CONTRATO DGRMIS- DAC-DGIT-005/2017.

CONTRATO PARA LOS "SERVICIOS ADMINISTRADOS DE SEGURIDAD PERIMETRAL" QUE CELEBRAN POR UNA PARTE EL EJECUTIVO FEDERAL POR CONDUCTO DE LA SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES, REPRESENTADA EN ESTE ACTO POR EL ING. EDUARDO JUAN GUERRERO VALDEZ, EN SU CARÁCTER DE DIRECTOR GENERAL DE RECURSOS MATERIALES, INMUEBLES Y SERVICIOS, ASISTIDO POR EL ING. RAMÓN ALEJANDRO ALCALÁ VALERA, EN SU CARÁCTER DE DIRECTOR DE ADQUISICIONES Y CONTRATOS, EL MTRO. MARIO HÉCTOR GÓNGORA PRECIADO, EN SU CARÁCTER DE DIRECTOR GENERAL DE INFORMÁTICA Y TELECOMUNICACIONES Y EL LIC. GREGORIO CASTILLA MUÑOZ, EN SU CARÁCTER DE DIRECTOR DE INFRAESTRUCTURA TECNOLÓGICA, COMO ADMINISTRADOR DEL PRESENTE CONTRATO, A QUIENES EN LO SUCESIVO SE LES DENOMINARÁ "LA SEMARNAT" Y POR LA OTRA, "SOLUCIONES INTEGRALES SAYNET, S.A. DE C.V.", REPRESENTADA EN ESTE ACTO POR LA C. ELIZABETH SALDAÑA ROBLES , EN SU CARÁCTER DE REPRESENTANTE LEGAL, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "EL PROVEEDOR", QUIENES ACTUANDO EN CONJUNTO SE LES DENOMINARÁ "LAS PARTES", DE CONFORMIDAD CON LAS SIGUIENTES:

D E C L A R A C I O N E S

1. Declara **"LA SEMARNAT"** bajo protesta de decir verdad:

   1.1. Que es una Dependencia del Poder Ejecutivo Federal de la Administración Pública Federal Centralizada en términos del Artículo 90 de la Constitución Política de los Estados Unidos Mexicanos y los artículos 2 y 26 de la Ley Orgánica de la Administración Pública Federal.

   1.2 Que de conformidad con lo establecido en el artículo 32 Bis de la citada Ley, le corresponde, entre otros asuntos: fomentar la protección, restauración y conservación de los ecosistemas y recursos naturales y bienes y servicios ambientales, con el fin de propiciar su aprovechamiento y desarrollo sustentable, así como formular y conducir la política nacional en materia de recursos naturales, siempre que no estén encomendados expresamente a otra dependencia, así como en materia de ecología, saneamiento ambiental, agua, regulación ambiental del desarrollo urbano y de la actividad pesquera, con la participación que corresponda a otras dependencias y entidades.

   1.3 El Ing. Eduardo Juan Guerrero Valdez, Director General de Recursos Materiales, Inmuebles y Servicios está facultado para suscribir el presente contrato, en atención a lo dispuesto en los artículos 19, fracción XXIII, y 36, fracción VI, del Reglamento Interior de la Secretaría de Medio Ambiente y Recursos Naturales, así como el numeral II.4.1 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de la Secretaría de Medio Ambiente y Recursos Naturales.

   1.4 El Ing. Ramon Alejandro Alcala Valera, Director de Adquisiciones y Contratos, firma el presente contrato en atención a lo dispuesto en el artículo 18, segundo párrafo del Reglamento Interior de la Secretaría de Medio Ambiente y Recursos Naturales, y en el numeral IV.16.1 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de la Secretaría de Medio Ambiente y Recursos Naturales, toda vez que de acuerdo a las funciones establecidas en el Manual de Organización Específico de la Dirección General de Recursos Materiales, Inmuebles y Servicios tiene a su cargo la elaboración y trámite para la formalización del presente contrato.

   1.5 Con fecha 12 de enero de 2017, a través de la Suficiencia Presupuestal registrada bajo el número de folio 00253 autorizada por el C.P. Eduardo Martínez Navarro, en su carácter de Director de Área de la Oficialía Mayor, se informa que dentro del Decreto de Presupuesto de Egresos de la Federación para el ejercicio fiscal 2017, específicamente en la partida presupuestal 31904 (SERVICIOS INTEGRALES DE INFRAESTRUCTURA DE CÓMPUTO), existe suficiencia presupuestal para cubrir la prestación económica que se genera con la suscripción de este contrato.

1.6 Que dentro de su estructura orgánica administrativa se encuentra la Dirección General de Informática y Telecomunicaciones, unidad administrativa que requiere de los servicios de **"EL PROVEEDOR"**, por lo que el Mtro. Mario Héctor Góngora Preciado, en su carácter de Director General de Informática y Telecomunicaciones, designa como Administrador del presente instrumento, al Lic. Gregorio Castilla Muñoz, en su carácter de Director de Infraestructura Tecnológica, o quien lo sustituya en el cargo, el cual será responsable de vigilar que se dé cumplimiento a las obligaciones que se deriven del presente contrato y hacerlas constar por escrito, informando a la Dirección General de Recursos Materiales, Inmuebles y Servicios del posible incumplimiento que se pudiera presentar.

1.7 Este contrato se celebra como resultado del procedimiento de Licitación Pública Número LA-016000997-ES1-2017 de carácter Nacional, mismo que se instrumentó de conformidad con los artículos 26 fracción I, 26 Bis fracción II y 28 fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, cuyo fallo fue emitido y dado a conocer el 30 de junio de 2017; aunado a que de conformidad con las Declaraciones del presente contrato y la documentación presentada y anexada al expediente correspondiente, las actividades desarrolladas por **"EL PROVEEDOR"** están plenamente relacionadas con los servicios objeto de este contrato y se garantiza que se reúnen las mejores condiciones disponibles para el Estado en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes.

1.8 Su Registro Federal de Contribuyentes es el número **SMA941228 GU8** y;

1.9 Señala como domicilio, para efectos de este contrato, el ubicado en Av. Ejército Nacional No. 223, Col. Anáhuac, Del. Miguel Hidalgo, C.P. 11320, Ciudad de México.

2. **"EL PROVEEDOR"** declara a través de su Representante Legal, bajo protesta de decir verdad, que:

2.1. Acredita la legal existencia de su representada con la Escritura Pública Número 18,204, de fecha 17 de agosto de 2004, otorgada ante la fe del Lic. Guillermo Eduardo Velázquez Quintana, Notario Público No. 21 del Estado de México, la cual es una persona moral legalmente constituida conforme a las leyes de la República Mexicana, debidamente inscrita en el Registro Público de la Propiedad y del Comercio, bajo el folio mercantil No. 322539 de fecha 20 de septiembre de 2004, bajo la denominación de "Soluciones Integrales SAYNET, S.A. de C.V.".

Mediante Escritura Pública Número 42,862, de fecha 27 de agosto de 2010, otorgada ante la fe pública del Lic. Luis Gerardo Mendoza Powell, Notario Público No. 106, del Estado de México, se autorizó el aumento de valor nominal de cada acción y aumento de capital de la persona moral "Soluciones Integrales SAYNET, S.A. de C.V.".

2.2. La C. Elizabeth Saldaña Robles, acredita su personalidad y facultades en su carácter de Representante Legal de Soluciones Integrales SAYNET, S.A. de C.V., mediante la Escritura Pública Número 58,016, de fecha 24 de agosto de 2016, otorgada ante la fe del Lic. Luis Gerardo Mendoza Powell, Notario Público No. 106 del Estado de México, mismas que no le han sido revocadas, limitadas o modificadas en forma alguna.

2.3. Cuenta con Cédula de Registro Federal de Contribuyentes **SIS040817 I1A**.

2.4. Es mexicana y conviene que, aún y cuando llegare a cambiar de nacionalidad, seguirse considerando como mexicana por cuanto a este contrato se refiere y no invocar la protección de ningún gobierno extranjero bajo pena de perder en beneficio de la nación mexicana, todo derecho derivado de este contrato.

2.5. La C. Elizabeth Saldaña Robles, en su carácter de Representante Legal, se identifica en este acto con Credencial de Votar con número de folio 0715022100189, expedido por el Instituto Federal Electoral en el año 2012 y vigente.

2.6. La persona moral que representa se encuentra inscrita en el Registro Federal de Contribuyentes con la clave de identificación fiscal **SIS040817 I1A** y tiene como objeto social entre otros: 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, bases de datos y todo lo relacionado a la Tecnología de Información.

2.7. Tiene capacidad jurídica para contratar y reúne las condiciones y recursos técnicos, humanos y económicos para obligarse a la ejecución de los servicios objeto de este contrato, y no existe impedimento alguno que le impida su celebración y cumplimiento.

2.8. Conoce plenamente el contenido y requisitos que establece la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento, así como las disposiciones legales y administrativas aplicables al presente contrato, en especial el alcance de los artículos 59 y 60 del mismo ordenamiento legal, relativos a la falsedad de información, así como las sanciones del orden civil, penal y administrativo que se imponen a quienes declaran con falsedad.

2.9. Bajo protesta de decir verdad, manifiesta no encontrarse en los supuestos de los artículos 50 y 60, tercer párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en caso de que alguna de las personas físicas que forman parte de **"EL PROVEEDOR"**, se encuentren en los supuestos señalados anteriormente, el contrato será nulo previa determinación de la autoridad competente.

2.10. Conoce el domicilio de **"LA SEMARNAT"**.

2.11. De manera previa a la formalización del presente contrato y en cumplimiento a lo dispuesto por el artículo 32-D, primero, segundo, tercero y cuarto párrafos del Código Fiscal de la Federación y de conformidad con la regla 2.1.31. de la Resolución Miscelánea Fiscal para el ejercicio 2017, publicada en el Diario Oficial de la Federación el 23 de diciembre de 2016 y que entró en vigor el día 1 de enero de 2017, presentó copia de respuesta, de fecha 10 de julio de 2017, con número de folio 17NB1026545, emitido por el Servicio de Administración Tributaria, sobre el cumplimiento de las obligaciones fiscales o en su caso, de las personas físicas o morales que para la prestación de los servicios subcontrataron.

De manera previa a la formalización del presente contrato y en cumplimiento a lo dispuesto por el artículo 32-D del Código Fiscal de la Federación y de conformidad con la regla Primera de las Reglas para la Obtención de la Opinión de Cumplimiento de Obligaciones Fiscales en Materia de Seguridad Social, publicada en el Diario Oficial de la Federación el 27 de febrero de 2015 y que entró en vigor el día 3 de marzo de 2015, presentó copia de respuesta, de fecha 10 de julio de 2017, con número de folio 14997366124351179472 69, emitido por el Instituto Mexicano del Seguro Social, sobre el cumplimiento de sus obligaciones fiscales en materia de seguridad social, o en su caso, de las personas físicas o morales que para la prestación.

2.12. Conoce plenamente las necesidades y características del servicio que requiere **"LA SEMARNAT"** y que ha considerado todos los factores que intervienen en su ejecución, por lo que manifiesta que dispone de elementos suficientes para contratar y obligarse en los términos de este contrato, y que para su cumplimiento y ejecución cuenta con la experiencia, los recursos técnicos, financieros, administrativos y humanos necesarios, para la entrega óptima del **SERVICIO.**

2.13. Que las actividades pactadas en el presente contrato son compatibles con su objeto social, por lo que no tiene impedimento alguno para obligarse en los términos del presente contrato y prestar sus servicios a **"LA SEMARNAT"** en los términos aquí estipulados y para poner su mayor capacidad, diligencia, calidad, esmero, eficiencia y oportunidad en el cumplimiento de sus obligaciones a favor de **"LA SEMARNAT"**, bajo su más estricta responsabilidad.

2.14. Reconoce y acepta que cuenta con los elementos propios a que se refiere el artículo 13 de la Ley Federal del Trabajo y en consecuencia es el único patrón de todas y cada una de las personas que intervengan en el desarrollo y ejecución del objeto de este contrato.

2.15. Señala como su domicilio para efectos del presente instrumento el ubicado en Calle Dramaturgos No. 47, Col. Ciudad Satélite, Del. Naucalpan de Juárez, C.P. 53100, Estado de México. Teléfono: 5871 6090. Correo Electrónico: esaldana@saynet.com.mx.

3. Declaran **"LAS PARTES"** que:

3.1. El presente contrato se celebra en términos de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y de forma supletoria en lo que corresponda, el Código Civil Federal, la Ley Federal de Procedimiento Administrativo y el Código Federal de Procedimientos Civiles, de conformidad con lo establecido por el artículo 11 de la Ley citada en primera instancia.

3.2. De conformidad con las anteriores declaraciones, las partes reconocen su personalidad jurídica y la capacidad legal que ostentan, asimismo conocen el alcance y contenido de este contrato y están de acuerdo en someterse a las siguientes:

C L Á U S U L A S

PRIMERA.- OBJETO

"EL PROVEEDOR" se obliga con **"LA SEMARNAT"** a realizar hasta su total terminación y prestar eficazmente los "Servicios administrados de seguridad perimetral". Para la ejecución del presente objeto **"EL PROVEEDOR"** tendrá que cumplir con las especificaciones estipuladas en el "Anexo Único", que forma parte integrante del presente instrumento, constante de 346 fojas útiles conforme a lo siguiente: declaraciones y clausulado (20 fojas útiles), Especificaciones Técnicas de **"LA SEMARNAT"** (54 fojas útiles), Acta de la Junta de Aclaraciones (62 fojas útiles), Propuesta Técnica (155 fojas útiles), Propuesta de Trabajo (52 fojas útiles) y Propuesta Económica (3 fojas útiles) de **"EL PROVEEDOR"**.

Las obligaciones que se convienen en el objeto de este contrato no son divisibles toda vez que por las características de los servicios materia del mismo, no pueden ser utilizados de manera incompleta, por lo que la garantía se hará efectiva por el monto total de la obligación garantizada.

SEGUNDA.- VIGENCIA DEL CONTRATO

Las partes convienen en que la vigencia del presente contrato iniciará el 01 de julio y concluirá el 31 de diciembre de 2017.

TERCERA.- MONTO DEL CONTRATO

El importe total a pagar por los servicios es de **$5,557,365.02 (CINCO MILLONES QUINIENTOS CINCUENTA Y SIETE MIL TRESCIENTOS SESENTA Y CINCO PESOS 02/100 M.N.)**, más la cantidad de **$889,178.40 (OCHOCIENTOS OCHENTA Y NUEVE MIL CIENTO SETENTA Y OCHO PESOS 40/100 M.N.)** correspondiente al 16% del Impuesto al Valor Agregado; por lo que el monto total de este contrato asciende a la cantidad de **$6,446,543.42 (SEIS MILLONES CUATROCIENTOS CUARENTA Y SEIS MIL QUINIENTOS CUARENTA Y TRES PESOS 42/100 M.N.)**.

El precio unitario de los servicios mismo que se considerará fijo y no estará sujeto a ajustes, de conformidad con lo siguiente:

No.	DESCRIPCIÓN DEL SERVICIO	COSTO MENSUAL SIN IVA	COSTO TOTAL POR 6 MESES DE SERVICIO SIN IVA
1	Servicio de seguridad perimetral para oficina central de la SEMARNAT	$290,224.01	$1,741,344.07
2	Servicio de seguridad perimetral para el centro de datos	$290,224.01	$1,741,344.07
3	Sistema de contención de ataques de disponibilidad en el perímetro de internet (mitigación en sitio)	$157,681.89	$946,091.37
4	Mesa de servicio	$188,097.58	$1,128,585.51
		SUB TOTAL	**$5,557,365.02**
		IVA	**$889,178.40**
		TOTAL	**$6,446,543.42**

El monto antes señalado incluye todos los gastos que se originen como consecuencia de su realización, tales como materiales, sueldos, honorarios, organización, dirección técnica propia, administración, prestaciones sociales y laborales a su personal, entre otros.

CUARTA.- PLAZO Y LUGAR DE PRESTACIÓN DEL SERVICIO

"EL PROVEEDOR" se obliga se obliga a prestar los servicios amparados en el presente contrato, a partir de 01 de julio y hasta 31 de diciembre de 2017.

La ejecución y el lugar de prestación de los servicios por parte de **"EL PROVEEDOR"** se realizarán conforme a las condiciones descritas en el "Anexo Único".

QUINTA.- FACTURACIÓN, PLAZO Y CONDICIONES DE PAGO

"LA SEMARNAT" efectuará el pago en pesos de los Estados Unidos Mexicanos, sobre el servicio devengado, siempre y cuando **"EL PROVEEDOR"** preste el mismo a entera satisfacción de **"LA SEMARNAT"** de acuerdo con lo establecido en el "Anexo Único" que forma parte integrante de este contrato.

Para que la obligación de pago se haga exigible, **"EL PROVEEDOR"** deberá sin excepción alguna presentar factura remitiéndola vía correo electrónico al Administrador del Contrato al correo electrónico Gregorio.castilla@semarnat.gob.mx, o al que en su caso se le notifique, así como toda la documentación que ampare la prestación de los servicios a entera satisfacción de **"LA SEMARNAT"**, de conformidad con los requerimientos, características y plazos contenidos en este contrato y en el "Anexo Único" que se acompaña al presente; el citado pago se realizará a través de medios de comunicación electrónica a la cuenta bancaria que al efecto haya acreditado **"EL PROVEEDOR"**, la cual deberá ser registrada en el Sistema Integral de Administración Financiera Federal, o bien según los procedimientos establecidos por **"LA SEMARNAT"**, a través de la Dirección General de Programación y Presupuesto, con la aprobación de Dirección General de Informática y Telecomunicaciones, dentro de los 20 días naturales posteriores a la presentación del recibo de honorarios o factura referida en líneas precedentes, área que deberá validar la documentación y dar su Visto Bueno.

El pago se realizará dentro del plazo señalado en el párrafo que antecede, considerando que no existan aclaraciones al importe o especificaciones a los trabajos facturados y que los documentos de cobro hayan sido presentados en tiempo, de lo contrario, el plazo para el pago se recorrerá en forma proporcional.

La factura deberá contener todos los datos y registros requeridos por las disposiciones fiscales vigentes; asimismo, el importe deberá presentar desglosado el concepto del Impuesto al Valor Agregado, y en su caso, de los impuestos aplicables.

Los impuestos que se deriven del contrato serán cubiertos por cada una de las partes de acuerdo a las disposiciones legales vigentes y aplicables en la materia.

En caso de que las facturas entregadas por **"EL PROVEEDOR"** para su pago presenten errores o deficiencias **"LA SEMARNAT"** dentro de los tres días hábiles siguientes a su recepción, indicará por escrito a **"EL PROVEEDOR"** las deficiencias que deberá corregir. El periodo que transcurra a partir de la entrega del citado escrito y hasta que **"EL PROVEEDOR"** presente las correcciones, no se computará para efectos del artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. Una vez corregida la factura correspondiente, reiniciará el cómputo del plazo antes mencionado.

Los pagos se harán a través de medios de comunicación electrónica. Para el caso de que se presenten pagos en exceso o se determine la rescisión del contrato se estará a lo dispuesto por los párrafos tercero y cuarto del artículo 51 la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

SEXTA.- TRANSFERENCIA DE DERECHOS

"EL PROVEEDOR" se obliga a no ceder en forma parcial o total, en favor de cualquier otra persona física o moral, sus derechos y obligaciones derivados de este contrato y su "Anexo Único", con excepción de los derechos de cobro por los servicios ejecutados, en cuyo supuesto se deberá contar con la previa autorización por escrito de **"LA SEMARNAT"** en los términos del último párrafo del artículo 46 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

"EL PROVEEDOR" podrá solicitar la realización de la cesión de los derechos de cobro a favor de un intermediario financiero de su elección, en virtud del acuerdo que **"LA SEMARNAT"** tiene concertado con Nacional Financiera, S.N.C. denominado "Programa de Cadenas Productivas", a efecto de apoyar a los proveedores, contratistas o prestadores de servicios de **"LA SEMARNAT"**, a través de operaciones de factoraje y descuento electrónico de hasta el 100% del importe de los títulos de crédito y/o documentos en que se consignen derechos de crédito expedidos por **"LA SEMARNAT"**, incluyendo los intereses correspondientes, por lo que será la misma Nacional Financiera, el canal para la recepción de los poderes, actas constitutivas y carta de adhesión que firmen los proveedores y contratistas. Todo lo anterior de conformidad con lo establecido en las "Disposiciones Generales a las que deberán sujetarse las Dependencias y Entidades de la Administración Pública Federal para su incorporación al Programa de Cadenas Productivas de Nacional Financiera, S. N. C., Institución de Banca de Desarrollo, sin menoscabo de lo establecido en el último párrafo del artículo 46 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Para tales efectos, **"EL PROVEEDOR"** deberá entregar a **"LA SEMARNAT"** copia certificada expedida por Notario Público del convenio que haya celebrado con Nacional Financiera, S. N. C., Institución de Banca de Desarrollo, en el que conste su incorporación al Programa de Cadenas Productivas, sin cuyo requisito no procederá la cesión de derechos de cobro solicitada por **"EL PROVEEDOR"** por este medio.

Independientemente de lo anterior, **"EL PROVEEDOR"** deberá presentar a **"LA SEMARNAT"** escrito en el que manifieste que los contra recibos por pagar, materia de la cesión de derechos de cobro, no han sido negociados o comprometidos previamente.

Si con motivo de la realización de la operación de la cesión de derechos de cobro solicitada por **"EL PROVEEDOR"** se origina un atraso en el pago, no procederá el pago de gastos financieros a cargo de **"LA SEMARNAT"** a que se refiere el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. En este caso, los gastos financieros serán cubiertos por el intermediario financiero que haya seleccionado **"EL PROVEEDOR"**.

SÉPTIMA.- PRECIOS FIJOS

"EL PROVEEDOR" se obliga a mantener fijos los precios unitarios de sus servicios establecidos en el "Anexo Único", no pudiendo incrementarlo, no obstante, las variaciones económicas en salarios mínimos, insumos, pasajes, cuotas, devaluación de la moneda, actos inflacionarios, entre otros, que se presenten en el país durante la vigencia del contrato, en cuyo caso, dicho sobreprecio será absorbido por él, sin que ello repercuta de manera cuantitativa o cualitativa en la prestación del servicio.

OCTAVA.- ANTICIPO

En el presente contrato **"LA SEMARNAT"** no otorgará anticipo a **"EL PROVEEDOR"**.

NOVENA.- VERIFICACIÓN Y ACEPTACIÓN DE LOS SERVICIOS

Al término de la vigencia del presente contrato, el servidor público responsable de verificar su cumplimiento, deberá entregar a **"EL PROVEEDOR"** la constancia de cumplimiento de las obligaciones contractuales, por escrito, en la que conste o certifique que el servicio ha sido realizado conforme a lo establecido en el presente acuerdo de voluntades y a entera satisfacción de **"LA SEMARNAT"**. Asimismo, **"EL PROVEEDOR"** manifiesta su conformidad de que hasta en tanto no sea otorgada dicha constancia, el servicio prestado se tendrán por no recibido, de conformidad con lo dispuesto por el artículo 84, último párrafo, del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

De conformidad con los artículos 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 107 de su Reglamento **"EL PROVEEDOR"** se obliga a proporcionar a la Secretaría de la Función Pública y al Órgano Interno de Control de **"LA SEMARNAT"** toda la información y documentación que en su momento se requiera con motivo de las auditorias, visitas o inspecciones que practiquen y que se relacionen con el presente contrato, aún concluida la vigencia del contrato y por el tiempo que de acuerdo a la regulación fiscal le corresponda conservarla.

DÉCIMA.- SUPERVISIÓN DE LOS SERVICIOS

"LA SEMARNAT" a través del Lic. Gregorio Castilla Muñoz, en su carácter de Director de Infraestructura Tecnológica, o quien lo sustituya en el cargo, quien fue designado como Administrador del Contrato, supervisará y vigilará en todo tiempo el servicio objeto de este contrato, el cual deberá realizarse en los plazos establecidos en el "Anexo Único".

"EL PROVEEDOR" acepta que el Administrador del Contrato de **"LA SEMARNAT"** vigilará, supervisará y revisará en todo tiempo el servicio objeto de este contrato y dará a **"EL PROVEEDOR"** por escrito, las instrucciones que estime pertinentes relacionadas con su ejecución en la forma convenida, a fin de que se ajuste a las especificaciones contenidas en el "Anexo Único" a que se alude en la cláusula denominada Objeto del presente instrumento jurídico, así como a las modificaciones que, en su caso, ordene por escrito **"LA SEMARNAT"** y sean aprobados por ésta.

La supervisión del servicio que realice **"LA SEMARNAT"** no libera a **"EL PROVEEDOR"** del cumplimiento de sus obligaciones contraídas en este contrato así, como de responder por deficiencias en la calidad del servicio una vez concluido éste. Lo anterior, en el entendido de que el ejercicio de esta facultad, no será considerada como aceptación tácita o expresa del servicio, ni libera a **"EL PROVEEDOR"** de las obligaciones que contrae bajo este contrato.

De conformidad con el artículo 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, la Secretaría de la Función Pública, podrá realizar las visitas e inspecciones que estime necesarias, así como verificar la calidad del servicio establecida en el presente contrato, pudiendo solicitar a **"LA SEMARNAT"** y a **"EL PROVEEDOR"** todos los datos e informes relacionados con los actos de que se trate.

En el caso de atraso en el cumplimiento de las fechas o plazos pactados para la prestación de los servicios, el Administrador del Contrato, procederá a notificar a **"EL PROVEEDOR"** o a su representante legal la pena respectiva, preferentemente dentro de los 30 (treinta) días hábiles siguientes a la fecha en que se hayan generado las penas convencionales, notificando, igualmente a la Dirección General de Programación y Presupuesto, para que ésta reciba de parte de **"EL PROVEEDOR"**, el comprobante que acredite el pago de la pena convencional formato "Pago Electrónico de Derechos, Productos y Aprovechamientos, Esquema e5cinco", o el que determine en su caso el Sistema de Administración Tributaria (SAT)].

