUS

El sistema de administración de las cámaras de Video Vigilancia de Schiller, se instalará en una PC en el SITE con las siguientes características: Procesador: Intel CORE i7, 16 Gb de RAM y 1 TB de Disco Duro el control de acceso del biométricos con teclado se realizará desde la PC Instalada en el site de Mazaryk, la cámara IP a instalar cuentan con al menos una resolución 720x480, de acuerdo con la respuesta de la convocante en la Junta de Aclaraciones.

Viaducto.

Soluciones Integrales SayNet S.A. de C.V , propone que para la comunicación entre Mazaryk y Schiller se realizará vía un enlace que será controlado por los Firewalls Instalados en los sitios de Viaducto y Mazaryk. La comunicación hacia el sitio de Schiller se enviara a Mazaryk y de Mazaryk se enviará a Schiller.

La solución propuesta para el Nucleo de Core tipo 2 por Soluciones Integrales SayNet S.A. de C.V , propone el equipo Marca: Extreme Networks, modelo: BlackDiamond 8806, el cual cumple las características solicitadas en el Anexo Técnico, cuenta con una tarjeta de puertos Ethernet de 48 puertos PoE modelo: G48Tc(PoE), la cual será utilizada para la conexión de dispositivos mediante Ethernet y brinda energía sobre los puertos Ethernet (PoE), una tarjeta de puertos de 24 Puertos a fibra modelo: G24Xc incluye 24 transeivers SFP-based 1-gigabit, la cual será utilizada para la interconexión a fibra del MDF a cada IDF del sitio Viaducto (CTRL_MDFPB_A, PB- CAPACITACION, IDF PISO 1) con el CORE tipo 2 formando un anillo con el CORE y cada IDF para garantizar la redundancia hacia cada uno de los IDF del sitio de Viaducto, dos tarjetas de administración o procesadoras modelo: MSM-48c, con lo que se garantiza la redundancia en la administración del Switch CORE Tipo 2, y tres fuentes de poder HOT SWAP modelo: PS-2431 con las tres fuentes se obtiene la redundancia en la alimentación del Switch de CORE tipo 2. En el Núcleo de Core tipo 2, se configuraran las VLANs y el direccionamiento IPv4, para que este Núcleo de Core tipo 2, sea el Gateway de las diferentes redes de la Secretaría en el sitio de Viaducto.

La solución propuesta para el SWITCH DE ACCESO 48 PUERTOS POE CAPA 2 por Soluciones Integrales SayNet S.A. de C.V , propone 14 equipos Marca: Extreme Networks, modelo: Summit X450e-48p, el cual cumple las características solicitadas en el Anexo Técnico, la distribución de los switches será de la siguiente manera; para el CTRL_MDFPB_A se realizará un apilamiento de 3 Switches Summit X450e-48p, los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada en el primero y ultimo switch de la apilamiento de Switches Summit X450e-48p, para el PB-CAPACITACION se conectará 1 Switch Summit X450e-48p, el mismo se unirá al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada al mismo switch Summit X450e-48p, para el IDF PISO 1 se realizará un apilamiento de 4 Switches Summit X450e-48p, los mismos que se unirán al switch de CORE Tipo2 BlackDiamond 8806, mediante fibra óptica conectada en el primero y ultimo switch de la apilamiento de Switches Summit X450e-48p.

La solución propuesta para la CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1 por Soluciones Integrales SayNet S.A. de C.V, propone 1 equipos Marca: Extreme Networks, modelo: C35 appliance la cual cumple las características solicitadas en el Anexo Técnico.

La solución propuesta para los PUNTOS DE ACCESO TIPO 1 por Soluciones Integrales SayNet S.A. de C.V, propone de forma inicial para el diseño de la, la distribución se acoplará a las necesidades de ubicación de los PUNTOS DE ACCESO TIPO 1, conforme a las necesidades de la Sectur, los PUNTOS DE ACCESO TIPO 1, son 17 equipos Marca: Extreme Networks, modelo: AP3935i-ROW y serán implementados de la siguiente forma; 3 APs Marca: Extreme Networks, modelo: AP3935i-ROW, para la Planta Baja, 6 APs Marca: Extreme Networks, modelo: AP3935i-ROW, para el Piso 1, 8 APs Marca: Extreme Networks, modelo: AP3935i-ROW, para el piso 2, serán conectadas y alimentadas por los switches Summit X450e-48p, y serán controladas por la CONTROLADORA PARA PUNTOS DE ACCESO TIPO 1 Marca: Extreme Networks, modelo: C35.