Las penas convencionales serán determinadas por el Administrador del Contrato, en función de los servicios no prestados oportunamente. En las operaciones en que se pacte ajuste de precios, la penalización se calculará sobre el precio ajustado.

DÉCIMA PRIMERA.- MODIFICACIONES

"LA SEMARNAT" podrá acordar con **"EL PROVEEDOR"** por razones fundadas y explícitas respecto del contrato vigente, el incremento en el monto o en la cantidad de los servicios del mismo, siempre que el monto total de las modificaciones no rebase, en conjunto, el 20% de los conceptos y volúmenes establecidos, el precio de los servicios sea igual al originalmente pactado, el contrato esté vigente y **"EL PROVEEDOR"** no se encuentre en incumplimiento.

Asimismo, en el caso de que **"LA SEMARNAT"** lo considere conveniente, podrá ampliar la vigencia del contrato.

En el caso de que el presente contrato incluya dos o más partidas, el porcentaje se aplicará para cada una de ellas.

Cualquier solicitud de modificación que se presente por parte de **"EL PROVEEDOR"** a las condiciones originalmente pactadas deberá tramitarse por escrito exclusivamente ante la Dirección General de Recursos Materiales, Inmuebles y Servicios de **"LA SEMARNAT"**, en el entendido de que cualquier cambio o modificación que no sea autorizada expresamente por el área citada, se considerará inexistente para todos los efectos administrativos y legales del presente contrato.

La solicitud de modificación por parte de **"EL PROVEEDOR"**, no interrumpirá el plazo para la conclusión de los servicios originalmente pactados.

En términos de lo establecido en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, no procederá ningún cambio que implique otorgar condiciones más ventajosas comparadas con las establecidas originalmente, podrá modificarse, igualmente por escrito, por detalles de forma que no desvirtúen el contenido esencial del presente instrumento jurídico y del procedimiento de adjudicación del cual se deriva.

En el caso de cualquier modificación a lo pactado en el contrato y/o sus anexos, **"EL PROVEEDOR"** se obliga a entregar a **"LA SEMARNAT"** dentro de los 10 (diez) días naturales siguientes a la fecha de la formalización del convenio modificatorio respectivo, el endoso o documento modificatorio de la fianza otorgada originalmente por la institución afianzadora correspondiente, conforme al artículo 91 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el cual deberá contener la estipulación de que es conjunto, solidario e inseparable de la fianza inicialmente presentada por **"EL PROVEEDOR"**.

En el caso de que **"EL PROVEEDOR"** no cumpla con dicha entrega, **"LA SEMARNAT"** podrá determinar la rescisión administrativa del contrato.

DÉCIMA SEGUNDA.- PAGOS EN EXCESO

En caso de que existan pagos en exceso que haya recibido **"EL PROVEEDOR"**, éste deberá reintegrar las cantidades pagadas en exceso, más los intereses correspondientes conforme a la tasa que establezca la Ley de Ingresos de la Federación en los casos de prórroga para el pago de créditos fiscales. Los intereses se calcularán sobre las cantidades pagadas en exceso en cada caso y se computarán por días naturales desde la fecha del pago hasta la fecha en que se pongan efectivamente las cantidades a disposición de **"LA SEMARNAT"**. **"LA SEMARNAT"** procederá a deducir dichas cantidades de las facturas subsecuentes o bien **"El PROVEEDOR"** cubrirá dicho pago con cheque certificado a favor de **"LA SEMARNAT"**.

DÉCIMA TERCERA.- OBLIGACIONES FISCALES

Las partes pagarán todas y cada una de las contribuciones y demás cargas fiscales que conforme a las leyes federales, estatales y municipales de los Estados Unidos Mexicanos tengan la obligación de cubrir durante la vigencia, ejecución y cumplimiento del presente contrato y sus anexos, sin perjuicio de que **"LA SEMARNAT"** realice, de los pagos que haga a **"EL PROVEEDOR"**, las retenciones que le impongan las leyes de la materia.

DÉCIMA CUARTA.- GARANTÍA DE CUMPLIMIENTO DEL CONTRATO

Con fundamento en los artículos 48 fracción II y 49 fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y el artículo 103 de su Reglamento **"EL PROVEEDOR"** a fin de garantizar el debido cumplimiento

de las obligaciones derivadas del contrato, así como para responder de los defectos, vicios ocultos de los bienes o servicios y cualquier otra responsabilidad en los términos señalados en el contrato, deberá presentar a **"LA SEMARNAT"**, dentro de los 10 (diez) días naturales a partir de la fecha de suscripción del contrato, la garantía de cumplimiento, en caso que el último día sea inhábil se deberá presentar a más tardar el último día hábil, de conformidad con:

Póliza de fianza que se constituirá por el 10% del importe total del contrato, estipulado en la Cláusula denominada Monto del Contrato de este instrumento, sin incluir el Impuesto al Valor Agregado, con una vigencia equivalente a la del contrato garantizado, otorgada por institución afianzadora legalmente constituida en la República Mexicana, en términos de la Ley de Instituciones de Seguros y de Fianzas y a favor de **"LA TESORERÍA DE LA FEDERACIÓN"**.

"EL PROVEEDOR" manifiesta expresamente:

(A) Su voluntad en caso de que existan créditos a su favor contra **"LA SEMARNAT"**, de renunciar al derecho a compensar que le concede la legislación sustantiva civil aplicable, por lo que otorga su consentimiento expreso para que en el supuesto de incumplimiento de las obligaciones que deriven del contrato, se haga efectiva la garantía otorgada, así como cualquier otro saldo a favor de **"LA SEMARNAT"**.

(B) Su conformidad para que la fianza que garantiza el cumplimiento del contrato, permanezca vigente durante la substanciación de todos los procedimientos judiciales o arbitrales y los recursos legales que se interpongan, con relación al contrato, hasta que sea dictada resolución definitiva que cause ejecutoria por parte de la autoridad o tribunal competente.

(C) Su aceptación para que la fianza de cumplimiento permanezca vigente hasta que las obligaciones garantizadas hayan sido cumplidas en su totalidad, en la inteligencia que la conformidad para la liberación deberá ser otorgada mediante escrito suscrito por **"LA SEMARNAT"**.

(D) Su conformidad en que la reclamación que se presente ante la afianzadora por incumplimiento de contrato, quedará integrada con la siguiente documentación:

1. Reclamación por escrito a la Institución de Fianzas.
2. Copia de la póliza de fianza y en su caso, sus documentos modificatorios.
3. Copia del contrato garantizado y en su caso sus convenios modificatorios.
4. Copia del documento de notificación al fiado de su incumplimiento.
5. En su caso, la rescisión del contrato y su notificación,
6. En su caso, documento de terminación anticipada y su notificación
7. Copia del finiquito y en su caso, su notificación.
8. Importe reclamado.

La fianza deberá contener como mínimo las siguientes declaraciones expresas:

I. Que se otorga atendiendo todas y cada una de las estipulaciones establecidas en este contrato.

II. Que para cancelar la fianza, será requisito contar con la constancia de cumplimiento total de las obligaciones contractuales de conformidad con lo establecido en la Cláusula denominada Precios Fijos del presente instrumento;

III. Que la fianza permanecerá vigente durante el cumplimiento de la obligación que garantice y continuará vigente en caso de que se otorgue prórroga al cumplimiento del contrato, así como durante la substanciación

de todos los recursos legales o de los juicios que se interpongan y hasta que se dicte resolución definitiva que quede firme, y

IV. Que la afianzadora acepta expresamente someterse a los procedimientos de ejecución previstos en la Ley de Instituciones de Seguros y de Fianzas para la efectividad de las fianzas, aún para el caso de que proceda el cobro de indemnización por mora, con motivo del pago extemporáneo del importe de la póliza de fianza requerida. El procedimiento de ejecución será el previsto en el artículo 282 de la citada Ley, debiéndose atender para el cobro de indemnización por mora lo dispuesto en el artículo 283 de dicha Ley;

En el supuesto de que las partes convengan la modificación del contrato vigente, en términos de la Cláusula denominada Modificaciones del presente Contrato, **"EL PROVEEDOR"** deberá contratar la ampliación de la fianza, presentando la modificación y/o endoso de la garantía dentro de los (10) diez días hábiles siguientes a la firma del convenio que modifique el instrumento original, por el importe del incremento o modificación correspondiente.

La garantía de cumplimiento deberá ser presentada en la Subdirección de Comité y Contratos, ubicada en Av. Ejército Nacional No. 223, Piso 17 Ala B, Col. Anáhuac, Del. Miguel Hidalgo, C.P. 11320, Ciudad de México.

DÉCIMA QUINTA.- PÓLIZA DE RESPONSABILIDAD CIVIL

"EL PROVEEDOR" será el único responsable por la mala ejecución de los servicios así como del incumplimiento a las obligaciones previstas en este instrumento cuando no se ajuste al mismo, al igual de los daños y perjuicios que ocasione con motivo de la no prestación de los servicios por causas imputables al mismo, una deficiente realización de los mismos o por no realizarlos de acuerdo con las especificaciones contenidas en el presente contrato, así como aquellos que resultaren como causa directa de la falta de pericia, dolo, descuido y cualquier acto u omisión negligente en su ejecución, salvo que el acto por el que se haya originado hubiese sido expresamente y por escrito ordenado por **"LA SEMARNAT"**.

"EL PROVEEDOR" deberá presentar una póliza de responsabilidad civil debidamente pagada, en original y copia para el expediente, por un importe equivalente al 10% del monto máximo de este contrato, incluido el I.V.A., a más tardar el día de inicio de la vigencia. Este documento deberá ser entregado en la Dirección General de Informática y Telecomunicaciones, sita en Av. Ejército Nacional No. 223, Piso 17 Ala A, Col Anáhuac, Del. Miguel Hidalgo, C.P. 11320, Ciudad de México.

DÉCIMA SEXTA.- DAÑOS Y PERJUICIOS

"EL PROVEEDOR" será el único responsable por la mala ejecución de los servicios así como del incumplimiento a las obligaciones previstas en este instrumento cuando no se ajuste al mismo, al igual de los daños y perjuicios que ocasione con motivo de la no prestación de los servicios por causas imputables al mismo, una deficiente realización de los mismos o por no realizarlos de acuerdo con las especificaciones contenidas en el presente contrato, así como aquellos que resultaren como causa directa de la falta de pericia, dolo, descuido y cualquier acto u omisión negligente en su ejecución, salvo que el acto por el que se haya originado hubiese sido expresamente y por escrito ordenado por **"LA SEMARNAT"**.

DÉCIMA SÉPTIMA.- PENAS CONVENCIONALES

Las penas convencionales a las que **"EL PROVEEDOR"** se haga acreedor por incumplimiento en la ejecución de los servicios, se calcularán, de acuerdo a lo establecido en el "Anexo Único" y el presente contrato, de conformidad con lo siguiente:

NUMERAL DEL ANEXO	OBLIGACIÓN	CÁLCULO PARA LA APLICACIÓN DE PENA CONVENCIONAL
17 Punto 2	Entrega del equipamiento para seguridad perimetral	1% del monto total del servicio mensual por cada día natural de atraso en la instalación de los equipos.

17 Punto 2	Instalación y configuración de equipamiento para seguridad perimetral	1% del monto total del servicio mensual por cada día natural de atraso en la instalación de los equipos.
10 Punto 10	Atraso en la entrega de la memoria técnica (especificado en los entregables) si se excede al plazo mayor de 15 días hábiles.	1% del monto total de la factura por cada día natural de atraso en la instalación de los equipos.
15	El proveedor no haga entrega de cada uno de los entregables en el plazo establecido	1% del monto total de la factura por cada día natural de atraso en los entregables.

Las penas convencionales serán cubiertas por **"EL PROVEEDOR"** mediante el "Pago electrónico de Derechos, Producto y Aprovechamientos, esquema eScinco" ante alguna de las instituciones bancarias autorizadas, acreditando dicho pago con la entrega del recibo bancario a la Dirección de Infraestructura Tecnológica.

La suma de todas las penas convencionales aplicadas a **"EL PROVEEDOR"** no deberá exceder el importe de la garantía de cumplimiento del contrato.

Cuando los servicios no se presten en la fecha o plazo convenido y la pena convencional por atraso rebase el monto de la garantía de cumplimiento del contrato, **"LA SEMARNAT"**, a través del Administrador del Contrato, previa notificación a **"EL PROVEEDOR"**, podrá rescindir este contrato, en términos de la Cláusula denominada Rescisión Administrativa.

En caso que sea necesario llevar a cabo la rescisión administrativa del contrato, la aplicación de la garantía de cumplimiento será proporcional al monto de las obligaciones incumplidas.

Independientemente de la aplicación de la pena convencional a que hace referencia el párrafo que antecede, se aplicarán además las sanciones que deriven de la Ley o la normatividad.

La penalización tendrá como objeto resarcir los daños y perjuicios ocasionados a **"LA SEMARNAT"** con el atraso en la prestación de servicios señalados en el contrato. Las penas son independientes de los daños y perjuicios que ocasionare **"EL PROVEEDOR"** por no cumplir con las condiciones pactadas en el presente contrato.

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

DÉCIMA OCTAVA.- DEDUCCIONES

"LA SEMARNAT" podrá realizar deducciones al pago de los servicios con motivo del incumplimiento parcial o deficiente en que pudiera incurrir **"EL PROVEEDOR"** respecto de los casos concretos especificados en el "Anexo Único" y el presente contrato, conforme a lo siguiente:

Numeral del Anexo	Obligación	CÁLCULO PARA LA APLICACIÓN DE LA DEDUCCIÓN		TIPO DE FALTA POR EVENTO	LÍMITE DE EVENTOS PERMITIDOS
		% deducción a aplicarse	Aplicación		
15	Si los entregables mensuales de MAAGTICSI no son entregados en su totalidad u no cumplan con lo requerido en el servicio	1% (Uno por ciento)	Calculado sobre el importe de los servicios prestados en forma parcial o	Baja	Hasta 3 ocasiones en la falta de entrega durante el mismo mes calendario para esta deductiva.

Numeral del Anexo	Obligación	CÁLCULO PARA LA APLICACIÓN DE LA DEDUCCIÓN		TIPO DE FALTA POR EVENTO	LÍMITE DE EVENTOS PERMITIDOS
		% deducción a aplicarse	Aplicación		
11.3	Incidentes con afectación de severidad 1	1% (Uno por ciento)	deficientemente.	Baja	Hasta 3 ocasiones en la falta de entrega durante la vigencia del servicio.
11.3	Incidentes con afectación de severidad 2	1% (Uno por ciento)		Media	Hasta 2 ocasiones en la falta de entrega durante la vigencia del servicio.
11.3	Incidentes con afectación de severidad 3	1% (Uno por ciento)		Alta	Hasta 1 ocasión en la falta de entrega durante la vigencia del servicio.
11.3	Incidentes con afectación de severidad 4	1% (Uno por ciento)		Muy Alta	Hasta 1 ocasión en la falta de entrega durante la vigencia del servicio.
16.5	Falla en la disponibilidad de la operación de la mesa por parte del licitante	1%(Uno por ciento)		Grave	Hasta 2 ocasiones en la falta de entrega durante el mismo mes calendario para esta deductiva.

Dichas deducciones deberán ser calculadas por el Administrador del Contrato desde que se presente el incumplimiento parcial o deficiente hasta la fecha en que materialmente se cumpla la obligación.

Los montos a deducir se deberán aplicar en la factura que **"EL PROVEEDOR"** presente para su cobro, inmediatamente después de que el Administrador del Contrato tenga cuantificada la deducción correspondiente y le notifique a **"EL PROVEEDOR"** que incluya el monto de la deducción en su próxima factura, o en su caso, presente la nota de crédito correspondiente acompañada de su factura.

DÉCIMA NOVENA.- RESCISIÓN ADMINISTRATIVA

Ambas partes convienen y **"EL PROVEEDOR"** está de acuerdo en que **"LA SEMARNAT"** podrá en cualquier momento, por causas imputables a **"EL PROVEEDOR"**, rescindir administrativamente el presente contrato, cuando éste último incumpla con cualquiera de las obligaciones estipuladas en el mismo. Dicha rescisión operará de pleno derecho, sin necesidad de declaración o resolución judicial, bastando que se cumpla con el procedimiento señalado en el artículo 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y en la Cláusula denominada Procedimiento de Rescisión Administrativa del Contrato.

Las causas que pueden dar lugar a que **"LA SEMARNAT"** inicie el procedimiento de rescisión administrativa del contrato, son las siguientes:

A. Si **"EL PROVEEDOR"** no entrega la garantía de cumplimiento conforme al plazo estipulado en la normatividad vigente y la cláusula denominada Garantía de cumplimiento.

B. Si **"EL PROVEEDOR"** no entrega la póliza de responsabilidad civil conforme al plazo estipulado en el presente contrato.

C. Cuando el importe de las penas convencionales alcance el monto de la garantía de cumplimiento.

D. Si **"EL PROVEEDOR"** es declarado, por autoridad competente, en concurso mercantil o de acreedores o en cualquier situación análoga que afecte su patrimonio.

E. Si **"EL PROVEEDOR"** cede, vende, traspasa o subcontrata en forma total o parcial los derechos y obligaciones derivados del contrato; o transfiere los derechos de cobro derivados del contrato, sin contar con el consentimiento de **"LA SEMARNAT"**.

F. Si **"EL PROVEEDOR"** no da a **"LA SEMARNAT"** o a quien éste designe por escrito, las facilidades o datos necesarios para la supervisión o inspección de los servicios.

G. Si **"EL PROVEEDOR"** incurriera en falta de veracidad, total o parcialmente respecto a la información proporcionada para la celebración de este contrato.

H. Por no observar discreción debida respecto de la información a la que tenga acceso como consecuencia de la prestación de los servicios contratados.

I. Si **"EL PROVEEDOR"** no cumple con los requerimientos establecidos con forme al Anexo Técnico.

J. Si **"EL PROVEEDOR"** tiene fallas continuas durante la operación del servicio y ponga en riesgo la infraestructura y seguridad de la Institución.

K. Que el personal asignado por "EL PROVEEDOR" sea sorprendido haciendo mal uso de la información o transfiera a terceros para bienes de uso propio y que afecten a la Institución.

L. Si **"EL PROVEEDOR"** tiene un tipo de falla por evento denominada muy alta por dos ocasiones durante la vigencia del contrato.

En caso de incumplimiento de **"EL PROVEEDOR"** a cualquiera de las obligaciones del contrato, **"LA SEMARNAT"** podrá optar entre exigir el cumplimiento del mismo y el pago de las penas convencionales por el atraso, o declarar la rescisión administrativa conforme al procedimiento que se señala en la Cláusula denominada Procedimiento de Rescisión Administrativa del Contrato y hacer efectiva la garantía de cumplimiento, en forma proporcional al incumplimiento, sin menoscabo de que **"LA SEMARNAT"** pueda ejercer las acciones judiciales que procedan.

En este caso, la aplicación de la garantía de cumplimiento será proporcional al monto de las obligaciones incumplidas, salvo que, por las características de los servicios, éstos no puedan ser utilizados por **"LA SEMARNAT"** por estar incompletos, en cuyo caso, la aplicación de la garantía correspondiente será total.

En el supuesto de que sea rescindido el contrato, no procederá el cobro de las penas por atraso ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento si la hubiere.

Si **"EL PROVEEDOR"** es quien decide rescindirlo, será necesario que acuda ante la autoridad judicial y obtenga la declaración o resolución correspondiente.

VIGÉSIMA.- PROCEDIMIENTO DE RESCISIÓN ADMINISTRATIVA DEL CONTRATO

Ambas partes convienen que para los efectos de que sea **"LA SEMARNAT"** quien determine rescindir el contrato, iniciará el procedimiento con la comunicación por escrito a **"EL PROVEEDOR"** del hecho u omisión que constituya el incumplimiento de cualquiera de sus obligaciones, con el objeto de que éste dentro de un plazo máximo de 5 (cinco) días hábiles manifieste por escrito lo que a su derecho convenga, y aporte en su caso, las pruebas que estime pertinentes; transcurrido dicho plazo **"LA SEMARNAT"** resolverá considerando los argumentos y pruebas que hubiere hecho valer **"EL PROVEEDOR"**, por lo que **"LA SEMARNAT"** en el lapso de los 15 (quince) días hábiles siguientes deberá fundar y motivar su determinación y comunicarlo por escrito a **"EL PROVEEDOR"**. Cuando se rescinda el contrato **"LA SEMARNAT"** elaborará y notificará el finiquito correspondiente, además declarará de pleno derecho y en forma administrativa la rescisión del mismo, sin necesidad de declaración judicial alguna.

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

Como consecuencia de la rescisión por parte de **"LA SEMARNAT"**, ésta quedará obligada a cubrir el costo del servicio, sólo hasta la proporción que éste haya sido devengado en forma satisfactoria para la misma, por lo tanto, **"LA SEMARNAT"** queda en libertad de contratar los servicios de otro proveedor y los costos que esto origine serán descontados del pago señalado en primer término, obligándose **"EL PROVEEDOR"** a reintegrar los pagos progresivos que haya recibido, más los intereses correspondientes, conforme a lo establecido en el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. Lo anterior, en forma independiente a las sanciones que establezcan las disposiciones legales aplicables en la materia y a las contenidas en el presente contrato.

Se podrá negar la recepción de los servicios una vez iniciado el procedimiento de rescisión administrativa del contrato, cuando **"LA SEMARNAT"** ya no tenga la necesidad de los servicios, por lo que en este supuesto **"LA SEMARNAT"** determinará la rescisión administrativa del contrato y hará efectiva la garantía de cumplimiento.

Si iniciada la rescisión **"LA SEMARNAT"** dictamina que seguir con el procedimiento puede ocasionar algún daño o afectación a las funciones que tiene encomendadas, podrá determinar no dar por rescindido el presente contrato, en cuyo caso, le establecerá otro plazo a **"EL PROVEEDOR"** para que subsane el incumplimiento que hubiere motivado el inicio del procedimiento. Dicho plazo deberá hacerse constar en un convenio modificatorio en términos de los dos últimos párrafos del artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, quedando facultada **"LA SEMARNAT"** para hacer efectivas las penas convencionales que correspondan.

De actualizarse el último párrafo del artículo 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"LA SEMARNAT"** podrá recibir los servicios, previa verificación de que continúa vigente la necesidad de los mismos y se cuenta con partida y disponibilidad presupuestaria del ejercicio fiscal vigente, en cuyo caso, mediante Convenio se modificará la vigencia del presente contrato con los precios originalmente pactados. Cualquier pacto en contrario se considerará nulo.

VIGÉSIMA PRIMERA.- CASO FORTUITO O FUERZA MAYOR Y SUSPENSIÓN DE LOS SERVICIOS

Ninguna de las partes será responsable ante la otra por causa que derive de caso fortuito o fuerza mayor.

Si durante la vigencia del contrato se presenta caso fortuito o fuerza mayor, **"LA SEMARNAT"** podrá suspender la prestación del servicio hasta por un plazo de 30 (treinta) días naturales, lo que bastará sea comunicado por escrito de una de las partes a la otra con 5 (cinco) días naturales contados a partir de que se presente el evento que la motivó, a través de un oficio con acuse de recibo, procediendo **"LA SEMARNAT"** al pago de los servicios efectivamente prestados; si concluido el plazo persistieran las causas que dieron origen a la suspensión, **"LA SEMARNAT"** podrá dar por terminada anticipadamente la relación contractual que se formaliza.

Cualquier causa de fuerza mayor o caso fortuito, no obstante que sea del dominio público deberá acreditarse documentalmente por la parte que la padezca y notificar a la otra parte dentro del plazo mencionado en el párrafo que antecede a través de un oficio con acuse de recibo. Cuando se le notifique a **"LA SEMARNAT"**, deberá ser ante la Dirección General de Recursos Materiales Inmuebles y Servicios, con copia al Administrador del Contrato. En caso de que **"EL PROVEEDOR"** no dé aviso en el término a que se refiere este párrafo, acepta que no podrá reclamar caso fortuito o fuerza mayor.

"EL PROVEEDOR" podrá solicitar la modificación al plazo y/o fecha establecida para la conclusión de los servicios, por caso fortuito o fuerza mayor que ocurran de manera previa o hasta la fecha pactada.

Para estos efectos cuando **"EL PROVEEDOR"** por causa de fuerza mayor o caso fortuito no pueda cumplir con sus obligaciones en la fecha convenida, deberá solicitar por escrito a la Dirección General de Recursos Materiales Inmuebles y Servicios, con copia al Administrador del Contrato, una prórroga al plazo pactado, sin que dicha prórroga implique una ampliación al plazo original, acompañando los documentos que sirvan de soporte a su solicitud, en la inteligencia de que si la prórroga solicitada se concede y no se cumple, se aplicará la pena convencional correspondiente en términos de la cláusula denominada Penas Convencionales.

Cuando se determine justificado el caso fortuito o fuerza mayor, se celebrará entre las partes, a más tardar dentro de los treinta días naturales siguientes a que se reanuden los servicios o se actualice la condición operativa a que hubiere quedado sujeta la misma, un convenio modificatorio de prórroga al plazo respectivo sin la aplicación de penas convencionales, en términos del artículo 91 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, debiendo **"EL PROVEEDOR"** actualizar las garantías correspondientes.

En caso de que **"EL PROVEEDOR"** no obtenga la prórroga de referencia, por ser causa imputable a éste el atraso, se hará acreedor a la aplicación de las penas convencionales correspondientes.

No se considera caso fortuito o fuerza mayor, cualquier acontecimiento resultante de la falta de previsión, negligencia, impericia, provocación o culpa de **"EL PROVEEDOR"**, o bien, aquellos que no se encuentren debidamente justificados, ya que de actualizarse alguno de estos supuestos, se procederá a la aplicación de las penas convencionales que se establecen en la cláusula correspondiente.

En caso de que la suspensión obedezca a causas imputables a **"LA SEMARNAT"**, ésta deberá reembolsar, además de lo señalado en el párrafo anterior, los gastos no recuperables que haya erogado **"EL PROVEEDOR"** siempre y cuando se encuentren debidamente comprobados y se relacionen directamente con el objeto del contrato, o bien, podrá modificar el contrato a efecto de prorrogar la fecha o plazo para la prestación de los servicios. En este supuesto deberá formalizarse el convenio modificatorio respectivo, no procediendo la aplicación de penas convencionales por atraso. Asimismo, y bajo su responsabilidad podrá suspender la prestación del servicio, en cuyo caso únicamente se pagarán aquellos que hubiesen sido efectivamente prestados.

VIGÉSIMA SEGUNDA.- TERMINACIÓN ANTICIPADA DEL CONTRATO

Ambas partes convienen que para los efectos de que sea **"LA SEMARNAT"** quien podrá en cualquier tiempo dar por terminada anticipadamente la relación contractual que se formaliza 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 al Estado o se determine la nulidad total o parcial de los actos que dieron origen al contrato con motivo de la resolución que emita la autoridad competente en un recurso de inconformidad o intervención de oficio emitida por la Secretaría de la Función Pública, lo anterior de conformidad con el artículo 54 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y primer párrafo del artículo 102 de su Reglamento.

En este supuesto **"LA SEMARNAT"** procederá a reembolsar, previa solicitud de **"EL PROVEEDOR"** los gastos no recuperables en que haya incurrido siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con este contrato, los cuales serán pagados dentro de un término que no podrá exceder de cuarenta y cinco días naturales posteriores a la solicitud fundada y documentada por **"EL PROVEEDOR"**.

"EL PROVEEDOR", en términos de lo dispuesto en el artículo 102 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, podrá solicitar de manera fundada y documentada a **"LA SEMARNAT"** el pago de gastos no recuperables, en un plazo máximo de un mes contado a partir de la fecha de la terminación anticipada del contrato.

Lo anterior, en términos del artículo 54 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. Para tal efecto pagará a **"EL PROVEEDOR"** los servicios efectivamente prestados, hasta la fecha de la terminación.

La terminación anticipada se sustentará mediante dictamen que **"LA SEMARNAT"** elabore y en el que se precisen las razones o las causas justificadas que dan origen a la misma.

VIGÉSIMA TERCERA.- CESIÓN DE DERECHOS

"EL PROVEEDOR" no podrá ceder, vender, traspasar o subcontratar los derechos y obligaciones derivados del presente contrato, en ninguna forma y por ningún concepto, a favor de cualquier otra persona, con excepción de los

derechos de cobro, en cuyo caso deberá contar con el consentimiento expreso y por escrito de **"LA SEMARNAT"**, en términos del artículo 46, último párrafo, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

"LA SEMARNAT" manifiesta su consentimiento, para que **"EL PROVEEDOR"** pueda ceder sus derechos de cobro a favor de un intermediario financiero, mediante operaciones de factoraje o descuento electrónico en cadenas productivas, conforme a lo previsto en las Disposiciones Generales a las que deberán sujetarse las Dependencias y Entidades de la Administración Pública Federal para su incorporación al Programa de Cadenas Productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo, publicados en el Diario Oficial de la Federación el 28 de febrero de 2007, y sus reformas y adiciones publicadas el 6 de abril de 2009 y 25 de junio de 2010.

VIGÉSIMA CUARTA.- AUTONOMÍA DE LAS DISPOSICIONES

La invalidez, ilegalidad o falta de coercibilidad de cualquiera de las disposiciones del presente contrato de ninguna manera afectarán la validez y coercibilidad de las demás disposiciones del mismo.

VIGÉSIMA QUINTA.- INTERVENCIÓN

LAS SECRETARÍAS DE HACIENDA Y CRÉDITO PÚBLICO, DE LA FUNCIÓN PÚBLICA, Y DE ECONOMÍA, así como el Órgano Interno de Control en **"LA SEMARNAT"** y demás órganos fiscalizadores tendrán la intervención que las leyes y reglamentos en la materia les señalen, en la celebración y cumplimiento de este contrato.

VIGÉSIMA SEXTA.- RESPONSABILIDAD LABORAL, CIVIL Y FISCAL

Para efectos del cumplimiento del presente contrato, **"EL PROVEEDOR"** se obliga a proporcionar el personal especializado para la ejecución de los servicios contratados y será responsable de los antecedentes de su personal, garantizándolos en forma adecuada, por lo que queda expresamente estipulado que el presente contrato se suscribe en atención a que **"EL PROVEEDOR"** cuenta con el personal técnico y profesional necesario, experiencia, materiales, equipo e instrumentos de trabajo propios para ejecutar los servicios objeto del mismo.

"EL PROVEEDOR" reconoce y acepta que actúa como empresario y patrón del personal que ocupa para la ejecución del objeto de este contrato, por lo que será el único responsable de las obligaciones derivadas de las disposiciones legales y demás ordenamientos en materia del trabajo y seguridad social para con sus trabajadores.

Asimismo, **"EL PROVEEDOR"** reconoce y acepta que, con relación al presente contrato, actúa exclusivamente como proveedor independiente, por lo que nada de lo contenido en este instrumento jurídico, ni la práctica comercial entre las partes, creará una relación laboral o de intermediación en términos del artículo 13 de la Ley Federal del Trabajo, entre **"EL PROVEEDOR"**, incluyendo sus vendedores y/o subcontratistas y sus respectivos funcionarios o empleados, y **"LA SEMARNAT"**.

Asimismo, las partes aceptan y reconocen expresamente que no son aplicables a este contrato, las disposiciones de la Ley Federal del Trabajo, ni de la Ley Federal de los Trabajadores al Servicio del Estado, reglamentaria del apartado "B" del artículo 123 constitucional sino únicamente la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y demás normatividad aplicable.

Por lo anterior, en caso de cualquier reclamación o demanda, relacionada con los supuestos establecidos en la presente cláusula y proveniente de cualquiera de las personas antes mencionadas, que pueda afectar los intereses de **"LA SEMARNAT"** o involucrarla, , **"EL PROVEEDOR"** exime desde ahora a **"LA SEMARNAT"** de cualquier responsabilidad fiscal, laboral y de seguridad social, civil, penal y de cualquier otra índole, que pudiera darse como consecuencia directa de la prestación de los servicios materia del presente instrumento, quedando obligado a intervenir de manera inmediata en estos casos, por lo que en ningún momento se considerará como patrón sustituto o solidario, ni como intermediaria a **"LA SEMARNAT"** respecto de dicho personal.

VIGÉSIMA SÉPTIMA.- INFORMACIÓN Y CONFIDENCIALIDAD

Que para garantizar el acceso a la información pública de conformidad con los artículos 1, 23 y 24, fracción XI de la Ley General de Transparencia y Acceso a la Información Pública, las partes otorgan su consentimiento, para que en caso de solicitarse de acuerdo al procedimiento correspondiente, se proporcionen los datos que obran en el presente instrumento jurídico, salvo los que dicha normatividad la considere como información confidencial o reservada, en términos de los artículos 3, 113, 114, 116 y 117 de la Ley General de Transparencia y Acceso a la Información Pública.

Por su parte, **"EL PROVEEDOR"** se obliga a comunicar a **"LA SEMARNAT"** de cualquier hecho o circunstancia que en razón de los bienes entregados sea de su conocimiento y que pueda beneficiar o evitar un perjuicio a la misma.

"EL PROVEEDOR" se obliga a guardar confidencialidad de los trabajos o bienes adquiridos y a no proporcionar ni divulgar datos o informes inherentes a los mismos.

"EL PROVEEDOR" igualmente conviene en limitar el acceso a dicha información confidencial, a sus empleados o representantes, a quienes en forma razonable podrá dar acceso, sin embargo, necesariamente los harán partícipes y obligados solidarios con él mismo, respecto de sus obligaciones de confidencialidad pactadas en virtud de este pedido.

Cualquier persona que tuviere acceso a dicha información deberá ser advertida de lo convenido en este pedido, comprometiéndose a realizar esfuerzos razonables para que dichas personas observen y cumplan lo estipulado en esta cláusula.

Ambas partes convienen en considerar información confidencial a toda aquella relacionada con las actividades propias de **"LA SEMARNAT"** así como la relativa a sus funcionarios, empleados, consejeros, asesores, incluyendo sus consultores.

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

También será considerada información confidencial, la proporcionada y/o generada por **"LA SEMARNAT"** que no sea del dominio público y/o del conocimiento de las autoridades.

Las obligaciones de confidencialidad asumidas por **"EL PROVEEDOR"** en virtud de este pedido subsistirán ininterrumpida y permanentemente con toda fuerza y vigor aún después de terminado o vencido el plazo del presente pedido, en el territorio nacional o en el extranjero.

En caso de incumplimiento a las obligaciones estipuladas en esta cláusula, **"EL PROVEEDOR"** conviene en pagar los daños y perjuicios que en su caso ocasione a **"LA SEMARNAT"**.

Que para garantizar el acceso a la información pública de conformidad con los artículos 3 y 5 de la Ley Federal de Transparencia y Acceso a la Información Pública y el artículo 70 fracciones XXVII, XXVIII de la Ley General de Transparencia y Acceso a la Información Pública, las partes otorgan su consentimiento, para que en caso de solicitarse de acuerdo al procedimiento correspondiente, se proporcionen los datos que obran en el presente instrumento jurídico, salvo los que la propia ley considera como información confidencial o reservada, en términos de los artículos 110 y 113 de la Ley Federal de Transparencia y Acceso a la Información Pública .

Por su parte, **"EL PROVEEDOR"** se obliga a comunicar a **"LA SEMARNAT"** de cualquier hecho o circunstancia que en razón de los servicios prestados sea de su conocimiento y que pueda beneficiar o evitar un perjuicio a la misma.

"EL PROVEEDOR" se obliga a guardar confidencialidad de los trabajos o servicios contratados y a no proporcionar ni divulgar datos o informes inherentes a los mismos.

"EL PROVEEDOR" igualmente conviene en limitar el acceso a dicha información confidencial, a sus empleados o representantes, a quienes en forma razonable podrá dar acceso, sin embargo, necesariamente los harán partícipes y obligados solidarios con él mismo, respecto de sus obligaciones de confidencialidad pactadas en virtud de este contrato.

Cualquier persona que tuviere acceso a dicha información deberá ser advertida de lo convenido en este contrato, comprometiéndose a realizar esfuerzos razonables para que dichas personas observen y cumplan lo estipulado en esta cláusula.

Ambas partes convienen en considerar información confidencial a toda aquella relacionada con las actividades propias de **"LA SEMARNAT"** así como la relativa a sus funcionarios, empleados, consejeros, asesores, incluyendo sus consultores.

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

También será considerada información confidencial, la proporcionada y/o generada por **"LA SEMARNAT"** que no sea del dominio público y/o del conocimiento de las autoridades.

Las obligaciones de confidencialidad asumidas por **"EL PROVEEDOR"** en virtud de este contrato subsistirán ininterrumpida y permanentemente con toda fuerza y vigor aún después de terminado o vencido el plazo del presente contrato, en el territorio nacional o en el extranjero.

En caso de incumplimiento a las obligaciones estipuladas en esta cláusula, **"EL PROVEEDOR"** conviene en pagar los daños y perjuicios que en su caso ocasione a **"LA SEMARNAT"**.

VIGÉSIMA OCTAVA.- PATENTES, MARCAS Y DERECHOS DE AUTOR

"EL PROVEEDOR" asume toda la responsabilidad por las violaciones que se causen en materia de patentes, marcas y derechos de autor, con respecto a la propiedad de los trabajos o servicios objeto de este contrato.

En caso de llegarse a presentar una demanda en los términos establecidos en el párrafo anterior, **"LA SEMARNAT"** notificará a **"EL PROVEEDOR"**, para que tome las medidas pertinentes al respecto, **"EL PROVEEDOR"** exime a **"LA SEMARNAT"** de cualquier responsabilidad.

"EL PROVEEDOR" tendrá derecho a que se respeten los derechos de autor que en su caso se generen por la prestación de los servicios objeto del presente contrato y cede, en todo caso, a **"LA SEMARNAT"** los derechos patrimoniales que le pudieran corresponder u otros derechos exclusivos que resulten, mismos que invariablemente se constituirán a favor de **"LA SEMARNAT"**.

VIGÉSIMA NOVENA.- RECONOCIMIENTO CONTRACTUAL

El presente contrato constituye el acuerdo único entre las partes en relación con el objeto del mismo y deja sin efecto cualquier otra negociación o comunicación entre éstas, ya sea oral o escrita, anterior a la fecha en que se firme el mismo.

Las partes acuerdan que en el caso de que alguna de las cláusulas establecidas en el presente instrumento fuere declarada como nula por la autoridad jurisdiccional competente, las demás cláusulas serán consideradas como válidas y operantes para todos sus efectos legales.

"EL PROVEEDOR" reconoce que los convenios modificatorios y/o de terminación anticipada y/o de prórroga serán suscritos por el servidor público que firma este contrato, o quien lo sustituya o quien esté facultado para ello.

"EL PROVEEDOR" reconoce y acepta que la rescisión administrativa de este contrato podrá llevarse a cabo por el servidor público que lo suscribe o quien esté facultado para ello.

Para el caso de que exista discrepancia entre la Convocatoria a la Licitación Pública y el Contrato, prevalecerá lo establecido en la Convocatoria, las modificaciones a la misma y las que resulten de la o las juntas de aclaraciones.

TRIGÉSIMA.- CONCILIACIÓN

De acuerdo con lo dispuesto por los artículos 77, 78 y 79 de la Ley de Adquisiciones, Arrendamientos y servicios del Sector Público, en cualquier momento durante la vigencia del presente contrato, se podrá solicitar ente la Secretaría de la Función Pública o el Órgano interno de Control de esta Secretaría, procedimiento de conciliación por desavenencias derivadas del cumplimiento del presente contrato, el cual podrá ser requerido por cualquiera de las partes.

El procedimiento de conciliación, no podrá solicitarse si el presente contrato fue rescindido administrativamente, ello sin perjuicio de que se solicite conciliación respecto del finiquito que deban formularse como consecuencia de la rescisión determinada.

Si en el procedimiento de conciliación, se llega a un acuerdo respecto del cumplimiento del presente contrato, la validez del mismo, estará condicionada a la formalización del convenio ante autoridad judicial.

No podrá iniciarse otra conciliación sobre los mismos aspectos cuando las partes en un procedimiento anterior no hayan logrado un arreglo, salvo que en la nueva solicitud de conciliación se aporten elementos no contemplados en la negociación anterior.

TRIGÉSIMA PRIMERA.- JURISDICCIÓN

Las partes convienen que, para la interpretación y cumplimiento de este contrato, así como para lo no previsto en el mismo, se someterán a la jurisdicción y competencia de los Tribunales Federales con residencia en la Ciudad de México, renunciando al fuero que pudiera corresponderles en razón de su domicilio o vecindad presente o futura o por cualquier otra causa.

LEÍDO QUE FUE POR LAS PARTES QUE EN EL INTERVIENEN Y SABEDORES DE SU CONTENIDO, ALCANCE Y EFECTOS LEGALES, SE FIRMA EL PRESENTE CONTRATO, CONSTANTE DE 20 FOJAS ÚTILES Y 326 FOJAS QUE CONFORMAN EL ANEXO ÚNICO, PARA HACER UN TOTAL DE 346, EN CINCO TANTOS, AL CALCE Y AL MARGEN POR TODOS LOS QUE EN EL INTERVIENEN EN LA CIUDAD DE MÉXICO, EL DÍA 14 DE JULIO DE 2017.

POR "LA SEMARNAT".

Ing. Eduardo Juan Guerrero Valdez.
Director General de Recursos Materiales, Inmuebles y Servicios.

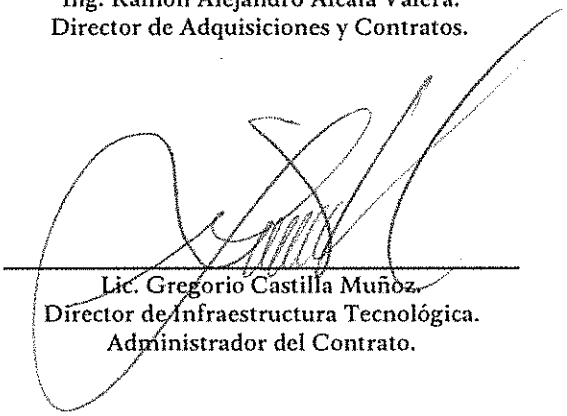
Mtro. Mario Héctor Góngora Preciado.
Director General de Informática y Telecomunicaciones.

POR "EL PROVEEDOR".

C. Elizabeth Saldaña Robles.
Representante Legal de "Soluciones Integrales SAYNET, S.A. de C.V.

CONTRATO DGRMIS- DAC-DGIT-005/2017.

Ing. Ramon Alejandro Alcala Valera.
Director de Adquisiciones y Contratos.



Lic. Gregorio Castilla Muñoz.
Director de Infraestructura Tecnológica.
Administrador del Contrato.

LAS ANTEFIRMAS Y FIRMAS QUE ANTECEDEN CORRESPONDEN AL CONTRATO DGRMIS-DAC-DGIT-005/2017, DE FECHA 14 DE JULIO DE 2017, QUE CELEBRA EL EJECUTIVO FEDERAL POR CONDUCTO DE LA SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES, CON "SOLUCIONES INTEGRALES SAYNET, S.A. DE C.V."- CONSTE.

ANEXO 1 "ESPECIFICACIONES TÉCNICAS"

SEMARNAT

Oficialía Mayor
Dirección General de Informática y Telecomunicaciones
Dirección de Infraestructura Tecnológica

ANEXO TÉCNICO

SERVICIOS ADMINISTRADOS DE SEGURIDAD PERIMETRAL

Contenido

1 Antecedentes

La SEMARNAT tiene alojados en su Datacenter buzones de correo electrónico para 2,000 cuentas habilitadas y da servicios de Internet a 4,000 usuarios activos (internos como externos), 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 la SEMARNAT otorga a las áreas responsables para su adecuado funcionamiento, requiere contar con las soluciones y/o herramientas tecnológicas.

A continuación, se describe brevemente el propósito específico de cada una de las soluciones tecnológicas que se requieren para los servicios descritos en el presente anexo técnico:

- 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. En eventos recientes se han saturado los enlaces de comunicaciones de la Secretaría, provocando con esto retrasos en la comunicación por correo electrónico, en los sistemas de acceso desde las delegaciones estatales y ventanillas, de igual forma para los servicios internos y en los externos que se proporcionan a la población. 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 para garantizar la disponibilidad, autenticidad e integridad de la información, previniendo también de posibles secuestros de la información.

Para cumplir con los puntos anteriores, se requiere de los servicios administrados (licenciamiento, soporte, mantenimiento y operación) para contar con las herramientas de seguridad perimetral de las oficinas centrales de la SEMARNAT y Datacenter.

La SEMARNAT es una Institución pública del Gobierno Federal, lo que la hace susceptible a ser blanco de diferentes tipos de ataques a través de Internet; por lo que se requiere de las herramientas y la administración adecuada de esta que protejan los servicios de la Institución y los accesos a la red interna en el perímetro como un primer punto de protección contra ataques dirigidos, intentos de engaños a los usuarios y aplicaciones maliciosas, que en caso de ingresar a la red pondría en riesgo la operación y continuidad de los servicios que se ofrecen a los usuarios internos y externos.

2 Objetivo General

Contar con los servicios administrados de seguridad perimetral, que incluya las herramientas tecnológicas actualizadas, y su soporte técnico que le permitan a la SEMARNAT la administración y protección de los servicios de Internet y la DMZ (este término se usa habitualmente para ubicar servidores a los cuales es necesario sean accedidos desde fuera, como servidores de: correo electrónico, aplicativos, filtrado de correo electrónico, DNS) y así obtener el mejor rendimiento e incrementar la eficiencia de operación para los usuarios y mitigar los riesgos de afectación para estos servicios por la entrada y ejecución de código malicioso o malware.

3 Objetivos especificos

- Contar con una solución integrada, flexible y robusta que le permita a la SEMARNAT proteger la información que analiza, genera y procesa.
- Alcanzar un modelo de seguridad de la información acorde a las necesidades actuales provenientes de Amenazas Avanzadas Persistentes (APTs), Técnicas Avanzadas de Evasión (EPS), y demás ataques cibernéticos.
- Identificar y analizar los huecos de seguridad que se puedan presentar en la infraestructura tecnológica.
- Brindar al usuario final un esquema funcional, confiable, seguro, libre de código malicioso en el intercambio de información que se realiza a través de internet y del correo electrónico en la Secretaria.

4 Alcance

La SEMARNAT tiene alojados en su Datacenter 2000 buzones de correo electrónico habilitadas, sistemas informáticos para uso interno y públicos y da servicios de Internet a 4,000 usuarios activos (internos como externos), los cuáles son usados para desempeñar funciones orientadas a los objetivos institucionales y cuyas actividades requieren, entre otros los servicios de navegación segura, así como tener acceso a la información y que sea garantizada su integridad.

El proyecto de "Servicios Administrados de Seguridad Perimetral" tiene como alcance la contratación de la protección para los activos de TI de la RED de SEMARNAT que permitirá proteger a 4,000 usuarios que cuenten con equipo de escritorio, a nivel nacional, cada oficina y delegación cuenta con infraestructura de comunicaciones y/o servidores que deben ser protegidos, al igual que los servicios del Centro de Datos, con esto se lograra:

- Proteger de la exposición a los riesgos de seguridad a la red y la información de la SEMARNAT.
- Tener la información necesaria para brindar al usuario final un esquema funcional, confiable, seguro, libre de código malicioso en el intercambio de información que se realiza a través de la RED de la Secretaria.
- Conocer la exposición a los riesgos para la seguridad de la red y la información.
- Con base en el nivel de riesgo de seguridad, se contará con las bases para robustecer la estrategia de seguridad de la información de la SEMARNAT.
- Identificación y priorización de brechas de seguridad que requieren mejoras en la SEMARNAT.
- Identificar de manera objetiva y eficiente, los controles de seguridad requeridos con base en los riesgos identificados, que permitan robustecer la postura de seguridad de la SEMARNAT.
- Habilitar una arquitectura de seguridad que brinde al usuario final un esquema de operación funcional, seguro y que minimice los riesgos de seguridad en la RED de la SEMARNAT.

En este sentido el proyecto ayudará a proporcionar servicios más seguros, rápidos y eficientes para el transporte de voz, datos y videoconferencia de manera convergente, mediante protocolo IP, con tecnología "Multi Protocol Label Switching" (MPLS) y enlaces a Internet, que se proporcionan a través de la red de telecomunicaciones de SEMARNAT.

Cabe precisar que existe un enlace MPLS con el INEGI que sirve de intermedio para conectarse a la red y hacer uso del aplicativo (COA WEB), estos servicios se usan eventualmente para dar atención a capacitaciones o seguimiento de dicho aplicativo.

5 Beneficios

Con la contratación de los "Servicios Administrados de seguridad Perimetral" se alcanzarán los siguientes beneficios, los cuales contribuirán para brindar mejores servicios a los ciudadanos:

- Permitirá mejorar el desempeño y uso del ancho de banda de las aplicaciones sustantivas e institucionales desarrolladas y publicadas por la SEMARNAT mediante internet.
- Permitirá contar con elementos de confidencialidad, protección de datos y análisis del tráfico en la infraestructura tecnológica de la SEMARNAT.
- Permitirá generar información con capacidad de análisis de eventos y de gestión de cambios eficientes que apoyen a la definición de los procesos de mejora continua en el ámbito de seguridad informática.
- Con el establecimiento de políticas de seguridad, la información que se almacene diariamente en nuestros aplicativos publicado en internet contarán con protección para ataques de negación de Servicio Distribuido (DDoS).

6 Consideraciones sobre la Infraestructura Tecnológica

El licitante deberá tomar en cuenta las siguientes consideraciones para realizar su oferta:

- SEMARNAT cuenta con un centro de datos y ha optimizado su infraestructura con 28 Hipervisores los cuales están localizados en un sitio principal y uno alterno para optimizar los servicios y contarán con un total de 150 servidores entre físicos y virtuales.
- El Centro de Datos cuenta con un enlace de 70 Mbps para el acceso a Internet y en sus oficinas centrales con capacidad de 250Mpbs.
- La SEMARNAT da servicios de internet a 4,000 usuarios activos, los cuáles para desempeñar funciones orientadas a los objetivos institucionales y cuyas actividades requieren de entre otros, los servicios de Internet lo cual es proporcionado por un enlace de 250 Mbps, y este deberá de ser protegido.
- La SEMARNAT requiere de los servicios administrados de seguridad perimetral para el Datacenter y Oficinas centrales, que incluya al menos FW, IPS, AntiBot e Inspección avanzada de Malware en alta disponibilidad.

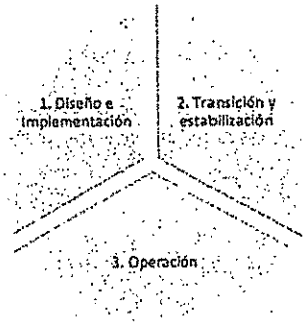
- Deberá contar con el establecimiento de mecanismos de cifrado de datos para la información que se transfiera mediante el uso de internet y MPLS.
- El equipamiento a considerar por el proveedor soporte al menos 200 Mbps para transferencia de información en Oficinas Centrales y 100 Mbps para el Centro de Datos.
- Considerar la criticidad de los datos para cada una de las etapas de Habilitación del Servicio, conforme a cada uno de los procesos de administración del MAAGTICSI requeridos para este servicio.
- El equipamiento requerido para proporcionar dichos servicios, deberá soportar preferentemente la versión 4 y 6 del protocolo de internet.
- Dichos servicios a contratar por la SEMARNAT serán adjudicados a un solo proveedor.