La solución propuesta para el Servicio de Firewall/IPS/Filtrado de Contenido, FIREWALL TIPO 1 por Soluciones Integrales SayNet S.A. de C.V, propone 1 equipo Marca: FORCEPOINT Next Generation Firewall (NGFW), modelo: NGFW 1035, el cual cumple con las características solicitadas en el Anexo Técnico, en el Firewall NGFW 1035, se activaran las funcionalidades de IPS para la prevención de ataques informáticos y Filtrado de Contenido, para el control de acceso a sitios web y aplicaciones, así mismo será el concentrador de VPNs Site-to-Site y Client-To-Site, se controlaran los enlaces de Internet, L2L, MPLS, etc, con los que cuente la Secretaría y será el único punto de contacto entre las redes internas de la Secretaría en Schiller y los enlaces de Internet de la Secretaría garantizando la seguridad de acceso de los usuarios hacia redes públicas y protegiendo los portales web de la Secretaria de los accesos desde el Internet, la Gestión Centralizada, se realizará con el software FORCEPOINT NGFW Security Management Center (SMC) y será instalado como un ambiente virtual controlado por VMWare ESXi 6.5, sobre un servidor con las siguientes características: marca: HP, Modelo: Proliant DL20 Gen9, Procesador: 4 CPUs Intel Xeon CPU E3-1220 v6 @ 3.00 Ghz, memoria ram: 8 Gb, disco duro 4.5 TB, este sistema de Gestión Centralizada instalado en el Site del sitio Mazaryk, será el encargado de gestionar los firewalls de los sitios de Mazaryk, Schiller y Viaducto.

Biométricos, Chapas Electromagnéticas y Cámaras IP de Video Vigilancia.

Soluciones Integrales SayNet S.A. de C.V. instalará las cámaras de videovigilancia de la siguiente forma; una Cámara IP marca: GrandStream modelo: GXV3601LL en el SITE de Planta Baja, una Cámara IP marca: GrandStream modelo: GXV3601LL en la entrada al cuarto de soporte de la Planta Baja, las cámaras IP a instalar cuentan con al menos una resolución 720x480.

Soluciones Integrales SayNet S.A. de C.V. instalará 11 cámaras de videovigilancia para exterior en las 3 sedes de la SECTUR, Masaryk, Schiller y Viaducto, de la marca Hikvision con las siguientes caracteristicas: cámara Turret IP 5 Megapixel / Lente 2.8 mm / 40 mts IR / Exterior IP67 / Micrófono y Bocina Integrado / ACUSENSE (Evita Falsas Alarmas) / WDR 120 dB

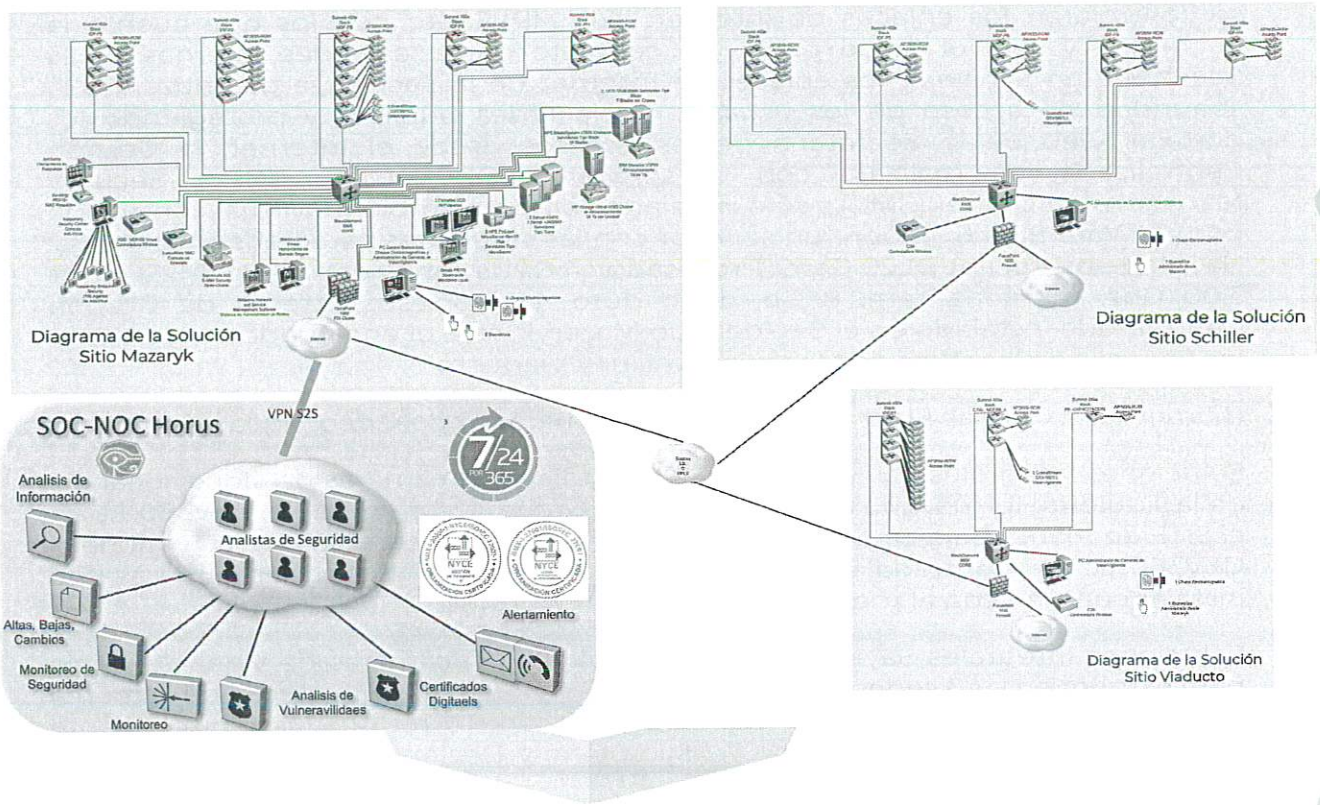
Adicionalmente Soluciones Integrales SayNet S.A. de C.V. instalará 3 cámaras de videovigilancia para exterior turret IP de 4 Megapixel, imagen a color 24/7 para alimentación POE, con Lente 2.8 mm, luz blanca 30 mts, protección contra agua y polvo IP67, rango dinámico (WDR) de 120 dB que soporte H.265+/ONVIF y considerar 3 NVR con 8 canales IP con 8 Puertos POE+, que soporte cámaras con tecnología contra falsas alarmas, 2 bahías para disco duro con capacidad de almacenamiento de las grabaciones de por lo menos 30 días