7 **Descripción de los Servicios**

El servicio solicitado consta principalmente de tres componentes, los cuales permitirán alcanzar un modelo de seguridad sostenible en el tiempo:

1. Tecnología: Proporcionará el aseguramiento en toda la infraestructura tecnológica (en los sitios de Ejercito Nacional, CONAGUA, 31 delegaciones, 4 sitios externos en la zona metropolitana y 1 en el estado de Aguascalientes -INEGI-), hardware y software para lograr el esquema de seguridad que la SEMARNAT requiere para garantizar el óptimo funcionamiento de los sistemas, preservar la seguridad de la información en su infraestructura tecnológica (enlaces de MPLS e Internet, routers y switches, equipo de filtrado web), garantizando el óptimo uso de los recursos de telecomunicaciones.
2. Procesos: Durante la implementación y operación de los servicios se deberán seguir los procesos y procedimientos definidos en el MAAGTICSI para tal fin, por lo que la propuesta del licitante deberá de estar adecuada a estos procesos, para trabajar con las mejores prácticas e interactuar con el personal de la SEMARNAT para garantizar la disponibilidad de los servicios sustantivos.
3. Personas: Para contar con una estrategia de seguridad completa y llegar a un modelo de alto nivel sostenible en el tiempo, se requiere contar con los recursos humanos suficientes y con los conocimientos adecuados tanto para operar como para ejecutar las acciones necesarias para este fin, los cuales deberán ser integrados por el licitante ganador desde el proceso de implementación, durante la operación y el proceso de administración, monitoreo y mejora continua del servicio.

8 Fases de Habilitación del Servicio



8.1 Diseño e Implementación.

Esta fase comprende la implementación-migración del servicio, debe tener una duración máxima de 4 semanas a partir del día hábil siguiente a la notificación del fallo e inicia con una reunión entre el licitante ganador y el servidor público designado por la SEMARNAT, para administrar el servicio. Al día hábil siguiente de la notificación del fallo se dará inicio la planeación del servicio y el licitante ganador realizará la entrega oficial del programa de trabajo y logística con la aprobación por parte de la SEMARNAT, en un máximo de 1 semana.

En su propuesta técnica el licitante debe proporcionar un programa de actividades a ejecutar para cumplir con los entregables que la SEMARNAT le solicita para esta fase.

El licitante incluirá en el programa la fecha de entrega de los componentes y demás entregables que habilitarán el servicio, que no deben de exceder 4 semanas a partir del día hábil siguiente de la notificación del fallo.

8.1.1 Actividades de la fase de Diseño e Implementación:

Las siguientes actividades correspondientes a esta fase son enunciativas más no limitativas:

- Planeación y Diseño.

Durante esta fase se validará el plan de trabajo de implementación de la solución en conjunto con la SEMARNAT, además se adicionará al mismo las tareas necesarias para la revisión y adecuación de los procesos tanto internos del licitante como los de SEMARNAT para lograr la alineación al MAAGTICSI en los procesos de ADS, ACNF, ASI, AOP y OPEC.

Para lo anterior, el licitante deberá asignar un Administrador del Proyecto, un Arquitecto y al menos 1 Ingeniero capacitado en las herramientas propuestas para que en conjunto con el personal que SEMARNAT, realicen las reuniones de trabajo en las cuales se definirán los alcances (línea base) de los servicios solicitados.

Para cada reunión con el licitante, se deberá generar una minuta de acuerdo, en la que se especifiquen las fechas compromiso, de acuerdo a la fase o etapa correspondiente de los servicios solicitados y que estén alineadas al cronograma de trabajo.

El plan de trabajo, deberá incluir cada una de las funciones de los integrantes a participar en cada una de sus actividades y tiempos para alcanzar la realización de las demás fases del servicio solicitado.

- Entregables:
    1. Plan de trabajo de la fase de Implementación

- **Instalación.**

Una vez definidas las actividades de implementación y haber recabado la información técnica necesaria se deberá empezar con la implementación de los equipos que conforman la solución, además de la adecuación de los procedimientos para alinearlos con MAAGTICSI.

Por tanto, al cumplir la totalidad de los requerimientos solicitados para cada servicio en base a lo establecido en el plan de trabajo de la fase anterior, el prestador del servicio generará por localidad un "Acta de Entrega-Recepción de Servicios", firmada por un representante del prestador del servicio y por personal de SEMARNAT asignado para tal efecto, en la cual se indicarán los servicios instalados, así como la fecha de inicio de su operación.

Además, el Arquitecto por parte del Licitante, deberá dar seguimiento al plan de trabajo y deberá de recopilar todas las evidencias (minutas de las reuniones, avances de la alineación de los procesos y procedimientos de acuerdo a MAAGTICSI) que den sustento a las tareas concluidas.

- Entregables:
  1. Acta de Entrega-Recepción de Servicio

- Configuración.

La configuración de los componentes que habilitan el servicio de seguridad perimetral debe:

1. Habilitar el sistema de firewall de siguiente generación
2. Habilitar el sistema de IPS y prevención de amenazas
3. Habilitar el sistema de Consola de Administración

En esta etapa se deberán integrar las configuraciones de todos los componentes que habilitan el servicio, definir y crear los perfiles de administración indicados por la SEMARNAT y definir las políticas de operación de las soluciones.

SEMARNAT proporcionará la información técnica requerida para la configuración de las soluciones como: reglas de los equipos actuales, tablas de ruteo, objetos, direccionamiento, tipos de reportes, definiciones para crear alertas, etc.

El licitante deberá incluir mecanismos de seguridad que soporten y habiliten servicios para red privada o local, así como también soportar el envío de información y datos para la seguridad perimetral.

El licitante podrá realizar la instalación de los dispositivos o componentes que conforman el servicio estableciendo de común acuerdo con SEMARNAT las ventanas de tiempo. De ser posible estas serán en el horario laboral indicado por SEMARNAT.

- Entregables:
  1. Memoria técnica de la solución implementada.

- **Pruebas y Validación.**

El licitante realizará las pruebas necesarias para verificar que se tiene acceso a los servicios institucionales, correo, navegación internet e intranet, DNS, WINS, SAP y los sistemas que indique SEMARNAT, el personal de SEMARNAT validará que la solución funciona conforme lo establecido durante la fase de planeación y diseño.

SEMARNAT en conjunto con el licitante deberá definir el protocolo de pruebas que será aplicado por el licitante, mismas que deberán ser avaladas por el responsable del Servicio de SEMARNAT.

Si el protocolo de pruebas no fue satisfactorio, se considerará como servicio no entregado con la consecuente aplicación de la deductiva, por cada día de atraso en la entrega del protocolo satisfactorio, siempre y cuando sea atribuible al licitante.

El personal autorizado de SEMARNAT tendrá en todo momento la facultad para supervisar los trabajos que realice el licitante, con motivo de la prestación de los servicios. El licitante debe responder a cualquier consulta técnica que surja por parte del personal responsable acerca del servicio contratado, en el periodo de duración del servicio.

- Entregables:
  1. Protocolo de pruebas avalado por personal de la SEMARNAT
  2. Notificación por parte del licitante de conclusión de la fase de diseño y planeación e inicio de la fase de transición y estabilización.

8.2 Transición y Estabilización.

La fase de transición y estabilización del servicio tiene el objetivo de garantizar que los servicios implementados se encuentran estables y listos para la operación del servicio administrado. Dicha fase tendrá una duración máxima de 1 semana, concluida la fase de Diseño e Implementación.

8.2.1 Actividades de la fase de Transición y Estabilización

Las siguientes actividades a esta fase son enunciativas más no limitativas:

- Afinación y estabilización.

Durante esta fase el licitante deberá detectar y ejecutar los puntos de mejora en las políticas, configuraciones, permisos o cualquier configuración que degrade la operación del servicio administrado.

- Entregables:
  1. Reporte de hallazgos y recomendaciones implementadas derivadas de la fase de afinación y estabilización.
  2. Notificación por parte del licitante de conclusión de la fase de transición y estabilización e inicio de la fase de operación.

8.3 Operación.

La puesta en marcha de la operación, inicia el día siguiente de la finalización del periodo de transición y estabilización, con un oficio validado por la SEMARNAT que ha concluido la implementación y estabilización de los servicios, dando comienzo a la fase de operación de la seguridad administrada.

8.3.1 Actividades de la fase de Operación

Las siguientes actividades a esta fase son enunciativas más no limitativas:

- Monitoreo.

El principal objetivo del monitoreo es mantener la disponibilidad del servicio de seguridad perimetral conforme a los niveles de servicio establecidos en este documento.

El monitoreo de los componentes que habilitan el servicio debe ser continuo, las 24 horas del día durante todos los días del año, a partir del inicio de la fase de operación y hasta el final de la vigencia del contrato.

La solución de seguridad perimetral debe permitir el acceso a través de un canal seguro para dicho monitoreo.

El equipamiento y software proporcionados por el licitante deberán ser retirados de las instalaciones de la SEMARNAT una vez formalmente terminado el contrato de servicio.

Las especificaciones técnicas de este equipo, serán a consideración del licitante, así como el esquema de conexión.

Con el fin de mantener la integridad, confidencialidad y disponibilidad de los activos clave de información relacionados al servicio de seguridad perimetral, el licitante debe levantar de manera proactiva el ticket o solicitud correspondiente cuando producto del monitoreo, se detecte la no disponibilidad, degradación o falla de cualquiera de los dispositivos o componentes que habilitan el servicio, manteniendo en todo momento la comunicación y seguimiento con la mesa de servicios.

El licitante debe permitir el acceso al personal autorizado de la SEMARNAT al sistema de monitoreo con perfil de solo lectura.

- Administración.

El licitante debe contar con una Mesa de Servicios para la atención a solicitudes de servicio e incidentes, cuyo objetivo es fungir como punto de contacto entre el licitante y el personal de la SEMARNAT, con la capacidad de atender dichas solicitudes, en el horario laboral de la SEMARNAT.

Proporcionar asistencia y soporte técnico de segundo y tercer nivel, telefónico o presencial, en formato de 7X24 y en español, durante toda la vigencia del contrato.
El licitante será responsable en todo momento de la gestión satisfactoria de los reportes generados, asegurando que los incidentes y requerimientos reportados sean resueltos dentro de los niveles de servicio acordados, realizando o emprendiendo acciones para eliminar las causas de raíz y/o para prevenir fallas potenciales.

En caso de que la falla sea atribuible a la SEMARNAT se turnará el reporte al área indicada de la SEMARNAT para resolverla lo antes posible y no aplicará deducción-penalización. Si la falla es atribuible al licitante éste le dará una atención hasta la solución de la misma y en su caso aplicará la deducción-penalización correspondiente de acuerdo a los niveles de servicio.

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

9 Especificaciones Generales del Servicio

El licitante deberá presentar su propuesta técnica ajustándose a los requerimientos técnicos solicitados por SEMARNAT, los cuales deberán considerarse como mínimos salvo que se exprese lo contrario. Será motivo de descalificación no cumplir con alguno de los requerimientos técnicos mínimos.

El licitante debe considerar los cables, accesorios y herrajes de sujeción necesarios para el montaje de sus equipos a ofertar para su instalación, solo se proporcionará el espacio físico en los Racks.

El licitante y su personal se obligan a no difundir, por ningún medio y por ningún motivo, la documentación ni información que por virtud de los servicios objeto de este contrato tenga acceso, sin la autorización previa o por escrito de la SEMARNAT. Asimismo, se obliga a no hacer uso indebido de los activos de la dependencia.

Todas las erogaciones y gastos que para la prestación de los servicios que haga el licitante por concepto de pagos a su personal, adquisición, transporte de los bienes, amortizaciones, viáticos, mantenimientos, adquisición de materiales, útiles, artículos, primas de seguros y deducibles, impuestos y por cualquier otro concepto serán directamente a cargo del licitante.

10 Solución Requerida

Se necesita que con los servicios propuestos sea posible estructurar una primera línea de protección bajo un esquema de seguridad institucional. Por esto, la SEMARNAT requiere de una solución que opera acorde a los procesos de "Administración de Servicios "(ADS), "Administración de la Operación" (AOP), "Administración de la Seguridad de la Información" (ASI) , "Operación de los Controles de la Información y del ERISC" (OPEC), "Administración de la Configuración" (ACNF) definidos en el MAAGTICSI.

Las características mínimas requeridas que deberán acompañar a esta solución:

1. Configurar las reglas de seguridad en los equipos administrados, las cuales serán propuestas por el equipo de seguridad del "Licitante" y validadas por el personal designado de acuerdo a los objetivos y a los lineamientos de normatividad bajo el cual se rige la SEMARNAT.
2. Mejorar la administración de la seguridad implementada en la SEMARNAT en relación a la normatividad vigente del MAAGTICSI.
3. Monitoreo proactivo de la solución.
4. Mantenimiento y soporte operativo de la solución para cumplir con los niveles de servicio solicitados.
5. Cambios a políticas y requerimientos de seguridad por parte de la SEMARNAT solicitados al licitante, que deberán estar alineados a los niveles de servicios y tiempos de respuesta establecidos por la Institución.
6. Diagnosticar las fallas de hardware o software de los dispositivos que sean parte de la solución, así como generar y dar seguimiento a los reportes que deberán de tener relación con los fabricantes directamente involucrados, mismas que deberán ser aplicados para garantizar la continuidad del servicio.

7. Administración y monitoreo de los equipos requeridos para este servicio.
8. Generación de reportes para apoyo a auditorías y los solicitados como entregables.
9. Las solicitudes de reportes establecidos son enunciativos más no limitativos, por lo que la SEMARNAT podrá solicitar cualquier otro que se requiera de acuerdo a los requerimientos según el anexo técnico.
10. El licitante deberá entregar una MEMORIA TÉCNICA, 15 días hábiles posterior a la implementación, que deberá contener los siguientes aspectos:
    a. Descripción del Proyecto.
    b. Cronograma del Proyecto.
    c. Diagrama a Bloques del Diseño del Proyecto (conforme a lo establecido en el cronograma)
    d. Diagrama Esquemático de Conexiones y configuraciones de cada localidad.
    e. Documentación de rutas, políticas y configuraciones iniciales de los equipos.
    f. Respaldo en medio magnético de todas las configuraciones realizadas a todos los equipos.
    g. Hojas técnicas de los equipos y servicios instalados (la cual deberá contener numero serie, equipo, modelo, etc.) los campos quedarán a definición de la SEMARNAT para dicha entrega.
    h. Memoria fotográfica y/o imágenes con detalle de la instalación sobre el avance y desarrollo del Proyecto (antes y después de la instalación).
    i. Se deberá entregar en medio electrónico al administrador del contrato.

Los "Servicios Administrados de Seguridad Perimetral" deberán operar bajo los procesos definidos por la SEMARNAT para la "Administración de Servicios "(ADS), "Administración de la Operación" (AOP), "Administración de la Seguridad de la Información" (ASI) y "Operación de los Controles de la Información y del ERISC" (OPEC), "Administración de la Configuración" (ACNF) definidos por la SEMARNAT:

Clasificación	Funcionalidad
Implementación de la solución alineado con MAAGTICSI - ADS	Elaboración, diseño e implementación en la infraestructura de seguridad, así como la elaboración del establecimiento de políticas en materia de seguridad de la información de acuerdo a las necesidades requeridas por la Secretaría.
Admón. de Servicios conforme a MAAGTICSI – ADS	Análisis y reportes de tendencia de uso, utilización y tráfico.
	Monitoreo y administración de variables de desempeño para mejoramiento operativo, proactivo y correctivo.
	Configuración inicial y evolutiva de variables de equipo para mejora en desempeño
	Activación de funcionalidades soportadas por el equipo y de acuerdo a recomendación de desempeño.
	Revisión de log's obtenidos de los equipos bajo administración
	Generación de reportes para auditorías
Admón. de monitoreo, incidentes y problemas de la solución conforme a MAAGTICSI – AOP –OPEC	Notificación de eventos derivados del monitoreo realizado.
	Mantenimiento y actualización de plataforma operativa y software (Fixes y parches) de acuerdo a validación y aceptación.
	Reportes de Solicitudes de Requerimientos
	Reporte de eventos e incidentes

Clasificación	Funcionalidad
	Escalación de incidentes hacia fabricante de ser requerido o necesario
	Seguimiento de problemas hasta su resolución
	Cierre de problemas con recomendación.
Admón. de Configuración conforme a MAAGTICSI – ACNF	Actualización y almacenamiento de configuraciones
	Respaldo de configuraciones de equipo e infraestructura
	Admón. de inventario de equipo, licenciamiento y contratos de soporte del fabricante
	Admón. de reemplazos por falla, eficiencia, cambio de domicilio, etc.
	Admón. de accesos lógicos a los componentes de la solución.
Admón. de Cambios conforme a MAAGTICSI – AOP	Validación inicial de cambios solicitados
	Solicitud y manejo de cambios solicitados por mesa de servicio
	Escalación y seguimiento de solicitudes de cambio que requieran autorización
	Instalación y configuración de nuevas versiones
	Apoyo en la validación de versiones para su instalación
	Admón. y seguimiento de cambios
	Soporte técnico del "Licitante" ganador para cambios y/o modificaciones a esquemas de red solicitados por SEMARNAT.
	Manejo de reemplazo de equipo o partes de acuerdo a los servicios solicitados.
Admón. y análisis de riesgos conforme a MAAGTICSI – ASI	Identificar, clasificar y priorizar los Riesgos para evaluar su impacto sobre los procesos y los servicios de SEMARNAT.
	Generación de los controles de cambios para la mitigación de riesgos.
Operación de controles de seguridad de la información y respuesta a incidentes de seguridad de la información conforme a MAAGTICSI – OPEC	Ejecución de actividades de seguimiento a la implementación de controles.
	Integración con el Equipo de Respuesta a Incidentes de Seguridad de la Información, para aquellos incidentes de seguridad de la información en alcance del servicio.
	Identificación y categorización de incidentes de seguridad de la información.
	Atención a incidentes de seguridad de la información con base en la Guía técnica de atención a incidentes del proceso OPEC.

10.1 Alineación a Normatividad y Procesos

El licitante deberá alinearse a los procesos indicados en el MAAGTICSI para asegurar la confidencialidad, integridad y disponibilidad de la información y de los activos de información que protegen este servicio, así como la Operación de los Controles de Seguridad, como se indica a continuación:

Para el proceso ASI – Administración de la Seguridad de la Información, el licitante deberá contar con un especialista en gobierno de seguridad de la información en ASI, OPEC de MAAGTICSI, durante la fase de diseño e implementación y estabilización del servicio, lo que permitirá ejecutar actividades de alineación del servicio administrado de seguridad perimetral de la SEMARNAT a la normatividad aplicable en materia de seguridad de la información de la SEMARNAT, ejecutando de manera enunciativa mas no limitativa, las siguientes actividades:

1. Integración del Servicio Administrado de Seguridad Perimetral con el Modelo de Gobierno de Seguridad de la Información de SEMARNAT.
2. Actualización de la documentación de acuerdo al SGSI del SEMARNAT con base en la habilitación del Servicio Administrado de Seguridad Perimetral y definición de los mecanismos de seguimiento al servicio respecto al programa de evaluaciones del SGSI de SEMARNAT.
3. Análisis y ejecución de actividades de alineación de los dispositivos o componentes que habilitarán el servicio con el catálogo de activos de información e infraestructura clave de SEMARNAT
4. Actividades de análisis y actualización de la Arquitectura de Servicios relacionada al servicio administrado de seguridad perimetral de la SEMARNAT con base en las mejoras prácticas de la industria.
5. Actualización del catálogo de activos de información clave e infraestructuras críticas.
6. Con base en la metodología y los mecanismos de SEMARNAT en la administración de riesgos, el licitante deberá integrar a la evaluación de riesgos, posterior a la implementación de los componentes solicitados en el servicio administrado de seguridad perimetral de la SEMARNAT.
7. Actualización de la directriz rectora de respuesta a incidentes de seguridad de la información, derivado de los componentes del servicio.
8. Evaluación del SGSI con la integración de los componentes del servicio de seguridad perimetral, para la detección de hallazgos de mejora y generación de recomendaciones.

Para el proceso OPEC – Operación de los Controles de Seguridad de la Información y del ERISC, el licitante deberá contar con un especialista en gobierno de seguridad de la información en ASI, OPEC de MAAGTICSI, durante la fase de diseño e implementación y estabilización del servicio, lo que permitirá ejecutar actividades de alineación del servicio administrado de seguridad perimetral de la SEMARNAT a la normatividad aplicable en materia de seguridad de la información de la SEMARNAT, ejecutando de manera enunciativa mas no limitativa, las siguientes actividades:

- Seguimiento con base en el SGSI de la SEMARNAT, el diseño y la implementación de los controles de seguridad de la información que habilita el servicio administrado de seguridad perimetral de la SEMARNAT.
    - Diseño de los controles de seguridad que habilita el servicio administrado de seguridad perimetral de la SEMARNAT.
- Establecimiento de los procesos y guías de operación para la atención de incidentes de seguridad perimetral, con base lo definido en la Guía técnica de atención de incidentes de la SEMARNAT.

- Procesos y guías de operación para la atención de incidentes de seguridad perimetral de la SEMARNAT.
- Criterios para la identificación de incidentes de Seguridad perimetral y la interacción con el ERISC de SEMARNAT
- Criterios para la categorización de incidentes de seguridad perimetral
- Criterios de priorización de incidentes de seguridad perimetral
- Criterios para el cierre de incidentes de seguridad perimetral

10.2 Personal en sitio durante fase de implementación

Deberá designar el licitante, un Arquitecto Líder de la solución ofertada, durante la fase de Diseño e Implementación, para la coordinación de los servicios durante su implementación y puesta en operación, considerando el liderazgo del diseño de arquitecturas de red para diferentes escenarios de seguridad perimetral y en proporcionar soluciones que combinen tecnologías de diferentes propósitos, integrándolas bajo las mejores prácticas que se centran en el proceso de seguridad de redes e información con el objetivo de mitigar los riesgos y alinear los esfuerzos a la normatividad aplicable en materia de seguridad de la información.

El prestador del servicio proporcionará a su personal los medios y herramientas tecnológicas de trabajo (equipos de cómputo, líneas telefónicas celulares y demás aplicables) requeridas para llevar a cabo sus funciones.

El personal designado por el prestador del servicio, acudirá a las instalaciones de la SEMARNAT debidamente identificado y cumplirá con el código de Conducta de la institución.

10.3 Monitoreo de la solución

El servicio del Licitante deberá integrar una solución que permita monitorear el equipamiento considerados para el servicio requerido, de acuerdo al diseño propuesto de manera que pueda dar respuesta a los incidentes.

El servicio deberá contar con las siguientes funcionalidades:

1. Monitoreo de la disponibilidad de la infraestructura administrada y desempeño de la misma como
   a. Utilización de los recursos (red, CPU, memoria, disco, etc.)
   b. Bitácoras de los diferentes componentes habilitados para proveer los servicios.
      i. Sistema de seguridad perimetral

2. Se deberá desarrollar un tablero ejecutivo y ser accesible por un acceso VPN para contar con un resumen en tiempo real del monitoreo.
3. SEMARNAT una vez implementada la solución llave en mano, se reserva el derecho de visitar las instalaciones del centro de monitoreo del cliente de manera periódica para validar el monitoreo de la solución.
4. El licitante deberá proporcionar un número telefónico para reportes de incidentes del interior de la república.
5. La administración y monitoreo de seguridad deberá ser en un centro con las siguientes características mínimas:

    a. Atención y soporte de un equipo de personal con experiencia en las tecnologías propuestas, proveyendo un esquema continúo de operaciones y monitoreo proactivo 24x7, los 365 días del año.
    b. Los servicios de administración de seguridad deberán estar enlazados con la Mesa de Servicios del Licitante, lo cual permita tener información de incidentes que potencialmente afectan a SEMARNAT.
    c. El licitante deberá encargarse de contar con una de Mesa de Servicios preferentemente certificada en el estándar ISO/IEC 20000 y disponible en un esquema 7x24x365 se registren los requerimientos y se les dé seguimiento hasta su conclusión.
    d. El centro de monitoreo deberá contar con la infraestructura necesaria para albergar las consolas de administración y monitoreo de la solución propuesta.
    e. El centro de monitoreo del licitante deberá contar con acceso a Internet que permita la conectividad a través de VPN con SEMARNAT el cual garantice el monitoreo de los equipos y su administración.
    f. El centro de monitoreo y administración de seguridad deberá proporcionar visibilidad del servicio por medio de un portal Web.
    g. La SEMARNAT en cualquier momento podrá realizar una visita programada al Centro de Monitoreo por parte del licitante para verificar el monitoreo de sus servicios solicitados.

10.4 Mantenimiento preventivo y correctivo

El mantenimiento correctivo deberá cubrir la totalidad de los equipos que proporcionan el servicio objeto del presente procedimiento, garantizando la continuidad de éste, conforme a los niveles de servicio requeridos.

Además, se deberá de incluir el mantenimiento necesario en hardware, software y firmware para mantener la operación de los servicios requeridos.

11 Niveles de Servicio

11.1 *Atención de Incidentes*

Para todas las notificaciones hacia la SEMARNAT por motivo de algún incidente o evento identificado desde el centro de monitoreo, se deberán llevar a cabo mediante alguno de los siguientes medios en un lapso no mayor a 20 minutos después de ocurrido éste:

1. Teléfono
2. Correo electrónico
3. Notificación electrónica vía el Portal WEB de Mesa de Servicio

Con niveles de escalamiento de acuerdo a la severidad, definida a continuación:

Actividad	Severidad	Descripción
Incidente de Seguridad	Severidad 4	Afectación de Servicio. Eventos de alto riesgo, los cuales pueden ocasionar un daño severo en los activos de la SEMARNAT.
Incidente de Seguridad	Severidad 3	Degradación al Servicio. Eventos en donde se requiere que la SEMARNAT lleve a cabo una acción a partir de la notificación emitida por el licitante ganador.
Incidente de Seguridad	Severidad 2	Intermitencia de Servicio.
Solicitud de requerimiento	Severidad 1	Eventos de investigación, actualización de contenido de seguridad, cambios en configuraciones, Actualizaciones.

11.2 *Confirmación de Recepción de Solicitud de Cambios.*

Se refiere a la confirmación hecha hacia la SEMARNAT por parte del licitante de la recepción de solicitudes para cambios o modificaciones en la configuración o políticas de la infraestructura operada:

> Nivel de Servicio: La confirmación de la recepción de la solicitud de cambios se deberá hacer en un lapso no mayor de 30 minutos.

Este objetivo deberá aplicar para las solicitudes de cambio (altas, bajas y modificaciones) a la infraestructura solicitadas por el contacto designado por la SEMARNAT y de acuerdo a los procedimientos de control de cambios que se establecerán en conjunto con el licitante, alineado a los procesos del MAAGTICSI.

11.3 Administración de Incidentes Reportes de fallas

El equipo de especialistas del licitante deberá identificar los incidentes con severidad 1, 2 y 3 que afecten la operación del servicio basado en la información recibida del Centro de Monitoreo y Operaciones deberán ser atendidos de acuerdo a lo siguiente:

Actividad	Severidad	Detección / Notificación	Tiempo de Atención / Resolución
Afectación de servicio	Severidad 1	Incidentes con afectación al servicio (severidad 1) al contacto designado en sitio y al responsable designado por SEMARNAT en un lapso no mayor a 20 minutos de la afectación del servicio en las Oficinas Centrales.	30 min / restablecimiento del servicio máximo 1 hora
Degradación del servicio	Severidad 2	Notificación de incidentes con degradación al servicio (severidad 2) al contacto de seguridad designado por SEMARNAT en un lapso no mayor a 20 minutos de la afectación del servicio.	1 hora / 4 horas
Intermitencia del Servicio	Severidad 3	Notificación de incidentes con intermitencia al servicio (severidad 3) al contacto de seguridad designado por SEMARNAT en un lapso no mayor a 20 minutos de las intermitencias del servicio	1 hora / 8 horas
Solicitud de requerimiento	Severidad 4	Incidente sin afectación de servicio, en esta severidad se consideran los tiempos determinados, para cambios de configuraciones urgentes.	1 hora / 8 horas
		Respaldo de configuración	30 min / 18 horas
		Actualización de memoria técnica.	30 min / 3 días
		Actualización de sistema operativo	1 hora / 12 horas
		Ventanas de mantenimiento programadas y requeridas por el licitante (según el requerimiento)	30 min / 4 hrs hasta 8 horas

11.4 Cambios

Las actividades relacionadas con solicitudes de cambio hechas por SEMARNAT hacia el licitante ganador estarán conforme a los procesos y procedimientos definidos los cuales estarán alineados al proceso de ADS de MAAGTICSI y deberá incluir los siguientes niveles de servicio:

11.4.1 Análisis y revisión del cambio

El Licitante ganador deberá revisar y validar los cambios solicitados por SEMARNAT y alienados al proceso de AOP de MAAGTICSI, esto antes de ejecutarlos en producción siguiendo así un esquema que control de las solicitudes.

Nivel de servicio: Se llevará el análisis y revisión del cambio de las solicitudes para cambios a la infraestructura en un lapso no mayor a 5 (cinco) horas hábiles a partir de la confirmación de recepción de la solicitud. En caso de que dicha solicitud sea identificada con un estatus de "espera" debido a la falta de información o solicitud de ventana de mantenimiento por afectación, esta deberá ser solicitada a SEMARNAT en este mismo lapso.

Posterior a la revisión se le asignara un nivel de prioridad, de acuerdo al nivel de priorización y afectación del mismo.

11.4.2 *Implementación de cambios*

Se refiere a llevar a cabo la implementación de los cambios o modificaciones de configuración solicitados por la SEMARNAT esto alineado al proceso AOP de MAAGTICSI. Estos cambios se deberán dar en función de la siguiente medida:

Nivel de servicio: Se llevará a cabo la implementación de las solicitudes para cambios a la infraestructura en un lapso no mayor a 8 (ocho) horas hábiles posteriores al análisis y revisión del cambio. En caso de que dicha solicitud necesite de una ventana de mantenimiento esta será solicitada a SEMARNAT en el paso anterior y la implementación será realizada en dicha ventana.

Este objetivo solamente deberá aplicar para las solicitudes de cambios de políticas enviadas por el contacto designado por la SEMARNAT y de acuerdo a los procedimientos acordados con el Licitante.

12 Mesa de Servicio

La mesa de servicios de SEMARNAT será el único punto de contacto para que los usuarios de los activos y servicios de TIC hagan llegar sus solicitudes de servicio. Por lo tanto, la mesa de servicios del licitante deberá ejecutar la integración pertinente y definir los mecanismos de comunicación, control y seguimiento hacia la misma, para la atención de los incidentes de servicio y solicitudes del Servicio Administrado de Seguridad Perimetral, con base en los niveles de servicio acordados. La mesa de servicios deberá de operar el primer día de la puesta en marcha de la fase de Operación del Servicio.

El licitante deberá ejecutar procedimientos que permitan resolver con rapidez y eficiencia los requerimientos e incidentes que se presenten, así como la integración con la mesa de servicios de SEMARNAT.

Con el fin de mantener la integridad, confidencialidad y disponibilidad de los activos clave de información relacionados al servicio de seguridad perimetral, el licitante debe levantar de manera proactiva el ticket o solicitud correspondiente cuando producto del monitoreo, se detecte la no disponibilidad, degradación o falla de cualquiera de los dispositivos o componentes

que habilitan el servicio, manteniendo en todo momento la comunicación y seguimiento con la mesa de servicio de SEMARNAT.

13 Cartas y certificaciones

El licitante deberá presentar carta o cartas membretadas del fabricante de los equipos que formen parte de su propuesta la cual deberá venir dirigida a la SEMARNAT, donde especifique:

1. Que está autorizado para comercializar las soluciones propuestas para la prestación de los servicios de este procedimiento y que es distribuidor autorizado del mismo, deberá de venir firmada por el represente legal del fabricante.
2. El licitante deberá presentar documento donde especifique que los equipos que proporcione no tengan anuncio de fin de vida, ni anuncio de fin de mantenimiento.

TABLA DE PERFILES ESPECIALIZADOS

Arquitecto líder de la Solución	Arquitecto Líder Especialista en soluciones con experiencia en el diseño de arquitecturas de red para diferentes escenarios de seguridad perimetral y en proporcionar soluciones que combinen tecnologías de diferentes propósitos, integrándolas bajo las mejores prácticas que se centran en el proceso de seguridad de redes e información con el objetivo de mitigar los riesgos y alinear los objetivos de la organización con la estrategia de seguridad. Para las actividades que forman parte del Servicio Administrado de Seguridad Perimetral la SEMARNAT requiere por normatividad vigente, que en las fases de Diseño e Implementación de la arquitectura de seguridad, el licitante cuente con un Arquitecto líder que gestione las acciones de análisis, alineación y definición de políticas, procesos y mejores prácticas en la implantación de la solución así como asegurarse de la estabilización del servicio, establecer las directrices en materia de respuesta a incidentes de seguridad de la información con base en la normatividad aplicable para la SEMARNAT. Por lo tanto, es necesario que el Arquitecto líder de la solución cuente con habilidades técnicas que permitan la gestión de incidentes de seguridad de la información mediante la comprensión de las técnicas comunes de ataque, vectores y herramientas, que permitan habilitar las contramedidas necesarias ante la materialización de un incidente de seguridad de la información, incluyendo actividades de detección, respuesta y resolución El Arquitecto líder de la solución, debera demostrar experiencia de al menos 5 años y contar con al menos una de las siguientes certificaciones vigentes: • Certified Incident Handler (GCIH). • Certified Information Systems Security Professional (CISSP) • Maxima certificacion por parte del fabricante de la solucion
Especialista en alineación de servicios	Especialista en establecer alineaciones entre mesas de servicio, con la finalidad de garantizar la estabilidad de la operación, elaboración de catálogos, categorías, interfaces entre procesos, con la finalidad de garantizar que la operación y las solicitudes de servicio sean atendidas de acuerdo a los niveles de servicio establecidos. Experiencia en establecimiento de acuerdos de nivel de operación (OLAs) y modelos de operación que permitan el cumplimiento de los niveles de servicio (SLAs) solicitados. Experiencia en la integración eficiente, segura y oportuna de los cambios, mediante la definición y el establecimiento de criterios técnicos y mecanismos para la administración de solicitudes de cambio. Especialista en la integración al ambiente operativo las liberaciones de las soluciones tecnológicas o servicios de TIC y efectuar las pruebas para asegurar que cumplen con los requerimientos técnicos establecidos. El recurso especialista deberá demostrar experiencia de al menos 5 años y contar con al menos una de las siguientes certificaciones: • Operational Support and Analysis (OSA). • Service Offerings & Agreements (SOA).

Especialista en gobierno de seguridad de la información en ASI, OPEC de MAAGTICSI.	Especialista con experiencia en el establecimiento de mecanismos que permitan la administración de la Seguridad de la información, así como disminuir el impacto de eventos adversos, que pueden constituir una amenaza. Especialista con experiencia en el diseño y operación de los controles de seguridad de la información, así como los correspondientes a la capacidad de respuesta a incidentes. El recurso especialista deberá demostrar experiencia de al menos 5 años y contar con al menos una de las siguientes certificaciones: • CISA, emitido por Information Systems Audit and Control Association (ISACA), centro de educación acreditado o equivalente. • ISO/IEC 27001, emitido por Internacional Standard Organization (ISO/IEC), centro de educación acreditado o equivalente.

14 Transferencia de Conocimiento

El Licitante para los servicios ofertados, deberá realizar la transferencia de conocimientos para 5 personas de la solución ofertada sin tener algún costo adicional para la Secretaría, así como entregar el material necesario para la capacitación.

Por lo que deberá de ponerse de acuerdo con la SEMARNAT para programar la fecha una vez concluida la fase de implementación y puesta en operación de los servicios.

Deberá entregar con una semana de anticipación el temario a razón de verificar que consideran todos los servicios solicitados en este anexo técnico.

Posterior de la transferencia de conocimiento el licitante deberá entregar, al administrador del contrato, a más tardar 15 días hábiles posteriores al evento, la o las listas de asistencia y una carta o documento comprobatorio debidamente firmado, de haber llevado a cabo la transferencia de conocimientos con forme a las especiaciones de este anexo técnico.

15 Entregables

La parte de reportes deberán permitir dar a conocer el funcionamiento y situaciones de la operación de los equipos de la solución. El licitante deberá proporcionar mensualmente los reportes solicitados, detallando los eventos más relevantes durante el mes, así como las situaciones más importantes, tendencias en uso y desempeño (alienados a los procedimientos surgidos de MAAGTICSI).

El Reporte mensual estará basado en los requerimientos de análisis de las soluciones de seguridad propuestas y administradas por el licitante.

Los entregables de los servicios durante la vigencia del contrato serán condicionantes para el pago de factura y estos deberán de ser entregados a la Dirección General de Informática y Telecomunicaciones (DGIT). Los entregables de la fase de operación se deberán entregar durante los primeros 5 días hábiles posteriores al mes transcurrido.

Id. Entregable	Apartado del anexo técnico	Nombre del entregable	Tipo	Descripción	Fecha de entrega	Periodicidad
1	Diseño e Implementación	Documento de Planeación y Diseño	Físico y en electrónico	El licitante deberá entregar al administrador del contrato: Plan de trabajo de la fase de Implementación	A más tardar 5 días hábiles después de la reunión inicial de planeación.	1 vez
2	Diseño e Implementación	Documento de Instalación	Físico y en electrónico	El licitante deberá entregar al administrador del contrato; Acta de entrega y recepción del Servicio	A más tardar 5 días después de la entrega e instalación de física de los equipos en las localidades solicitadas.	1 vez
3	Diseño e Implementación	Documento de Configuración	Físico y en electrónico	El licitante deberá entregar al administrador del contrato; Memoria Técnica de la Solución implementada	A más tardar 5 días después de concluida la fase de Diseño e Implementación.	1 vez
4	Diseño e Implementación	Documento de Pruebas y Validación	Físico y en electrónico	El licitante deberá entregar al administrador del contrato: • Protocolo de pruebas avalado por personal de la SEMARNAT. • Oficio de notificación de conclusión de la fase de diseño y planeación e inicio de la fase de transición y estabilización.	Al día siguiente de concluida la fase de Diseño e Implementación.	1 vez
5	Transición y Estabilización	Documento de Afinación y Estabilización	Físico y en electrónico	El licitante deberá entregar al administrador del contrato: • Reporte de hallazgos y recomendaciones implementadas derivadas de la fase de afinación y estabilización • Oficio de notificación de conclusión de la fase de transición y estabilización e inicio de la fase de operación.	Al día siguiente de concluida la fase de transición y estabilización.	1 vez
6	Diseño e Implementación	Procedimientos de Integración para la Mesa de Servicios	Físico y en electrónico	El licitante deberá entregar al administrador del contrato. • Procedimiento de comunicación monitoreo y seguimiento de incidentes entre la mesa de servicios del licitante y la mesa de servicios de SEMARNAT. • Procedimiento de clasificación de incidentes de la mesa de servicios del licitante y el mapeo hacia la Mesa de Servicios de SEMARNAT. • Procedimiento de priorización de la mesa de servicios del licitante y el mapeo hacia la mesa de servicios de SEMARNAT. • Procedimiento de investigación y diagnóstico de la mesa de servicios	5 días posteriores al concluir la fase de Diseño e Implementación	1 vez

				del licitante y el mapeo hacia la mesa de servicios de SEMARNAT. • Procedimiento de resolucion y recuperación (Deberá establecer los códigos de cierre de los incidentes) de la mesa de servicios del licitante y el mapeo hacia la mesa de servicios de SEMARNAT. • Identificacion de formatos para los mesa de servicios de SEMARNAT, requerimientos de servicio de la mesa de servicios del licitante y el mapeo hacia la mesa de servicios de SEMARNAT. • Modelos de atención de requerimientos de la mesa de servicios del licitante y el mapeo hacia la mesa de servicios de SEMARNAT.		
7	Diseño e Implementación	Alineación a normatividad y procesos – ASI	Físico y en electrónico	El licitante debera entregar al administrador del contrato: Entregables de Alineacion a Normatividad y Procesos, para el proceso ASI – Administración de la Seguridad de la Información. • Propuesta de integración del servicio Administrado de Seguridad Perimetral con el Modelo de Gobierno de Seguridad de la Información de SEMARNAT • Procesos, políticas, mecanismos, formatos y documentación relacionada al SGSI de la SEMARNAT con base en la habilitación del Servicio Administrado de Seguridad Perimetral y la normatividad aplicable. • Catálogo de activos de información y infraestructura clave actualizado • Arquitectura de Servicios • Catálogo de activos de información clave o infraestructuras críticas, actualizado. • Análisis de Riesgos actualizado con base en la habilitación del servicio administrado de seguridad perimetral de la SEMARNAT. • Directriz rectora de respuesta a incidentes con base en la la habilitación del servicio administrado de seguridad perimetral de la SEMARNAT. • Hallazgos y recomendaciones al SGSI de la SEMARNAT con base en la habilitacion del servicio	30 días posteriores al iniciar la fase de Operación	1 vez

				administrado de seguridad perimetral de la SEMARNAT.		
8	Diseño e Implementación	Alineación a normatividad y procesos – OPEC	Físico y en electrónico	El licitante deberá entregar al administrador del contrato: • Entregables de Alineación a Normatividad y Procesos, para el proceso OPEC – Operación de los Controles de Seguridad de la Información y del ERISC. • Diseño de los controles de seguridad que habilita el servicio administrado de seguridad perimetral de la SEMARNAT. • Procesos y guías de operación para la atención de incidentes de seguridad perimetral de la SEMARNAT. • Criterios para la identificación de Incidentes de Seguridad perimetral y la interacción con el ERISC de SEMARNAT • Criterios para la categorización de incidentes de seguridad perimetral • Criterios de priorización de incidentes de seguridad perimetral • Criterios para el cierre de incidentes de seguridad perimetral	30 días posteriores al iniciar la fase de Operación	1 vez
9	Operación	Reporte de Operación - Reporte de Incidencias de Seguridad perimetral	Físico y en electrónico	El licitante deberá entregar al administrador del contrato de manera mensual; • Reporte de servicio de control de acceso (top users, top destinos, top servicios, todos en base a número de conexiones y bytes transmitidos/recibidos). • Reporte de servicio de prevención de intrusos (comportamiento general de incidencias, actividades sospechosas, destinos con mayor número de incidencias, tipos de ataques, etc.) • Informe sobre la recomendación de remediación de los hallazgos detectados producto de la gestión de la seguridad contratada. • Reporte de Ataques (IP's públicas) • Reporte de actividades sospechosas • Reporte de recomendaciones del Aseguramiento de Vulnerabilidades basado en los hallazgos encontrados. • Top de conexiones • Top de conversaciones	A más tardar el día 5 posterior al mes transcurrido.	Mensualmente

10	Operación	Reporte de Operación - Reporte Top de Incidentes de Disponibilidad de Servicio	Físico y en electrónico	El licitante deberá entregar al administrador del contrato de manera mensual, • Top ten de ataques de origen y destino. • Vectores y tipo de ataques. • Utilización de tráfico por aplicación protegida.	A más tardar el día 5 posterior al mes transcurrido.	Mensualmente
11	Operación	Reporte de Operación - Reporte de Monitoreo de disponibilidad y utilización de los recursos que habilitan el servicio administrado de seguridad perimetral	Físico y en electrónico	El licitante deberá entregar al administrador del contrato de manera mensual: • Utilización de los recursos (red, CPU, memoria, disco, etc.) • Bitácoras de los diferentes componentes habilitados para proveer los servicios.	A más tardar el día 5 posterior al mes transcurrido.	Mensualmente
12	Operación	Reporte de Operación - Reportes de Gestión de Servicios	Físico y en electrónico	El licitante deberá entregar al administrador del contrato de manera mensual: • Reporte mensual de cambios • Reporte mensual de requerimientos • Reporte mensual de incidentes de servicio • Reporte mensual de Niveles de Servicio	A más tardar el día 5 posterior al mes transcurrido.	Mensualmente
13	Transferencia de conocimientos	Carta o documento comprobatorio de la transferencia de conocimientos	Físico y en electrónico	El licitante deberá entregar al administrador del contrato, a más tardar 45 días hábiles posteriores a la notificación del fallo, la o las listas de asistencia y una carta o documento comprobatorio debidamente firmado, de haber llevado a cabo la transferencia de conocimientos con forme a las especificaciones de este anexo técnico.	A más tardar 45 días hábiles posteriores a la notificación del fallo	1 vez

15 Especificaciones generales de la solución propuesta

El servicio, deberá considerar las siguientes características descritas a continuación:

1. Servicio de Seguridad Perimetral para las Oficinas Centrales de la SEMARNAT.
2. Servicio de Seguridad Perimetral para el Datacenter.
3. Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para la Oficina Central y para el centro de datos (Data Center)

16.1 Seguridad perimetral para Oficina Central de la SEMARNAT

La SEMARNAT requiere del servicio de seguridad informática perimetral, a través de una arquitectura de seguridad en capas que garantice la continuidad y disponibilidad de las aplicaciones críticas del negocio de manera perimetral, proporcionando una tecnología de detección, mitigación y neutralización automática de ataques que busquen consumir los recursos de las aplicaciones críticas, adicionalmente tendrá la función de gestionar y filtrar la totalidad del tráfico entrante y saliente de Internet y de la red interna de LA SECRETARÍA, cubriendo de ataques a través de estos componentes se configuran las políticas de operación para establecer los servicios permitidos en base a puertos lógicos y aplicaciones.

Deberá analizar el tráfico en tiempo real y alta velocidad, así como incluir las siguientes características mínimas necesarias:

- El servicio deberá contar con dispositivos basados en Appliance de propósito específico los cuales deberán contar con sistema operativo propietario con un hardening comprobable, el mismo que debe ser desarrollado íntegramente por el fabricante de los dispositivos utilizados. Adicionalmente por la alta criticidad del nodo se deberá contar con Fuentes de poder redundantes Hot-Swap, así como almacenamiento, firmware o BIOS redundantes.
- El servicio deberá contar con una arquitectura de Clustering basada en el esquema de alta disponibilidad Activo/Activo o Activo/Pasivo, el licitante en conjunto con la INSTITUCIÓN definirá la mejor opción de acuerdo con las necesidades de la dependencia.
- El servicio deberá considerar al menos de 10Gbps Throughput para el servicio de Firewall, 10Gbps de Throughput para el servicio de IPS y 10 Gbps de Throughput para el servicio de VPN.
- El servicio deberá brindar soporte al menos 10,000,000 de sesiones concurrentes y al menos 185,000 conexiones por segundo.
- El servicio deberá contar con al menos 1 Puerto 10/100/1000 dedicado para administración remota, al menos 8 puertos 10/100/1000 Ethernet en cobre y al menos 2 puertos de 10Gbps para la distribución de zonas según lo requiera la Secretaría.
- El servicio deberá contar con el licenciamiento necesario para las funcionalidades de Firewall IPS, Prevención y Eliminación o Extracción de Amenazas Conocidas, así como ataques de Día Cero.

16.1.1 Firewall

- La solución deberá contar con un Motor de Next Generation Firewall con la certificación "Recommended" por parte de NSS Labs en las pruebas de 2016.
- Deberá tener la capacidad de analizar todas las conexiones que crucen el equipo, entre interfaces, grupos de interfaces o bien Zonas y VLANs.
- Deberá tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación

que se está analizando, así como los puertos TCP/UDP de servicios asociados, para al menos brindar la capacidad de aceptar, bloquear o rechazar la comunicación, teniendo capacidad de establecer limitantes y/o vigencia para mantener los controles de seguridad 100% del tiempo.

- Deberá de brindar la capacidad de hacer traducción de direcciones estáticas, uno a uno, NAT (Network Address Translation) y hacer PAT (Port Address Translation)
- Deberá incluir la capacidad de definir nuevos servicios TCP/UDP que no estén contemplados en los predefinidos, de igual forma poder definir el tiempo de vida para la expiración de una sesión inactiva de forma independiente por puerto y protocolo (TCP /UDP).
- Se requiere contar con el servicio de Sandboxing que permita analizar código malicioso desconocido o software de terceros de dudosa confiabilidad que le permita emular el comportamiento de archivos o ejecutables que puedan ser susceptibles a ser clasificados como ataques de día cero.
- Deberá contar con la capacidad de soportar etiquetas de VLAN (802.1q) para crear subinterfaces VLAN interfaces asociadas a dichas etiquetas y soporte a LCAP (802.3ad).
- Deberá contar soportar ruteo estático con capacidad de brindar políticas que permitan ante la presencia de dos enlaces a Internet, se pueda decidir cuál tráfico sale por un enlace y cual qué tráfico sale por otro enlace (Ruteo por política) además se deberá contar con la capacidad de Ruteo dinámico y/o Ruteo Multicast.
- Deberá contar con capacidad de colectar flujos UDP acorde a cualquiera de los siguientes estándares: Netflow, Jflow, NetStream, Cflowd, Rflow, AppFlow, para exportar hacia un colector externo para la captura, análisis de patrones y volumetría de tráfico.
- Deberá contar con la capacidad de acceso de puertos USB para simplificar la implementación de la infraestructura de Next Generation Firewall y los procesos de RMA para cambio de equipo dañado permitiendo así la simplificación de la recuperación de los servicios de la INSTITUCIÓN
- Deberá brindar un mecanismo de protección a fallas en los dispositivos de la infraestructura de Next Generation Firewall y Prevención de amenazas que permita de forma remota actualizar, administrar y/o monitorear el equipamiento en forma independiente de la interface de administración.
- Las comunicaciones entre la consola de administración y los dispositivos administrados deberán ser cifradas (Encriptadas), esto al considerarse equipos perimetrales altamente críticos
- A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptaran componentes de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE alimentadas por el NIST) que no hayan sido remediadas oportunamente en un plazo no mayor a 12 días naturales.

16.1.2 IPS y Prevención de Amenazas

- Deberá contar con un módulo de IPS con inspección profunda que se encuentre integrada con el motor del Firewall contando con los siguientes mecanismos de detección: Firmas contra exploits, anomalías de protocolo, control de aplicaciones y detección basada en comportamientos.
- Deberá contar el módulo de IPS con una eficiencia comprobada de un mínimo de 98% de eficiencia por parte NSS Labs de acuerdo a las pruebas de Next Generation Intrusion Prevention System de 2016.
- Deberá contar con una eficiencia de 99% contra exploits de malware, además de brindar una tasa de detección 100% de Amenazas Avanzadas Persistentes (APTs), mediante malware HTTP – SMTP, cifrado SSL e infecciones fuera de línea; soportado por las últimas pruebas realizadas de NSS Labs sobre Breach Detection System.
- Deberá de inspeccionar la presencia de malware a nivel de archivos que utilicen los siguientes protocolos de aplicación: http, SMTP, IMAP, POP3, FTP, SMB.
- Deberá comprobar su capacidad de prevención de amenazas brindando una eficiencia de al menos 95% para fabricantes como Adobe, Apple, IBM, Microsoft y Oracle.
- Deberá contar con las opciones de crear políticas para activar protecciones basadas ya sea para clientes y servidores o bien una combinación de ambos.
- Deberá contar con la capacidad de contar dos Perfiles o políticas Out-of-the-box que puedan ser usados en forma inmediata y que estas puedan ser personalizables.
- Deberá contar con un mecanismo automatizado de activar nuevas firmas desde las actualizaciones frecuentes del módulo de IPS.
- Deberá soportar excepciones de Red basado en fuente, destino, servicios o una combinación de los tres.
- Deberá ser capaz de hacer recomendaciones de afinación (tunning) de reglas de prevención en base a la información aprendida de la red.
- Deberá ser capaz el módulo de IPS de detectar y prevenir las siguientes amenazas: Protocol misuse, comunicaciones de malware, intentos da tunneling attempts y ataques genéricos sin requerir de firmas predefinidas
- Deberá identificar vulnerabilidades de los hosts de la red en tiempo real, sin necesidad de correr un análisis de vulnerabilidades

- Deberá permitir las protecciones del Módulo de IPS incluir una descripción del tipo de situaciones que se está detectando, dando información detallada sobre el tipo de amenaza, además de referencias como por ejemplo la CVE para obtener más información externa.
- Deberá permitir para la capacidad de capturar tráfico de protecciones específicas para análisis forense.
- Deberá permitir proteger la infraestructura DNS de la INSTITUCIÓN contra ataques maliciosos y DNS Cache Poisoning.
- Deberá permitir la configuración de las políticas en forma centralizada de los módulos del IPS
- Deberá contar con la capacidad de detectar y detener comportamientos anormales y sospechosos de la red de la INSTITUCIÓN
- Deberá contar detecciones de malware, spyware y adware.
- Deberá contar con la capacidad de inspeccionar tráfico encriptado sobre SSL.
- Deberá tener la capacidad de actualizaciones en tiempo real por medio de servicios de inteligencia de Seguridad cooperativa y en tiempo real, donde pueda ser integrada con diferentes fuentes enfocadas a protección de infraestructuras de la INSTITUCION.
- Deberá contar con la capacidad de detener la descarga de archivos maliciosos.
- Deberán los módulos de IPS poder contar con una correlación y reportes en forma centralizada en la consola de administración de propósito específico.
- Deberán los Módulos de IPS permitir bloquear en una forma sencilla tanto el tráfico de entrada como de salida.