Soluciones Integrales SayNet S.A. de C.V. instalará las chapas de acceso electromagnético de la siguiente forma; una chapa electromagnética en la entrada del Site de la planta baja con el botón de control de salida para la misma chapa electromagnética. Los Biométricos a instalar serán de la marca: NITGEN, modelo: NAC-2500 PLUS

El sistema de administración de las cámaras de Video Vigilancia de Viaducto se instalará en una PC en el SITE con las siguientes características: Procesador: Intel CORE i7, 16 Gb de RAM y 2 TB de Disco Duro, el control de acceso del biométrico

se realizará desde la PC Instalada en el site de Mazaryk, las 2 cámaras IP a instalar cuentan con al menos una resolución 720x480.

Diagrama Global de la Arquitectura.



ATENTAMENTE

Lic. Elizabeth Saldaña Robles
APODERADO LEGAL
Soluciones Integrales Saynet S.A. de C.V.
esaldana@saynet.com.mx

SayNet

LICITACIÓN PUBLICA
N° LA-21-510-021000999-N-6-2023
"Solución de infraestructura de red (LAN, WIFI), seguridad perimetral y servidores"

Formato 7: Propuesta Económica

Aviso de Privacidad y Derechos de Autor

Ciudad de Mexico a 24 de febrero de 2023

FORMATO 7: PROPUESTA ECONÓMICA

SECRETARÍA DE TURISMO
P R E S E N T E

Nombre de la Empresa Licitante: Soluciones Integrales SAYNET S.A. de C.V.
Licitación Pública de Carácter Nacional Electrónica No.: N° LA-21-510-021000999-N-6-2023
Denominada: "Solución de infraestructura de red (LAN, WIFI), seguridad perimetral y servidores"

		Servicio (fracción de marzo a diciembre 2022)		
Partida	Descripción del Servicio	Fracción del mes de marzo (del 16 al 31 de marzo)	Precio Total Mensual (mes completo)	Costo total del periodo (fracción de marzo a diciembre)
UNICA	Servicio de infraestructura de red.	$ 119,963.00	$ 239,926.00	$ 2,279,297.00
	Servicio de Seguridad Perimetral (Firewall /IPS filtrado de Contenido)	$ 70,556.00	$ 141,112.00	$ 1,340,564.00
	Servicio de Antispam	$ 90,538.00	$ 181,076.00	$ 1,720,222.00
	Servicio de Antivirus	$ 55,499.00	$ 110,998.00	$ 1,054,481.00
	Servicio de Respaldos	$ 57,312.00	$ 114,624.00	$ 1,088,928.00
	Servicio de Infraestructura de servidores	$ 113,486.00	$ 226,972.00	$ 2,156,234.00
	Servicio de Monitoreo de red y Mesa de Ayuda	$ 64,308.00	$ 128,616.00	$ 1,221,852.00
	Escaneo de vulnerabilidades y Certificados digitales	$ 12,862.00	$ 25,724.00	$ 244,378.00
	Soporte a SITE, cuartos de comunicaciones y cableado estructurado	$ 61,098.00	$ 122,196.00	$ 1,160,862.00
	Subtotal	$ 645,622.00	$ 1,291,244.00	$ 12,266,818.00
	IVA	$ 103,299.52	$ 206,599.04	$ 1,962,690.88
	TOTAL	$ 748,921.52	$ 1,497,843.04	$ 14,229,508.88

Consideraciones Comerciales:

- Todos los precios están expresados en moneda nacional.
- El Monto Total Reflejado de la presente cotización incluye el IVA y los impuestos aplicables
- El servicio cotizado incluye todos los precios de los conceptos detallados en el anexo uno como una sola unidad de cobro.
- Vigencia de la cotización: 4 meses.

ATENTAMENTE

Lic. Elizabeth Saldaña Robles
APODERADO LEGAL
Soluciones Integrales Saynet S.A. de C.V.
esaldana@saynet.com.mx