16.1.3 VPN.

- Deberá brindar túneles IPSec que soporten algoritmos de cifrado AES con la capacidad de configurar longitudes de llave de 128 o 256 bits, permitiendo configurar al menos los grupos de Diffie-Hellman 1, 2, 5, 14 junto con la capacidad de configurar los siguientes algoritmos de integridad: MD5, SHA, SHA-1 y SHA256.
- Deberá brindar soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to- site) y soporte para IKEv2 y IKE main y agressive mode
- De manera opcional deberá poder ser configurada en modo interface, donde en esta funcionalidad deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interfaz.

16.2 Seguridad perimetral para el Data Center (Centro de Datos)

La SEMARNAT requiere de la seguridad informática perimetral, a través de una arquitectura de seguridad en capas que garantice la continuidad y disponibilidad de las aplicaciones críticas del negocio de manera perimetral, proporcionando una tecnología de detección, mitigación y neutralización automática de ataques que busquen consumir los recursos de las aplicaciones críticas, así como mecanismos que le permitan gestionar y filtrar la totalidad del tráfico entrante y saliente de Internet y de la red interna de la SECRETARÍA en el Data Center, a través de estos componentes se configurarán políticas de operación para establecer los servicios permitidos en los aplicativos y sus bases de datos, en base a puertos lógicos y aplicaciones, además, se realizará la configuración de las áreas denominadas Zonas Desmilitarizadas (DMZ) para la protección de servicios que requieran publicación a internet por parte de la SEMARNAT.

Deberá analizar el tráfico en tiempo real y alta velocidad, así como incluir las siguientes características mínimas necesarias:

- El servicio deberá contar con dispositivos basados en Appliance de propósito específico los cuales deberán contar con sistema operativo propietario con un hardening comprobable, el mismo que debe ser desarrollado íntegramente por el fabricante de los dispositivos utilizados. Adicionalmente por la alta criticidad del nodo se deberá contar con Fuentes de poder redundantes Hot-Swap, así como almacenamiento, firmware o BIOS redundantes.
- El servicio deberá contar con una arquitectura de Clustering basada en el esquema de alta disponibilidad Activo/Activo o Activo/Pasivo, el licitante en conjunto con la INSTITUCIÓN definirá la mejor opción de acuerdo con las necesidades de la dependencia.
- El servicio deberá considerar al menos de 10Gbps Throughput para el servicio de Firewall, 10Gbps de Throughput para el servicio de IPS y 10 Gbps de Throughput para el servicio de VPN.
- El servicio deberá brindar soporte al menos 10,000,000 sesiones concurrentes y 185,000 Conexiones por segundo.
- El servicio deberá contar con al menos 1 Puerto 10/100/1000 dedicado para administración remota, al menos 8 puertos 10/100/1000 Ethernet en cobre y al menos 2 puertos de 10Gbps para la distribución de zonas según lo requiera la Secretaría.
- El servicio deberá contar con el licenciamiento necesario para las funcionalidades de Firewall IPS, Prevención y Eliminación o Extracción de Amenazas Conocidas, así como ataques de Día Cero.

16.2.1 Firewall

- La solución deberá contar con un Motor de Next Generation Firewall con la certificación "Recommended" por parte de NSS Labs en las pruebas de 2016.
- Deberá tener la capacidad de analizar todas las conexiones que crucen el equipo, entre interfaces, grupos de interfaces o bien Zonas y VLANs.

- Deberá tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando, así como los puertos TCP/UDP de servicios asociados, para al menos brindar la capacidad de aceptar, bloquear o rechazar la comunicación, teniendo capacidad de establecer limitantes y/o vigencia para mantener los controles de seguridad 100% del tiempo
- Deberá de brindar la capacidad de hacer traducción de direcciones estáticas, uno a uno, NAT (Network Address Translation) y hacer PAT (Port Address Translation)
- Deberá incluir la capacidad de definir nuevos servicios TCP/UDP que no estén contemplados en los predefinidos, de igual forma poder definir el tiempo de vida para la expiración de una sesión inactiva de forma independiente por puerto y protocolo (TCP /UDP).
- Se requiere contar con el servicio de Sandboxing que permita analizar código malicioso desconocido o software de terceros de dudosa confiabilidad que le permita emular el comportamiento de archivos o ejecutables que puedan ser susceptibles a ser clasificados como ataques de día cero.
- Deberá contar con la capacidad de soportar etiquetas de VLAN (802.1q) para crear subinterfaces VLAN interfaces asociadas a dichas etiquetas y soporte a LCAP (802.3ad).
- Deberá contar soportar ruteo estático con capacidad de brindar políticas que permitan ante la presencia de dos enlaces a Internet, se pueda decidir cuál tráfico sale por un enlace y cual què tráfico sale por otro enlace (Ruteo por política) además se deberá contar con la capacidad de Ruteo dinámico y/o Ruteo Multicast.
- Deberá contar con capacidad de colectar flujos UDP acorde a cualquiera de los siguientes estándares: Netflow, Jflow, NetStream, Cflowd, Rflow, AppFlow, para exportar hacia un colector externo para la captura, análisis de patrones y volumetría de tráfico.
- Deberá contar con la capacidad de acceso de puertos USB para simplificar la implementación de la infraestructura de Next Generation Firewall y los procesos de RMA para cambio de equipo dañado permitiendo así la simplificación de la recuperación de los servicios de la INSTITUCIÓN
- Deberá brindar un mecanismo de pròtección a fallas en los dispositivos de la Infraestructura de Next Generation Firewall y Prevención de amenazas que permita de forma remota actualizar, administrar y/o monitorear el equipamiento en forma independiente de la interface de administración.
- Las comunicaciones entre la consola de administración y los dispositivos administrados deberán ser cifradas (Encriptadas), esto al considerarse equipos perimetrales altamente críticos.
- A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptaran componentes de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE

alimentadas por el NIST) que no hayan sido remediadas oportunamente en un plazo no mayor a 12 días naturales.

16.2.2 *IPS y Prevención de Amenazas*

- Deberá contar con un módulo de IPS con inspección profunda que se encuentre integrada con el motor del Firewall contando con los siguientes mecanismos de detección: Firmas contra exploits, anomalías de protocolo, control de aplicaciones y detección basada en comportamientos.
- Deberá contar el módulo de IPS con una eficiencia comprobada de un mínimo de 98% de eficiencia por parte NSS Labs de acuerdo a las pruebas de Next Generation Intrusion Prevention System de 2016.
- Deberá contar con una eficiencia de 99% contra exploits de malware, además de brindar una tasa de detección 100% de Amenazas Avanzadas Persistentes (APTs), mediante malware HTTP – SMTP, cifrado SSL e infecciones fuera de línea; soportado por las últimas pruebas realizadas de NSS Labs sobre Breach Detection System.
- Deberá de inspeccionar la presencia de malware a nivel de archivos que utilicen los siguientes protocolos de aplicación: http, SMTP, IMAP, POP3, FTP, SMB.
- Deberá comprobar su capacidad de prevención de amenazas brindando una eficiencia de al menos 95% para fabricantes como Adobe, Apple, IBM, Microsoft y Oracle.
- Deberá contar con las opciones de crear políticas para activar protecciones basadas ya sea para clientes y servidores o bien una combinación de ambos.
- Deberá contar con la capacidad de contar dos Perfiles o políticas Out-of-the-box que puedan ser usados en forma inmediata y que estas puedan ser personalizables.
- Deberá contar con un mecanismo automatizado de activar nuevas firmas desde las actualizaciones frecuentes del módulo de IPS.
- Deberá soportar excepciones de Red basado en fuente, destino, servicios o una combinación de los tres.
- Deberá ser capaz de hacer recomendaciones de afinación (tunning) de reglas de prevención en base a la información aprendida de la red.
- Deberá ser capaz el módulo de IPS de detectar y prevenir las siguientes amenazas: Protocol misuse, comunicaciones de malware, intentos de tunneling attempts y ataques genéricos sin requerir de firmas predefinidas

- Deberá permitir las protecciones del Módulo de IPS incluir una descripción del tipo de situaciones que se está detectando, dando información detallada sobre el tipo de amenaza, además de referencias como por ejemplo la CVE para obtener más información externa.
- Deberá permitir para la capacidad de capturar tráfico de protecciones específicas para análisis forense.
- Deberá permitir proteger la infraestructura DNS de la INSTITUCIÓN contra ataques maliciosos y DNS Cache Poisoning.
- Deberá permitir la configuración de las políticas en forma centralizada de los módulos del IPS
- Deberá contar con la capacidad de detectar y detener comportamientos anormales y sospechosos de la red de la INSTITUCIÓN
- Deberá contar detecciones de malware, spyware y adware.
- Deberá contar con la capacidad de inspeccionar tráfico encriptado sobre SSL.
- Deberá tener la capacidad de actualizaciones en tiempo real por medio de servicios de inteligencia de Seguridad cooperativa y en tiempo real, donde pueda ser integrada con diferentes fuentes enfocadas a protección de infraestructuras de la INSTITUCION.
- Deberá contar con la capacidad de detener la descarga de archivos maliciosos.
- Deberán poder contar con una correlación y reportes en forma centralizada en la consola de administración de propósito específico.
- Deberán los Módulos de IPS permitir bloquear en una forma sencilla tanto el tráfico de entrada como de salida.

16.2.3 VPN.

- Deberá brindar túneles IPSec que soporten algoritmos de cifrado AES con la capacidad de configurar longitudes de llave de 128 o 256 bits, permitiendo configurar al menos los grupos de Diffie-Hellman 1, 2, 5, 14 junto con la capacidad de configurar los siguientes algoritmos de integridad: MD5, SHA, SHA-1 y SHA256. Deseablemente, para el uso de túneles por medio de SSL (Secure Sockets Layer) versión 3, con al menos los siguientes algoritmos de cifrado simétrico y longitud de llaves: AES (128bits y 192bits)
- Deberá brindar soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to- site) y soporte para IKEv2 y IKE main y agressive mode
- De manera opcional deberá poder ser configurada en modo interface, donde en esta funcionalidad deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interfaz.

16.3 Consola de Administración

La infraestructura de protección perimetral deberá incluir una consola de administración centralizado que realice aprovisionamiento de las políticas de seguridad, configuración de dispositivos, gestión de actualizaciones, monitoreo y control de los mismos.

Especificaciones para la consola de Administración y Reportes:

1. Deberá ser un software para el manejo, administración de la seguridad, reportes de la Infraestructura de Next Generation Firewall y prevención de Amenazas.
2. Deberá estar basada en software, compatible para su instalación en ambientes virtualizados o servidores dedicados, mediante el cual se lleva a cabo la administración de la seguridad y reporteo de la infraestructura de los Next Generation Firewalls, de la solución perimetral, y centro de datos. Deberá centralizar la configuración y monitoreo de los dispositivos de seguridad, así como todas sus funciones de protección de red.
3. Deberá ser capaz de crear un perfil de tráfico de la red para crear baselines del tráfico existente en la red.
4. Deberá contar con la capacidad de creación, almacenamiento e implementación automatizada de configuraciones de dispositivos bajo un solo repositorio de almacenamiento centralizado y administración de configuraciones.
5. Deberá contar con la capacidad de administrar el software de la infraestructura de Next Generation Firewall y Prevención de Amenazas, permitiendo programar y aplicar actualizaciones de sistema operativo de forma automática a un equipo o grupo de equipos administrados por la consola.
6. Las comunicaciones entre la consola de administración y los dispositivos administrados deberán ser cifradas por medio de una GUI. Se podrán ofertar soluciones que usen WebUI sobre HTTPS debido a las vulnerabilidades reportadas de Cross-site-scripting (XSS), de diversos fabricantes que pueden poner en riesgo la seguridad de la Secretaría.
7. La administración deberá ser basada en roles para permitir a los administradores delegar los derechos de acceso a dispositivos específicos con los privilegios adecuados de lectura/escritura.
8. La consola de administración deberá permitir la automatización de tareas operativas, cuya implementación pueda ser de forma masiva y/o a larga escala con tiempos de aplicación mínimos a los dispositivos y/o permitiendo que los procesos de administración puedan ser automáticos.
9. Deberá contar con la capacidad de realizar respaldos calendarizados de la configuración y las bitácoras, realizando operaciones sobre grupos de dispositivos, permitiendo el hospedaje local de actualizaciones.

10. Deberá contar con la capacidad de crear, exportar y almacenar versiones de configuración de los dispositivos administrados, de manera automatizada, antes de aplicar cambios a un dispositivo.
11. Deberá incluir un componente de Monitoreo en Tiempo-Real que permita a la consola de administración obtener el estado actual de la infraestructura de dispositivos administrados, y permitir actuar proactivamente a un evento de seguridad y operación de los dispositivos de seguridad administrados.
12. Deberá contar con una herramienta de búsqueda que permita fácilmente filtrar objetos de red, donde permita incluir la opción de buscar objetos duplicados (con la misma IP) y objetos no usados (en una regla o política) y una lista de reglas en que un objeto específico es usado para una simplificación de las operaciones.
13. Deberá soportar distintos tipos de filtros para la personalización de los reportes y que puedan ser estos referenciables (ej. Origen, destino, nombre del ataque, número de regla)
14. El sistema de administración centralizada debe soportar la integración de productos de análisis de vulnerabilidades.
15. Las alertas deben poder ser agrupadas de acuerdo a información de campos comunes.
16. A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptarán componentes de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE alimentadas por el NIST) que no hayan sido remediadas oportunamente en un plazo no mayor a 12 días naturales.

16.4 ***Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) y para el Centro de Datos***

La Secretaría requiere una solución que garantice la continuidad y disponibilidad de las aplicaciones críticas del negocio de manera perimetral, que proporcione una tecnología de detección, mitigación y neutralización automática de ataques de ancho de banda reducido antes de que afecten los servicios críticos de la SEMARNAT, el licitante deberá proporcionar un sistema de protección en el perímetro, con un equipo por sitio.

La solución deberá contar y operar al menos con las siguientes características:

1. Deberá ser un appliance de propósito específico dedicado a proporcionar disponibilidad (detección y mitigación ante ataques de DDoS/DoS); la solución deberá ser 100% enfocada a la prevención de ataques de negación de servicio o que no mantengan el estado de la conexión, tales como cortafuegos, sistemas de prevención de intrusiones, balanceadores de carga, sistemas de detección de anomalías

basados en tasas de tráfico y las variantes o combinaciones como UTM, NGFW, NGIPS, NBA, etcétera, ya que al conservar el estado de la conexión son por sí mismos susceptibles a DDoS (ataques de exhaustación).

2. La solución deber incluir plantillas de políticas pre-configuradas para mitigar amenazas de disponibilidad de servicios.
3. Contar los recursos suficientes para cubrir los parámetros óptimos de operación.
4. Permitir la creación de políticas de seguridad, por aplicación, protocolo o direccionamiento IP.

16.4.1 Capacidad y Rendimiento

1. La solución propuesta deberá tener por lo menos 5 interfaces 10/100/0/1000 Ethernet, una para la administración y las otras 4 para protección de hasta dos enlaces de Internet.
2. La solución propuesta deberá tener un puerto de consola y un puerto auxiliar mediante una interfaz RJ 45 o USB.
3. El equipo deberá de tener embebido el bypass físico interno en pares de interfaces y/o en cada interface para garantizar la disponibilidad y continuidad de los servicios activándose en los siguientes casos:
   - Pérdida de energía eléctrica y/o
   - Falla lógica en la interface de control y/o
   - Pérdida de conectividad con la tarjeta madre del dispositivo y/o
   - Colapso del sistema operativo.
4. La solución propuesta deberá contar con fuente de alimentación redundante del tipo AC.
5. El equipo deberá ser capaz de soportar un modo de prueba "inactivo" o "monitoreo" cuando se configura en línea, que permita el ajuste de la configuración de protección sin bloquear el tráfico y proporcione reportes de todo el tráfico que bloquearía si se define como "activo".
6. El equipo de seguridad deberá venir respaldado con investigación y análisis global del tráfico, para poder mitigar las amenazas y vectores de ataque actuales. Por lo que el fabricante de la solución deberá contar con algún sistema de inteligencia donde se esté monitoreando las amenazas de Internet a nivel mundial y podrá proporcionar información sobre:
   - Botnets oDDoS
   - Scans
   - Phishing
7. El equipo deberá contar con los siguientes modos de operación:
   - En línea (con o sin medidas de protección habilitadas)
   - fuera de Línea (a través de un puerto span o tap' de red, sin medidas de protección)

8. La solución propuesta deberá contar con bloqueo de tráfico malformado DNS, SIP y HTTP, Detección de fragmentación de paquetes e inundación de ICMP, Detección de inundación UDP, soporte TLS, Detección de inundación TCP SYN y/o SYN suplantados, reseteo de conexiones TCP, límite de conexiones TCP, bloqueo de tráfico basado en umbrales, prevención de botnets y filtrado mediante listas para inspeccionar y bloquear tanto tráfico entrante como saliente.
9. La solución deberá detectar direcciones IP o dominios orígenes que envíen cantidades excesivas de tráfico bajo umbrales configurables, para después colocar esas fuentes en listas de hosts bloqueados temporalmente (bloqueo basado en la tasa de tráfico).
10. La solución deberá Descartar paquetes según puertos TCP o UDP específicos y payloads que coincidan o no con expresiones regulares configurables.
11. La solución debe de incorporar medidas de protección específicas para el protocolo DNS tales como Autenticación y malformación de paquetes.
12. La solución deberá detectar y eliminar paquetes con formatos incorrectos de HTTP que no se ajusten a los RFC's para los encabezados de solicitud y poner al host origen en una lista negra.
13. La solución debe de contar con un módulo de análisis y captura de paquetes.
14. La solución debe de detener ataques conocidos de tipo aplicativo mediante la coincidencia de patrones a través actualización de firmas.
15. El sistema deberá de poder bloquear tráfico Multicast
16. El sistema deberá soportar TLS
17. El sistema podrá de identificar web crawlers y monitorear su uso
18. La solución deberá realizar la detección y protección de ataques de Red como:
    - Ataques DDoS sobre la capa aplicativa
    - Ataques de exhaustación.
    - Ataques volumétricos.
19. El sistema deberá estar preparado para interactuar con el Licitante de Servicios de Internet de la Secretaría.
20. La solución de mitigación de DDoS del lado del CPE (perímetro/datacenter/contenedor) deberá de ser gestionada a través de una GUI de administración que permita a la dependencia detectar rápidamente la presencia de actividad maliciosa.
21. La solución deberá permitir la administración:
    - Por interfaz gráfica, o utilizando la interfaz de línea de comandos; SSH.
22. La solución deberá permitir definir diferentes niveles de usuario de administración.

23. La solución deberá contar con la capacidad de enviar eventos hacia la Consola de Administración de los dispositivos Perimetrales y DataCenter para poder correlacionar eventos.
24. La solución deberá permitir enviar notificaciones de alertas del sistema a los administradores de red vía e-mail.
25. La solución deberá proporcionar un panel de estado de dispositivo que incluya información sobre las alertas activas, todas las protecciones aplicadas al tráfico, total del tráfico permitido y bloqueado a través de las interfaces, estado del CPU y memoria de sistema.
26. El sistema debe mostrar estadísticas de protección en tiempo real sobre tráfico permitido y bloqueado en bytes y paquetes, con estadísticas en bps y pps.
27. La solución deberá mostrar una lista de protecciones activas en conjunto con estadísticas resumidas de la cantidad de tráfico permitido y bloqueado para cada grupo de protección configurado.
28. La solución deberá soportar el protocolo SNMP más actual para el monitoreo de los mismos.
29. La solución debe de ser capaz de generar reportes en formato PDF o CSV.
30. A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptaran componentes de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE alimentadas por el NIST) que no hayan sido remediadas oportunamente en un plazo no mayor a 12 días naturales.

16.5 Mesa de Servicios

El licitante deberá contar con una Mesa de Servicios preferentemente certificada en el estándar ISO/IEC 20000 y disponible en un esquema 7x24x365 con capacidad de recepción, atención y seguimiento de eventos de manera telefónica, por correo electrónico y en herramienta web, mediante una metodología de Punto Único de Contacto.

La herramienta que habilite a la Mesa de Ayuda del licitante, podrá estar alineada y preferentemente certificada en el cumplimiento de la totalidad en los procesos de Operación del Servicio especificados en ITIL v3.

Se deberá entregar un reporte mensual obtenido de los registros de la herramienta donde se resuma el comportamiento de al menos los siguientes rubros:

1. Incidentes
2. Problemas

3. Solicitudes de servicio
4. Resumen general e histórico acumulado de los tickets
5. Tiempo de atención de los tickets
6. Tiempo de solución de los tickets

17 **Lugar, tiempo y Control de entrega de los Servicios.**

Para Seguridad Perimetral:

1. Los servicios de implementación y configuración deberán ser prestados por personal certificado por el fabricante de la infraestructura solicitada.
2. 4 semanas máximo para el tuneo e instalación de la seguridad perimetral.
3. Entrega de los servicios para la solución propuesta:
4. Para la Oficina Central de la SEMARNAT:
   - El lugar de entrega de los servicios, estará ubicado en el MDF de la Oficina Central con domicilio en Ejército Nacional 223, Planta Baja, Col. Anáhuac, C.P.11320, Delegación Miguel Hidalgo; o donde la SEMARNAT defina.
5. Para el DataCenter (Centro de Datos):
   - El lugar de entrega de los servicios, estará ubicado en las instalaciones de CONAGUA con domicilio en Av. Insurgente Sur Col. Copilco el Bajo, Delegación Coyoacán, C.P. 04340 o donde la SEMARNAT defina.
6. En caso de que la SEMARNAT requiera de alguna reubicación de domicilio y configuración del equipamiento solicitado en este anexo técnico, deberá notificarse al menos con una semana de anticipación al licitante del presente contrato, el cual no deberá representar un costo para para la Secretaría en la instalación y puesta en operación del mismo, el licitante no deberá de excederse de un plazo de más de 10 días naturales.
7. Para el correcto control para la prestación de los servicios el licitante deberá proporcionar una herramienta web para el Control y Gestión de los Servicios que se prestarán por un ingeniero de campo en las diversas localidades definidas por la SEMARNAT sin costo adicional para la convocante, esta herramienta deberá estar disponible las 24 hrs del día los 365 días del año con un nivel de servicio del 99%. Esta herramienta web ayudará a la (Dirección General de Informática y Telecomunicaciones (DGIT,) a controlar y administrar de una forma fácil y sencilla las órdenes de servicio solicitadas, deberá permitir al menos lo siguiente:

- El control por localización geográfica de llegadas y salidas de los ingenieros de campo
- El seguimiento de actividades asignadas, pendientes, programadas, terminadas o canceladas mediante un dashboard de información ejecutivo en tiempo real, accesado mediante web.

Esta herramienta web deberá contar al menos con las siguientes funcionalidades:

- Administración y carga de información en tiempo real de los servicios a ejecutar
- Despachar y agendar las órdenes de servicio individualmente a los ingenieros de servicio asignados, basándose en su especialidad, confiabilidad y disponibilidad.
- Monitorear por localización geográfica en línea, la operación en campo de los servicios que se están llevando a cabo.
- Permitir tomar acción inmediata para corregir desviaciones o notificar al cliente.
- Reportar en línea el seguimiento del estatus y avance de cada uno de los servicios que están en ejecución.
- Permitir identificar desviaciones en los servicios y tomar acciones correctivas inmediatas
- Para el control de los ingenieros de campo deberá contar con una aplicación accesible mediante cualquier dispositivo móvil tipo Smartphone (IOS, Windows, Android) mediante la cual se consultará el detalle del servicio a realizar y las actividades necesarias, realizar los informes de la llegada del personal al sitio, y la conclusión de cada actividad, y la notificación de observaciones y finalización del servicio en tiempo real.
- Toda la información de la aplicación deberá incluir la localización geográfica, fecha y hora de ejecución en tiempo real.

Los equipos ofertados para el servicio, deberán ser nuevos de una sola marca, una vez adjudicado, el proveedor deberá entregar copias de las facturas de los equipos instalados.

18 Cronograma de Trabajo

Para la contratación de este servicio, la SEMARNAT, requiere de lo siguiente:

El servicio requerido es a partir del día siguiente de la notificación del fallo y hasta el 31 de diciembre de 2017.

El Plan de trabajo estimado para la entrega del servicio es el siguiente:

2017									
Mes	JUL				AGO	SEP	OCT	NOV	DIC
Actividades	S1	S2	S3	S4					
Diseño e Implementación									
Transición y Estabilización									
Operación									
Mesa de Servicio									
Transferencia de Conocimiento									

19 Vigencia

El periodo del servicio será a partir del día siguiente de la notificación del fallo y hasta el 31 de diciembre de 2017

20 Normas aplicables para la prestación del Servicio

No Aplica

21 Pruebas para la contratación del Servicio

No aplica

22 Garantías

22.1 Garantía de Cumplimiento del Contrato

A fin de garantizar el debido cumplimiento de las obligaciones derivadas del contrato en los términos señalados en el contrato, el proveedor deberá entregar dentro de los diez días naturales siguientes a la firmas del contrato, fianza indivisible expedida por una institución legalmente autorizada para ello a favor de la Tesorería de la Federación, en el formato autorizado por ésta Institución, por una cantidad equivalente al 10% del monto máximo del contrato antes del IVA, la cual deberá de mantener vigente hasta la terminación de la vigencia del contrato y en su caso convenio modificatorio.

La fianza deberá ser entregada en la Dirección de Adquisiciones y Contrataciones de "SEMARNAT", sita en Ejército Nacional 223, Col. Anáhuac, Delegación Miguel Hidalgo, C.P. 11320, México, D.F. piso 17, Ala Norte.

23 Póliza de Responsabilidad Civil.

El Prestador del servicio, deberá mantener durante la vigencia del contrato un seguro de responsabilidad civil, contratado con la empresa aseguradora legalmente autorizada, y entregar endoso de la póliza de responsabilidad civil del licitante que ampare una cantidad equivalente al 10% (diez por ciento) del monto máximo del contrato a favor de la convocante por una compañía aseguradora debidamente autorizada, sin incluir el impuesto al valor agregado (IVA), a efecto de garantizar el pago de indemnización hasta por dicha cantidad, por los daños que se puedan ocasionar a los bienes muebles e inmuebles propiedad de la SEMARNAT a sus empleados o a terceras personas, o de cualquier causa imputable al prestador del servicio o a su personal.

El Prestador del servicio será responsable de la relación laboral de su personal, que esté involucrado en la prestación de los servicios objeto de la presente licitación, liberando de cualquier responsabilidad a la SEMARNAT.

Si ante cualquier evento o siniestro, esta cobertura resulta insuficiente, los gastos que queden sin cubrir serán por cuenta directamente de "EL PRESTADOR DEL SERVICIO".

En caso de que se presente un evento o siniestro y se dictamine la responsabilidad de "EL PRESTADOR DEL SERVICIO", éste tendrá un plazo máximo de 5 (cinco) días hábiles, para realizar los pagos de los daños directamente a la Institución afectada y/o terceros implicados; o iniciar las gestiones correspondientes ante la aseguradora que corresponda, para que haga los pagos inmediatamente a dicha institución.

"EL PRESTADOR DEL SERVICIO" queda obligado a mantener vigente la póliza de seguro de responsabilidad civil mencionada, en tanto permanezca en vigor el contrato, y durante la substanciación de todos los recursos legales o juicios que se interpongan, hasta que se dicte resolución definitiva por autoridad competente.

En caso de que la SEMARNAT decida prorrogar el plazo por la prestación de los servicios, "EL PRESTADOR DEL SERVICIO" se obliga a presentar una póliza de seguro de responsabilidad civil en los mismos términos señalados y por el periodo prorrogado.

24 Deducciones, Penalizaciones y Causales de Rescisión

24.1 *Penas convencionales.*

La aplicación de las penas convencionales para este servicio, será del 1% diario sobre el importe de los servicios no prestados de acuerdo a la especificación de la fecha y hora de cumplimiento especifica en este anexo técnico.

- Tabla 1. Penas convencionales a aplicar a cada entregable

Numeral del Anexo Técnico	ID	Descripción	Pena Convencional
17 Punto 2	1	Entrega del equipamiento para seguridad perimetral	1% del monto total del servicio mensual por cada día natural de atraso en la instalación de los equipos.
17 Punto 2	2	Instalación y configuración de equipamiento para seguridad perimetral	1% del monto total del servicio mensual por cada día natural de atraso en la instalación de los equipos.

Numeral del Anexo Técnico	ID	Descripción	Pena Convencional
10 Punto 10	3	Atraso en la entrega de la memoria técnica (especificado en los entregables) si se excede al plazo mayor de 15 días hábiles.	1% del monto total de la factura por cada día natural de atraso en la instalación de los equipos.
15	4	El proveedor no haga entrega de cada uno de los entregables en el plazo establecido	1% del monto total de la factura por cada día natural de atraso en los entregables.

24.2 *Deducciones.*

La aplicación de las deducciones, será del 1% por cada día natural sobre el importe de los servicios prestados en forma parcial o deficientemente.

Las deducciones se aplicarán en la facturación próxima posterior a la fecha en que se haya generado dicha deductiva.

La SEMARNAT considerará como deductiva al menos lo siguiente:

Numeral del Anexo Técnico	Obligación	Cálculo para la aplicación de la deducción		Tipo de falta por evento	Límite de eventos permitidos
		% deducción a aplicarse	Aplicación		
15	Si los entregables mensuales de MAAGTICSI no son entregados en su totalidad y no cumplan con lo requerido en el servicio	1% (Uno por ciento)	Calculado sobre sobre el importe de los servicios prestados en forma parcial o deficientemente.	Baja	Hasta 3 ocasiones en la falta de entrega durante el mismo mes calendario para esta deductiva.
11.3	Incidentes con afectación de severidad 1	1% (Uno por ciento)		Baja	Hasta 3 ocasiones en la falta de entrega durante la vigencia del servicio.
11.3	Incidentes con afectación de severidad 2	1% (Uno por ciento)		Media	Hasta 2 ocasiones en la falta de entrega durante la vigencia del servicio.
11.3	Incidentes con afectación de severidad 3	1% (Uno por ciento)		Alta	Hasta 1 ocasión en la falta de entrega durante la vigencia del servicio.
11.3	Incidentes con afectación de severidad 4	1% (Uno por ciento)		Muy Alta	Hasta 1 ocasión en la falta de entrega durante la vigencia del servicio.
16.5	Falla en la disponibilidad de la operación de la mesa por parte del licitante	1% (Uno por ciento)		Grave	Hasta 2 ocasiones en la falta de entrega durante el mismo mes calendario para esta deductiva.

24.3 Causales de Rescisión

La Dependencia con la que se formalice el contrato podrá en cualquier momento rescindir administrativamente el mismo, en caso de cualquier incumplimiento a las obligaciones a cargo del prestador de servicios, sin necesidad de acudir a los tribunales competentes en la materia. Si previamente a la determinación de dar por rescindido el contrato se prestaren los servicios, el procedimiento iniciado quedará sin efecto, previa aceptación y verificación de la Dependencia de que continúa vigente la necesidad de la prestación del servicio, aplicando, en su caso, las penas convencionales correspondientes; por lo que, de manera enunciativa, mas no limitativa, se entenderá por incumplimiento:

1. Que el proveedor no cumpla con los requerimientos establecidos conforme al Anexo Técnico.
2. El proveedor tenga fallas continuas durante la operación del servicio y ponga en riesgo la infraestructura y seguridad de la Institución.
3. Que el personal asignado por el proveedor sea sorprendido haciendo mal uso de la información o transfiera a terceros para bienes de uso propio y que afecten a la Institución.
4. Si el prestador del servicio tiene un tipo de falla por evento denominada muy alta por dos ocasiones durante la vigencia del contrato.

25 Forma de pago, Administrador de Contrato y Facturación

NO HABRÁ ANTICIPO ALGUNO y la SECRETARÍA efectuará los pagos por servicios prestados en pesos mexicanos de acuerdo a lo siguiente:

1. Pagos a mes vencido contra entregables a entera satisfacción

Para ello la propuesta y la factura deberán venir desglosadas en costos unitarios de cada uno de los puntos de la TABLA PROPUESTA ECONÓMICA.

El administrador del contrato y responsable de verificar la correcta prestación del servicio será el Lic. Gregorio Castilla Muñoz, Director de Infraestructura Tecnológica o quien lo sustituya en el cargo, adscrito a la Dirección General de Informática y Telecomunicaciones.

El prestador del servicio deberá enviar la factura, desglosando el Impuesto al Valor Agregado.

Las facturas deberán enviarse a la siguiente dirección de correo electrónico:

INSTITUCIÓN	CORREO PARA RECEPCIÓN DE FACTURACIÓN
SEMARNAT	gregorio.castilla@semarnat.gob.mx

26 Propuesta Económica

Para ello la propuesta de cotización y la factura deberá de venir desglosada en costos unitarios diarios de cada uno de los servicios descritos en el presente anexo y de acuerdo a la tabla siguiente:

1. Servicio de Seguridad Perimetral para Oficina Central de la SEMARNAT.
2. Servicio de Seguridad Perimetral para el Datacenter.
3. Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para la Oficina Central
4. Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para el Centro de Datos

NO.	DESCRIPCIÓN DEL SERVICIO	COSTO MENSUAL SIN I.V.A.	COSTO TOTAL POR 6 MESES DE SERVICIO SIN I.V.A.
1	Servicio de Seguridad Perimetral para Oficina Central de la SEMARNAT		
2	Servicio de Seguridad Perimetral para el Centro de Datos		
3	Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para la Oficina Central		
4	Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio para el Centro de Datos		
5	Mesa de Servicio		
		SUBTOTAL	
		I.V.A.	
		TOTAL	

- Tipo de Contratación cerrada.
- Deberán cotizar todos y cada uno de los servicios ya que la falta de alguno podrá ser motivo de desechamiento.
- Se evaluara el precio aceptable de cada cotización.

27 Glosario de términos

- Activo de Información. Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.
- Activo clave: El activo de información que resulta esencial o estratégico para la operación y/o el control de una(s) infraestructura(s) de información esenciales y/o críticas, o incluso de una que no tenga este carácter, pero cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura o en los servicios que soporta.
- Adware. Un programa de clase adware es cualquier programa que automáticamente muestra publicidad web al usuario durante su instalación o durante su uso para generar lucro a sus autores. 'Ad' en la palabra 'adware' se refiere a 'advertisement' (anuncios) en idioma inglés.
- AES: Advance Encryption Standard, esquema o algoritmo de cifrado por bloques.
- Antibot: Mecanismo que permite detectar actividades maliciosas de un atacante en los equipos de punto final.
- Appliance. Término en el idiommecanisa inglés con significado en castellano como aparato, accesorio, artefacto, etc. En informática, este término se refiere a un aparato o dispositivo electrónico (hardware) provisto de un software embebido (firmware) con la función del sistema operativo, que se utiliza para realizar funciones específicas de la aplicación y enorme complejo de software, por lo que a menudo se utilizan en las grandes redes de ordenadores o la granja de servidores de negocio.
- CDN: Content delivery network, es una red de computadoras que contienen copias de datos, colocados en varios puntos de una red con el fin de maximizar el ancho de banda para el acceso a los datos de clientes por la red.
- DMZ: Zona desmilitarizada, es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red.
- ERISC: Equipo de respuesta a incidentes de seguridad en TIC de la Secretaría.
- GUI: Graphical user interface, o interfaz gráfica de usuario es un programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz.
- Malware: (del inglés malicious software), también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.[1] El término

virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.

- Spam. Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La palabra spam proviene de la segunda guerra mundial, cuando los familiares de los soldados en guerra les enviaban comida enlatada; entre estas comidas enlatadas estaba una carne enlatada llamada spam, que en los Estados Unidos era y sigue siendo muy común.
- Phishing. Conocido también como suplantación de identidad, es un término informático que denomina un tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).
- RFC's: Request for Comments, publicaciones que describen los aspectos principales del funcionamiento del Internet, protocolos y procedimientos.
- RMA: Return Merchandise Authorization (autorización de devolución de mercancía) usado por distribuidores o corporaciones, para la transacción por el retorno de un producto por defectos para luego repararlo o reemplazarlo o hacer una nota de crédito para la compra de otro producto.
- Spyware. El spyware o programa espía es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.
- Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.
- SLAs. Un acuerdo de nivel de servicio o Service Level Agreement, también conocido por las siglas ANS o SLA, es un contrato escrito entre un ficitante de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. SGSI
- SGSI: El sistema de gestión de seguridad de la información que, por medio del análisis de riesgos y de la definición de controles, define las guías para la implementación, operación, monitoreo, revisión y mejora de la seguridad de la información.

SEMARNAT

OFICIALÍA MAYOR
DIRECCIÓN GENERAL DE INFORMÁTICA Y TELECOMUNICACIONES
DIRECCIÓN DE INFRAESTRUCTURA TECNOLÓGICA

- TIC: las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

CIUDAD DE MÉXICO, A 19 DE MAYO DE 2017

Elaboró	Revisó:
Mtra. Aneli G. Zamorategui Hernández	Lic. Gregorio Castilla Muñoz
Subdirectora de Servicios Básicos de Equipos de Datos	Director de Infraestructura Tecnológica
aneli.zamoralegui@semarnat.gob.mx	gregorio.castilla@semarnat.gob.mx

Aprobó

TITULAR DE LA DIRECCIÓN GENERAL DE INFORMÁTICA Y TELECOMUNICACIONES
La presente hoja de firmas corresponde al Proyecto denominado "Servicios Administrados de Seguridad Perimetral"
MTRO. MARIO HECTOR GONGORA PRECIADO
mariohector.gongora@semarnat.gob.mx

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

En la Ciudad de México, siendo las **11:00 horas del día 15 de junio de 2017**, en Sala de Juntas de la Dirección General de Recursos Materiales, Inmuebles y Servicios, ubicada en Av. Ejército Nacional No. 223, Piso 17 ala "B", Col. Anáhuac, C.P. 11320, Delegación Miguel Hidalgo, Ciudad de México; se reunieron los servidores públicos cuyos nombres y firmas aparecen al final de la presente Acta, con objeto de llevar a cabo la Junta de Aclaraciones a la Convocatoria indicada al rubro, de acuerdo a lo previsto en los artículos 33 último párrafo, 33 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público en adelante "La Ley", así como en el Apartado III inciso b) numeral 3 de la Convocatoria.

I. INICIO DEL ACTO.

Este Acto fue presidido por el Ing. Ramón Alejandro Alcalá Valera, Director de Adquisicione y Contratos, servidor público designado por la convocante, de conformidad con el punto II.3.1 inciso a) de las Políticas, Bases y Lineamientos en materia de adquisiciones, arrendamientos y servicios de la SEMARNAT, quien al inicio de esta Junta comunicó a los asistentes que de conformidad con el artículo 33 Bis de "La Ley", solamente se atenderían solicitudes de aclaración a la convocatoria de las personas que hayan presentado, a través de CompraNet, el escrito en el que expresen su interés en participar en esta licitación, por sí o en representación de un tercero, y cuyas solicitudes de aclaración se recibieron con 24 horas de anticipación a este Acto.

El Presidente del Acto, fue asistido por los representantes de la Dirección General de Informática y Telecomunicaciones quienes solventaron las solicitudes de aclaración de carácter técnico y el representante del área contratante solventó las solicitudes de aclaración de carácter administrativo.

II. RECEPCIÓN DE SOLICITUDES DE ACLARACIÓN.

Se hace constar que se recibieron en tiempo y forma, de conformidad al artículo 33 Bis de **"La Ley"**, las solicitudes de aclaración a la convocatoria y el escrito de interés en participar, a través de CompraNet, de los siguientes licitantes:

No.	NOMBRE, RAZÓN O DENOMINACIÓN SOCIAL	No. DE SOLICITUD DE ACLARACIONES
1	Seguridad en la Nube, S.A. de C.V.	12
2	Total Play Telecomunicaciones, S.A. de C.V.	8
3	Soluciones Integrales Saynet, S.A. de C.V.	8
4	Productos y Servicios en TIC, S.A. de C.V.	30
5	Orben Comunicaciones SAPI de C.V.	33
6	Conmext Soluciones, S.A. de C.V.	9
7	Scitum, S.A. de C.V.	38
8	Grupo de Tecnología Cibernética, S.A. de C.V.	8
9	Indra Sistemas México, S.A. de C.V.	26
10	Security One, S.A. de C.V.	9

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Asimismo se hace constar que el licitante Cisco Systems de México, S.A. de C.V., presentó escrito de interés en participar, sin presentar solicitud de aclaraciones.

III. PRECISIONES.

POR PARTE DEL ÁREA REQUIRENTE Y TÉCNICA:

PRECISIÓN No. 1:

Numeral 26, "Propuesta Económica"

DICE:

Para ello la propuesta de cotización y la factura deberá de venir desglosada en costos unitarios diarios de cada uno de los servicios descritos en el presente anexo y de acuerdo a la tabla siguiente:

1. Servicio de Seguridad Perimetral para Oficina Central de la SEMARNAT.
2. Servicio de Seguridad Perimetral para el Datacenter.
3. Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para la Oficina Central
4. Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para el Centro de Datos

NO	DESCRIPCIÓN DEL SERVICIO	COSTO MENSUAL SIN IVA	COSTO TOTAL POR 6 MESES DE SERVICIO SIN I.V.A.
1	Servicio de Seguridad Perimetral para Oficina Central de la SEMARNAT		
2	Servicio de Seguridad Perimetral para el Centro de Datos		
3	Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para la Oficina Central		
4	Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio para el Centro de Datos		
5	Mesa de Servicio		
		SUBTOTAL	
		I.V.A.	
		TOTAL	

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

- Tipo de Contratación cerrada.
- Deberán cotizar todos y cada uno de los servicios ya que la falta de alguno podrá ser motivo de desechamiento.
- Se evaluara el precio aceptable de cada cotización.

DEBE DECIR:

Para ello la propuesta de cotización y la factura deberá de venir desglosada en **costos unitarios mensuales** de cada uno de los servicios descritos en el presente anexo y de acuerdo a la tabla siguiente:

1. Servicio de Seguridad Perimetral para Oficina Central de la SEMARNAT.
2. Servicio de Seguridad Perimetral para el Datacenter.
3. Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para la Oficina Central
4. Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para el Centro de Datos

NO	DESCRIPCIÓN DEL SERVICIO	COSTO MENSUAL SIN I.V.A.	COSTO TOTAL POR 6 MESES DE SERVICIO SIN I.V.A.
1	Servicio de Seguridad Perimetral para Oficina Central de la SEMARNAT		
2	Servicio de Seguridad Perimetral para el Centro de Datos		
3	Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio para el Centro de Datos		
4	Mesa de Servicio		
		SUBTOTAL	
		I.V.A.	
		TOTAL	

- Tipo de Contratación cerrada.
- Deberán cotizar todos y cada uno de los servicios ya que la falta de alguno podrá ser motivo de desechamiento.
- Se evaluara el precio aceptable de cada cotización.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Precisión No. 2:

IV.- CUMPLIMIENTO DE CONTRATOS (MECANISMOS DE EVALUACIÓN A TRAVÉS DEL CRITERIO DE PUNTOS O PORCENTAJES)
DICE:
Para acreditar el cumplimiento, los licitantes deberán presentar MÁXIMO 3 o MINIMO 1 contratos y/o pedidos en Firewall, acompañado cada uno de ellos con el oficio de cancelación de la garantía de cumplimiento o Carta de Término, firmada por el administrador del contrato y/o pedido, mediante la cual acredite que el licitante haya prestado los servicios de manera satisfactoria.
PARA EL CUMPLIMIENTO DE CONTRATOS ÚNICAMENTE SE CONTABILIZARÁN UN MÁXIMO DE 3 INSTRUMENTOS JURÍDICOS.
Las copias de los contratos deberán cumplir con lo siguiente:
Copia de contratos y/o pedidos formalizados con personas públicas y/o privadas, mediante los cuales se acredite el cumplimiento satisfactorio de todas y cada una de las obligaciones establecidas en los mismos, en los cuales hayan prestado el servicio de renovación de licenciamiento de filtrado de contenido web, los contratos y/o pedidos, deberán cumplir con lo siguiente:

- **Cada contrato y/o pedido deberá estar debidamente formalizado por las partes.**
- **Cada contrato y/o pedido deberá estar terminado a la fecha del acto de presentación y apertura de proposiciones.**
- **Cada contrato y/o pedido deberá tener una vigencia mínima de 1 mes.**
- **Cada contrato y/o pedido celebrado con alguna entidad o dependencia en cualquier nivel de la Administración Pública será verificado en COMPRANET, en caso de existir discrepancia en la información, no será considerada y por lo tanto no serán otorgados los puntos correspondientes.**
- **En caso de que dos o más licitantes acrediten el mismo número de contratos y/o pedidos, la convocante dará la misma puntuación a los licitantes que se encuentren en este supuesto.**
- **Los contratos y/o pedidos presentados para acreditar este rubro, podrán ser los mismos que presente para acreditar el rubro de especialidad.**
- **Máximo podrán acreditar 3 contratos y/o pedidos y mínimo 1 contrato y/o pedido.**
- **En caso de no acreditar por lo menos 1 contrato y/o pedido, no le serán otorgados los puntos y será causal de desechamiento.**

El cumplimiento de los contrato y/o pedido formalizados y terminados con cualquier dependencia o entidad del gobierno federal, estatal y/o municipal, deberán estar acompañado con la copia del documento, mediante el cual se haga constar la cancelación de la garantía del cumplimiento del contrato y/o pedido respectivo, o la liberación de la fianza respectiva, dicho documento deberá contener mínimo la siguiente información:

- **Fecha de emisión.**
- **Nombre del servidor público que firma el documento de cumplimiento del contrato y/o pedido.**
- **Numero de contrato y/o pedido.**
- **Objeto del contrato y/o pedido.**
- **Que indique que se han cumplido con las obligaciones establecidas en el contrato y/o pedido.**

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

El cumplimiento de los contratos y/o pedidos formalizado y terminado con cualquier persona física o moral privada, deberá estar acompañado con la copia del documento, mediante el cual se haga constar el cumplimiento de las obligaciones establecidas en el contrato y/o pedido respectivo, dicho documento deberá contener mínimo la siguiente información:

- **Fecha de emisión.**
- **Nombre de la persona que firma el documento de cumplimiento del contrato y/o pedido.**
- **Número de contrato y/o pedido.**
- **Objeto del contrato y/o pedido.**
- **Que indique que se han cumplido con las obligaciones establecidas en el contrato y/o pedido.**

DEBE DECIR:

Para acreditar el cumplimiento, los licitantes deberán presentar MÁXIMO 3 o MINIMO 1 contratos y/o pedidos en Firewall, acompañado cada uno de ellos con el oficio de cancelación de la garantía de cumplimiento o Carta de Término, firmada por el administrador del contrato y/o pedido, mediante la cual acredite que el licitante haya prestado los servicios de manera satisfactoria.

PARA EL CUMPLIMIENTO DE CONTRATOS ÚNICAMENTE SE CONTABILIZARÁN UN MÁXIMO DE 3 INSTRUMENTOS JURÍDICOS.

Las copias de los contratos deberán cumplir con lo siguiente:

Copia de contratos y/o pedidos formalizados con personas públicas y/o privadas, mediante los cuales se acredite el cumplimiento satisfactorio de todas y cada una de las obligaciones establecidas en los mismos, en los cuales hayan prestado servicio de firewall, los contratos y/o pedidos, deberán cumplir con lo siguiente:

- **Cada contrato y/o pedido deberá estar debidamente formalizado por las partes.**
- **Cada contrato y/o pedido deberá estar terminado a la fecha del acto de presentación y apertura de proposiciones.**
- **Cada contrato y/o pedido deberá tener una vigencia mínima de 1 mes.**
- **Cada contrato y/o pedido celebrado con alguna entidad o dependencia en cualquier nivel de la Administración Pública será verificado en COMPRANET, en caso de existir discrepancia en la información, no será considerada y por lo tanto no serán otorgados los puntos correspondientes.**
- **En caso de que dos o más licitantes acrediten el mismo número de contratos y/o pedidos, la convocante dará la misma puntuación a los licitantes que se encuentren en este supuesto.**
- **Los contratos y/o pedidos presentados para acreditar este rubro, podrán ser los mismos que presente para acreditar el rubro de especialidad.**
- **Máximo podrán acreditar 3 contratos y/o pedidos y mínimo 1 contrato y/o pedido.**
- **En caso de no acreditar por lo menos 1 contrato y/o pedido, no le serán otorgados los puntos y será causal de desechamiento.**

El cumplimiento de los contrato y/o pedido formalizados y terminados con cualquier dependencia o entidad del gobierno federal, estatal y/o municipal, deberán estar acompañado con la copia del documento, mediante el cual se haga constar la cancelación de la garantía del cumplimiento del contrato

y/o pedido respectivo, o la liberación de la fianza respectiva, dicho documento deberá contener mínimo la siguiente información:

- **Fecha de emisión.**
- **Nombre del servidor público que firma el documento de cumplimiento del contrato y/o pedido.**
- **Numero de contrato y/o pedido.**
- **Objeto del contrato y/o pedido.**
- **Que indique que se han cumplido con las obligaciones establecidas en el contrato y/o pedido.**

El cumplimiento de los contratos y/o pedidos formalizado y terminado con cualquier persona física o moral privada, deberá estar acompañado con la copia del documento, mediante el cual se haga constar el cumplimiento de las obligaciones establecidas en el contrato y/o pedido respectivo, dicho documento deberá contener mínimo la siguiente información:

- **Fecha de emisión.**
- **Nombre de la persona que firma el documento de cumplimiento del contrato y/o pedido.**
- **Número de contrato y/o pedido.**
- **Objeto del contrato y/o pedido.**
- **Que indique que se han cumplido con las obligaciones establecidas en el contrato y/o pedido.**

IV. SOLICITUDES DE ACLARACIÓN Y CONTESTACIONES.

CONMEXT SOLUCIONES, S.A. DE C.V.

Pregunta 1:

Tema: El servicio deberá brindar soporte al menos 10,000,000 de sesiones concurrentes y al menos 185,000 conexiones por segundo. Página: 31-53 / p 62 Inciso: 16.1 - Seguridad perimetral para Oficina Central de la SEMARNAT, punto 4

Pregunta: Se solicita a la convocante que para confirmar el cumplimiento del soporte de al menos 10,000,000 de sesiones concurrentes y al menos 185,000 debe estar encendida la identificación de aplicaciones ya que está evaluando un Next Generation Firewall ¿Es correcta nuestra apreciación?

Respuesta: La convocante confirma que para el cumplimiento de este punto será suficiente con presentar la información técnica documental emitida por el fabricante de los equipos propuestos que se usaran para la prestación de los Servicios Administrados de Seguridad Perimetral donde se demuestre el cumplimiento de las características técnicas solicitadas conforme al Anexo Técnico de la presente Licitación.

Pregunta 2:

Tema: A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptaran componentes

de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE alimentadas por el NIST) que no hayan sido remediadas oportunamente en un plazo no mayor a 12 días naturales. Página: 32-53 / p 63 Numeral: 16.1.1 - Firewall (Seguridad perimetral para Oficina Central de la SEMARNAT), punto 13

Pregunta: En el entendido de que se requiere minimizar la probabilidad de fallas, aumentar la disponibilidad de los servicios prestados, garantizar la interoperabilidad de los equipos y el soporte del fabricante en todos los componentes de hardware y software, ¿es correcto asumir que lo requerido por el licitante es que el fabricante de los componentes deba tener un esquema de respuesta a incidentes enfocado a notificar a sus usuarios sobre vulnerabilidades de manera oportuna, así como contar con un grupo de especialistas destinados a investigar y proveer soporte a vulnerabilidades identificadas las 24 horas y los 7 días de la semana, en vez de limitar el alcance a 12 días de tiempo de remediación lo cual reduce y limita la libre competencia entre fabricantes?

Respuesta: No es correcta su apreciación, se requiere que los Servicios de Seguridad Perimetral solicitados se presten con equipos de seguridad de fabricantes que estén comprometidos en la resolución inmediata de las vulnerabilidades que puedan ser detectadas en sus equipos, por lo que es necesario presentar el reporte conforme a lo manifestado en el anexo técnico de la presente Licitación.

Pregunta 3:

Tema: El servicio deberá brindar soporte al menos 10,000,000 de sesiones concurrentes y al menos 185,000 conexiones por segundo. Página: 35-53 / p 66 Numeral: 16.2.1 - Seguridad perimetral para el Data Center (Centro de Datos), punto 4

Pregunta: Se solicita a la convocante que para confirmar el cumplimiento del soporte de al menos 10,000,000 de sesiones concurrentes y al menos 185,000 debe estar encendida la identificación de aplicaciones ya que está evaluando un Next Generation Firewall ¿Es correcta nuestra apreciación?

Respuesta: La convocante confirma que para el cumplimiento de este punto será suficiente con presentar la información técnica documental emitida por el fabricante de los equipos propuestos que se usaran para la prestación de los Servicios Administrados de Seguridad Perimetral donde se demuestre el cumplimiento de las características técnicas solicitadas conforme al Anexo Técnico de la presente Licitación.

Pregunta 4:

Tema: A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptaran componentes de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE alimentadas por el NIST) que no hayan sido remediadas oportunamente en un plazo no mayor a 12 días naturales. Página: 36-53 / p 67 Numeral: 16.2.1 - Seguridad perimetral para el Data Center (Centro de Datos), punto 13

Pregunta: En el entendido de que se requiere minimizar la probabilidad de fallas, aumentar la disponibilidad de los servicios prestados, garantizar la interoperabilidad de los equipos y el soporte del

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

fabricante en todos los componentes de hardware y software, ¿es correcto asumir que lo requerido por el licitante es que el fabricante de los componentes deba tener un esquema de respuesta a incidentes enfocado a notificar a sus usuarios sobre vulnerabilidades de manera oportuna; así como contar con un grupo de especialistas destinados a investigar y proveer soporte a vulnerabilidades identificadas las 24 horas y los 7 días de la semana, en vez de limitar el alcance a 12 días de tiempo de remediación lo cual reduce y limita la libre competencia entre fabricantes?

Respuesta: No es correcta su apreciación, se requiere que los Servicios de Seguridad Perimetral solicitados se presten con equipos de seguridad de fabricantes que estén comprometidos en la resolución inmediata de las vulnerabilidades que puedan ser detectadas en sus equipos, por lo que es necesario presentar el reporte conforme a lo manifestado en el anexo técnico de la presente Licitación.

Pregunta 5:

Tema: Deberá contar con una herramienta de búsqueda que permita fácilmente filtrar objetos de red, donde permita incluir la opción de buscar objetos duplicados (con la misma IP) y objetos no usados (en una regla o política) y una lista de reglas en que un objeto especifico es usado para una simplificación de las operaciones. Página: 40-53 p 71 Numeral: 16.3 - Consola de Administración, numeral 12

Pregunta: Es correcto asumir que se cumple con este punto si la herramienta de gestión provee la capacidad de buscar y filtrar objetos de red al igual que la detección de conflictos en el orden de las reglas/políticas configuradas por el administrador?

Respuesta: El licitante deberá apegarse a lo establecido en el Anexo Técnico, Página: 40-53 p 71 Numeral: 16.3.

Pregunta 6:

Tema: El sistema de administración centralizada debe soportar la integración de productos de análisis de vulnerabilidades Página: 40-53 p 71 Numeral: 16.3 - Consola de Administración, numeral 14

Pregunta: Con la finalidad de reducir costos de operación, incrementar la efectividad y reducir los puntos de falla se propone que el sistema de administración centralizada deba soportar la integración de productos de análisis de vulnerabilidades sin requerir un appliance o software adicional. ¿Se acepta nuestra propuesta?

Respuesta: La convocante aclara que la solución deberá soportar lo solicitado en este punto, cada licitante deberá considerar lo necesario para cumplir con lo solicitado en este punto en su oferta técnica.

Pregunta 7:

Tema: A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptaran componentes de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE

alimentadas por el NIST) que no hayan sido remediadas oportunamente en un plazo no mayor a 12 días naturales. Página: 40-53 p 71 Numeral: 16.3 - Consola de Administración, numeral 16

Pregunta: En el entendido de que se requiere minimizar la probabilidad de fallas, aumentar la disponibilidad de los servicios prestados, garantizar la interoperabilidad de los equipos y el soporte del fabricante en todos los componentes de hardware y software, ¿es correcto asumir que lo requerido por el licitante es que el fabricante de los componentes deba tener un esquema de respuesta a incidentes enfocado a notificar a sus usuarios sobre vulnerabilidades de manera oportuna, así como contar con un grupo de especialistas destinados a investigar y proveer soporte a vulnerabilidades identificadas las 24 horas y los 7 días de la semana, en vez de limitar el alcance a 12 días de tiempo de remediación lo cual reduce y limita la libre competencia entre fabricantes?

Respuesta: No es correcta su apreciación, se requiere que los Servicios Administrados de Seguridad Perimetral solicitado se presten con equipos de seguridad de fabricantes que estén comprometidos en la resolución inmediata de las vulnerabilidades que puedan ser detectadas en sus equipos, por lo que es necesario presentar el reporte conforme a lo manifestado en el anexo técnico de la presente Licitación.

Pregunta 8:

Tema: Monitoreo, El monitoreo de los componentes que habilitan el servicio debe ser continuo, las 24 horas del día durante todos los días del año, a partir del inicio de la fase de operación y hasta el final de la vigencia del contrato. Página 13-53 inciso 2

Pregunta: Para el tema de monitoreo se entiende que el licitante deberá presentar un SOC habilitado con un acceso seguro para el personal de la Semarnat, es correcta nuestra apreciación?

Respuesta: No es correcta su apreciación, el servicio de monitoreo se debe realizar en la mesa de servicios solicitada, con las herramientas necesarias para el cumplimiento de los requisitos técnicos solicitados.

Pregunta 9:

Tema: Mesa de servicios. El licitante deberá contar con una Mesa de Servicio preferentemente certificada en el estándar iso/iec 20000... Página 43-53 inciso 16.5

Pregunta: El licitante podrá presentar certificaciones compatibles con la mencionada en las Bases, sin cambiar los requerimientos de atención, niveles de servicio y disponibilidad. Se acepta nuestra propuesta?

Respuesta: La convocante aclara que, tal y como se menciona en los requerimientos del Anexo Técnico para la prestación de los Servicios Administrados de Seguridad Perimetral, deberá estar certificado, preferentemente, con el estándar ISO/IEC 20000 o cualquier otro similar, siempre y cuando cumpla con los requerimientos de atención, niveles de servicio y de disponibilidad solicitados.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

GRUPO DE TECNOLOGIA CIBERNETICA, S.A. DE C.V.

Pregunta 1

Se solicita a la convocante aceptar que la traducción simple sea solo de la característica en la que se aprecie el cumplimiento de las especificaciones solicitadas. ¿Se acepta nuestra solicitud?

Referencia: Pagina 13 de 131 g) Propuesta técnica (ANEXO 1 "Especificaciones Técnicas") 4. En caso de ser requerido y/o necesario, las personas licitantes deberán incluir en su propuesta técnica los catálogos, folletos, manuales o documentos en los que se aprecie el cumplimiento de las especificaciones solicitadas por la convocante, estos podrán ser descargados de internet, siempre y cuando la información sea clara y legible y deberá de enviarlos en un archivo escaneando los documentos solicitados, en caso de estar en otro idioma estos deberán ir acompañados de una traducción simple al español.

Respuesta: La convocante acepta la solicitud.

Pregunta 2

Entendemos que en caso de tener los catálogos, folletos, manuales o documentos en forma digital no será necesario escanearlos y deberán enviarse en un archivo digital ¿Es correcta nuestra apreciación? En caso contrario favor de aclarar.

Referencia: Pagina 13 de 131 g) Propuesta técnica (ANEXO 1 "Especificaciones Técnicas") 4. En caso de ser requerido y/o necesario, las personas licitantes deberán incluir en su propuesta técnica los catálogos, folletos, manuales o documentos en los que se aprecie el cumplimiento de las especificaciones solicitadas por la convocante, estos podrán ser descargados de internet, siempre y cuando la información sea clara y legible y deberá de enviarlos en un archivo escaneando los documentos solicitados, en caso de estar en otro idioma estos deberán ir acompañados de una traducción simple al español.

Respuesta: Es correcta su apreciación.

Pregunta 3

Se solicita a la convocante aclarar si ¿el no foliar todas y cada una de las hojas que integran nuestras proposiciones es causa de desechamiento?

Referencia: Pagina 13 de 131 f) Instrucciones para la presentación de Proposiciones 5. En el caso de que alguna o algunas hojas de los documentos mencionados en el párrafo anterior carezcan de folio y se constate que la o las hojas no foliadas mantienen continuidad, la convocante no podrá desechar la proposición.

Página 19 de 131 1. Causas de desechamiento de proposiciones M) Si cada uno de los documentos que integren la proposición, no están foliados en todas y cada una de las hojas que los integren y no se actualiza alguno de los supuestos establecidos en el tercer párrafo del artículo 50 de EL RLAASSP.

RESPUESTA.- En el caso de que alguna o algunas hojas que integren la proposición y aquéllos distintos a ésta carezcan de folio y se constate que la o las hojas no foliadas mantienen

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES
Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017
"Servicios administrados de seguridad perimetral"

continuidad, la convocante no podrá desechar la proposición. En el supuesto de que falte alguna hoja y la omisión pueda ser cubierta con información contenida en la propia proposición o con los documentos distintos a la misma, la convocante tampoco podrá desechar la proposición, tal y como se señala en el artículo 50 último párrafo de la LAASSP.

Pregunta 4

Considerando que se trata de equipos de seguridad y que son para una instancia de gobierno la entrega de equipos lleva más de 4 semanas. Se solicita a la convocante permitir que la entrega de equipos sea en un periodo de 6 a 8 semanas. ¿Se acepta nuestra propuesta?

Referencia: Pagina 40 de 131 8.1 Diseño e implementación. El licitante incluirá en el programa la fecha de entrega de los componentes y demás entregables que habilitarán el servicio, que no deben de exceder 4 semanas a partir del día hábil siguiente de la notificación del fallo.

Respuesta: No se acepta la propuesta, deberá apegarse a lo establecido en el Anexo Técnico.

Pregunta 5

Se solicita a la convocante indicar ¿con cuanto espacio en rack dispone para la instalación de los equipos?

Referencia: Pagina 46 de 131 9. Especificaciones Generales del Servicio El Licitante debe considerar los cables, accesorios y herrajes de sujeción necesarios para el montaje de sus equipos a ofertar para su instalación, solo se proporcionará el espacio físico en los racks.

Respuesta: La convocante indica que el equipo sea de propósito específico para instalarse en un rack, tipo 4 postes. Así mismo se indica que se tiene el espacio suficiencia para el equipo a implementar.

Pregunta 6

Se solicita a la convocante aceptar carta firmada por el fabricante como acreditación de que se tiene el máximo nivel de certificación en México de la solución ofrecida ¿es aceptable nuestra solicitud?

Referencia: Pagina 56 de 131 Tabla de perfiles especializados, Arquitecto líder de la solución.

Respuesta: No se acepta su solicitud deber presentar el certificado del personal que lo acredite como experto en los equipos de la solución propuesta.

Pregunta 7

Se solicita a la convocante aceptar cedula profesional equivalente a la SEP con el fin de no limitar la participación a solo personas que cursaron sus estudios en el país ¿es aceptable nuestra solicitud?

Referencia: Pagina 85 de 131 1.- Capacidad del licitante, b) competencias o habilidades en el trabajo de acuerdo a sus conocimientos académicos o profesionales relacionados con el objeto de la contratación.

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

LPP El licitante para acreditar este concepto deberá presentar 1) copia simple de cedula profesional emitida por la SEP.

Respuesta: La convocante acepta la solicitud, siempre y cuando la Cedula Profesional o documento oficial emitido por entidad educativa mediante el cual se compruebe el nivel de estudios similares a los requeridos.

Pregunta 8

Con objeto de no limitar la libre participación y con base a que el proceso será calificado por puntos y porcentajes, se solicita a la convocante que el no cumplir con los requerimientos establecidos en la tabla de puntos y porcentajes, sea causa de pérdida de los puntos acreditados y no causa de desechamiento. ¿Se acepta nuestra propuesta?

Referencia: Pagina 85 a 89 de 131 Mecanismos de evaluación a través del criterio de puntos y porcentajes, puntos 1 Capacidad del licitante, II Experiencia y especialidad del licitante, III Propuesta de trabajo, IV cumplimiento de contratos.

Respuesta: No se acepta la propuesta, el licitante deberá apegarse a lo establecido en el mecanismo de evaluación de puntos y porcentajes.

SOLUCIONES INTEGRALES SAYNET S.A. DE C.V.

Pregunta 1

Con referencia a la página 13, numeral 5, dice lo siguiente:

"Cada uno de los documentos que integren la proposición y aquellos distintos a ésta, deberán estar foliados en todas y cada una de las hojas que lo integren. A efecto, se deberán numerar de manera individual la propuesta técnica y económica, así como el resto de documentos que entregue la persona licitante".

Pregunta: Es correcto entender que para la documentación legal y administrativa se le asignara un folio individual, así como a la técnica y a la económica, teniendo como resultado 3 series de folios, uno para cada una?

RESPUESTA.- Es correcta su apreciación.

Pregunta 2

Con referencia a la página 76 y 77, numeral 18 y 19, que dicen lo siguiente:

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Cronograma de Trabajo

Para la contratación de este servicio, y a manera de estudio de mercado, la SEMARNAT, requiere de lo siguiente:

Servicio comprende a partir del día siguiente de la notificación del fallo y hasta el 31 de diciembre de 2017.

El Plan de trabajo estimado para la entrega del servicio es el siguiente:

Vigencia

El periodo del servicio será a partir del día siguiente de la notificación del fallo y hasta el 31 de diciembre de 2017

Pregunta: Con base en estos dos puntos debemos entender que las fases de diseño e implementación y transición y estabilización, serán parte integral de los servicios y que serán parte de los entregables para el pago de la primer factura?

Respuesta: El presente procedimiento no se refiere a una investigación de mercado, corresponde a la contratación de un servicio, respecto a su pregunta es correcto su comentario.

Pregunta 3

Con referencia a la página 77 y 81, numeral 18 y 26, que dicen lo siguiente:

Cronograma de Trabajo

Para la contratación de este servicio, y a manera de estudio de mercado, la SEMARNAT, requiere de lo siguiente:

Servicio comprende a partir del día siguiente de la notificación del fallo y hasta el 31 de diciembre de 2017.

El Plan de trabajo estimado para la entrega del servicio es el siguiente:

Propuesta Económica

Para ello la propuesta de cotización y la factura deberá de venir desglosada en costos unitarios diarios de cada uno de los servicios descritos en el presente anexo y de acuerdo a la tabla siguiente:

1. Servicio de Seguridad Perimetral para Oficina Central de la SEMARNAT.
2. Servicio de Seguridad Perimetral para el Datacenter.
3. Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para la Oficina Central
4. Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para el Centro de Datos

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

N	DESCRIPCIÓN DEL SERVICIO	COSTO MENSUAL	COSTO TOTAL POR 6 MESES DE SERVICIO
1	Servicio de Seguridad Perimetral para Oficina Central de la SEMARNAT		
2	Servicio de Seguridad Perimetral para el Centro de Datos		
3	Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para la Oficina Central		
4	Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio para el Centro de Datos		
5	Mesa de Servicio		

Pregunta: Con base en estos dos puntos debemos entender que el periodo mínimo de contratación es de 6 meses?

Respuesta: El presente procedimiento no se refiere a una investigación de mercado, corresponde a la contratación de un servicio. Se aclara a la licitante que independiente de la fecha de notificación de fallo la vigencia del servicio será hasta el 31 de diciembre de 2017.

Pregunta 4

Con referencia a la página 81, numeral 26, que dicen lo siguiente:

Propuesta Económica

Para ello la propuesta de cotización y la factura deberá de venir desglosada en costos unitarios diarios de cada uno de los servicios descritos en el presente anexo y de acuerdo a la tabla siguiente:

1. Servicio de Seguridad Perimetral para Oficina Central de la SEMARNAT.
2. Servicio de Seguridad Perimetral para el Datacenter.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

3. Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para la Oficina Central
4. Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para el Centro de Datos

N	DESCRIPCIÓN DEL SERVICIO	COSTO MENSUAL	COSTO TOTAL POR 6 MESES DE SERVICIO
1	Servicio de Seguridad Perimetral para Oficina Central de la SEMARNAT		
2	Servicio de Seguridad Perimetral para el Centro de Datos		
3	Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para la Oficina Central		
4	Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio para el Centro de Datos		

Pregunta: En el texto dice "deberá de venir desglosada en costos unitarios diarios" y la tabla solicita precios mensuales, podría aclarar la convocante si se deben presentar precios unitarios diarios o mensuales?

Respuesta: Se solicita al licitante que se remita a la precisión No. 1

Pregunta 5

Con referencia a la página 13, Inciso g, punto 4, donde se solicita:

Que los catálogos, folletos, manuales o documentos, que acompañen la propuesta técnica sean con una traducción simple al español en caso de estar en otro idioma.

Pregunta: Se solicita a la convocante en el caso de incluir estos documentos como lo son los manuales se acepte la traducción simple del párrafo o párrafos que hagan referencia a la especificación solicitada,

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

esto debido a que algunos manuales constan de 500 páginas o incluso más y realizar la traducción completa sería imposible para este procedimiento. Se acepta la solicitud?

Respuesta: La convocante acepta la solicitud.

Pregunta 6

Con referencia a la página 74, punto 16.5, que dicen lo siguiente:

Mesa de Servicios

El licitante deberá contar con una Mesa de Servicios preferentemente certificada en el estándar ISO/IEC 20000 y disponible en un esquema 7x24x365 con capacidad de recepción, atención y seguimiento de eventos de manera telefónica, por correo electrónico y en herramienta web, mediante una metodología de Punto Único de Contacto.

Pregunta: Se entiende que la mesa de servicios estará en las instalaciones del proveedor y será prestado el servicio con la infraestructura con la que cuenta el mismo, es correcto nuestro entender?

Respuesta: Es correcta su apreciación, la mesa de servicio solicitada deberá estar instalada en las instalaciones del licitante.

Pregunta 7

Con referencia a la página 75, Numeral 17, punto 7, que dicen lo siguiente:

1 **Lugar, tiempo y Control de entrega de los Servicios.**

Para el correcto control para la prestación de los servicios el licitante deberá proporcionar una herramienta web para el Control y Gestión de los Servicios que se prestarán por los ingenieros de campo en las diversas localidades definidas por la SEMARNAT sin costo adicional para la convocante, esta herramienta deberá estar disponible las 24 hrs del día los 365 días del año con un nivel de servicio del 99%. Esta herramienta web ayudará a la (Dirección General de Informática y Telecomunicaciones (DGIT,) a controlar y administrar de una forma fácil y sencilla las órdenes de servicio solicitadas, deberá permitir al menos lo siguiente:

- El control por localización geográfica de llegadas y salidas de los ingenieros de campo
- El seguimiento de actividades asignadas, pendientes, programadas, terminadas o canceladas mediante un dashboard de información ejecutivo en tiempo real, accesado mediante web.

Pregunta: Se mencionan ingenieros en campo, para este requerimiento se requiere de ingenieros en sitio de manera permanente para la prestación del servicio? Y si es así cuantos se requieren por localidad?

Respuesta: La convocante aclara que no se requieren de ingenieros en sitio. El ingeniero en sitio se prestará cuando el servicio prestado así lo requiera.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 8

Con referencia a la página 55, Numeral 13, que dicen lo siguiente:

Cartas y certificaciones

Que está autorizado para comercializar las soluciones propuestas para la prestación de los servicios de este procedimiento y que es distribuidor autorizado del mismo, deberá de venir firmada por el represente legal del fabricante.

El licitante deberá presentar documento donde especifique que los equipos que proporcione no tengan anuncio de fin de vida, ni anuncio de fin de mantenimiento.

Pregunta: El documento que solicita la convocante de fin de vida podrá ser una impresión de la página Web del fabricante donde especifique que es un equipo de línea?

Respuesta: No se acepta su solicitud, el licitante deberá presentar carta del fabricante firmada por el representante legal de este que avale lo solicitado por la convocante.

ORBEN COMUNICACIONES SAPI DE C.V.

Pregunta 1

NUMERAL II OBJETO Y ALCANCE DEL PROCEDIMIENTO DE CONTRATACIÓN, solicitamos a convocante comparte las bases en formato WORD o PDF con mejor resolución para una mejor lectura e interpretación, ya que el documento publicado tiene secciones no legibles, ¿acepta nuestra propuesta?

Respuesta: Las bases de la presente licitación no se entregarán en formato "Microsoft Word" o PDF.

Pregunta 2

Junta de Aclaraciones, PAG 5, Al ser este un procedimiento de Licitación Pública Nacional Electrónico, ¿podría la convocante confirmar que una vez que la convocante suba el acta de Junta de Aclaraciones en la plataforma de Compranet e informe a los licitantes iniciara el plazo para formular las preguntas que consideremos necesarias en relación con las respuestas remitidas? Esto de conformidad al artículo 46 fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASSP), en donde se indica que se brindara un plazo para que formulemos las preguntas que consideremos necesarias en relación a las respuestas remitidas.

RESPUESTA.- Tal y como se señala en el artículo 46 fracción II segundo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios, se indicará el plazo que los licitantes tendrán para formular las preguntas que consideren necesarias en relación con las respuestas remitidas.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 3

Junta de Aclaraciones , PAG 5 , es de nuestro entendimiento y de conformidad al Artículo 33 Bis de la LAASSP , que en caso de que el Acto de Junta de Aclaraciones sea suspendido y reanudado en fecha posterior, el Acto el acto de presentación y apertura de proposiciones será pospuesto considerando un plazo de al menos seis días naturales desde el momento en que concluya la junta de aclaraciones hasta el momento del acto de presentación y apertura de proposiciones., ¿es correcto nuestro entendimiento?

RESPUESTA.- Es correcto, conforme al artículo 33 Bis de la LAASSP, se consideran seis días naturales entre la fecha de la última junta de aclaraciones y el acto de presentación y apertura de proposiciones

Pregunta 4

FIRMA DE CONTRATO, PAG 8 ¿Podría la convocante indicar en qué momento de formalización del contrato con el licitante ganador puede presentarse la solicitud para aprobación de la cesión de derechos de cobro?

RESPUESTA.- Una vez que se encuentre totalmente firmado por las partes, se podrá solicitar la cesión de derechos.

Pregunta 5

XVII. CONDICIONES DE PAGO, PAG 26 ¿Podría la convocante indicar si se tienen periodos vacacionales, toma de inventario físico, etc. que puedan interferir los tiempos de procesamiento de pagos?

Respuesta: La convocante informa que durante los periodos vacacionales los tiempos de procesamiento de pago no se verán afectados.

Pregunta 6

IV. REQUISITOS QUE LOS LICITANTES DEBEN CUMPLIR, FORMATO DE ACREDITACION PAGINA 15, solicitan presentar identificación oficial del representante legal, es de nuestro entendimiento que cualquiera de los siguientes documentos se considera una identificación oficial:

- Credencial para votar expedida por el Instituto Nacional Electoral vigente (antes Instituto Federal Electoral).
- Pasaporte vigente.
- Cédula profesional vigente.

Tratándose de extranjeros:

- Documento migratorio vigente que corresponda, emitido por autoridad competente (en su caso prórroga o refrendo migratorio)

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

RESPUESTA.- Es correcta su apreciación.

Pregunta 7

Pág. 3, e) Idioma, se indica que los catálogos que se presente en otro idioma deberán ir acompañados de su traducción simple al español. ¿Acepta la convocante se pueda entregar traducción únicamente de los párrafos que se utilicen para las referencias?

Respuesta: La convocante acepta la propuesta.

Pregunta 8

Pág. 39, se indica El equipamiento a considerar por el proveedor soporte al menos 200 Mbps para transferencia de información en Oficinas Centrales y 100 Mbps para el Centro de Datos. ¿Puede confirmar estas cantidades ya que 200 Mbps está por debajo de la capacidad de enlace de internet existente que es de 250 Mbps como se indica en la pág. 38?

Respuesta: La convocante precisa que se requiriere de al menos 250 Mbps y para Centro de Datos de al menos 100 Mbps, el ofertar transferencia superior no será causal de desechamiento.

Pregunta 9

Pág. 39, descripción de los servicios, se indica Proporcionará el aseguramiento en toda la infraestructura tecnológica (en los sitios de Ejercito Nacional. CONAGUA, 31 delegaciones. 4 sitios externos en la zona metropolitana y 1 en el estado de Aguascalientes -INEGI-). ¿Puede confirmar que en el alcance de esta licitación están fuera todos los sitios mencionados a excepción de las Oficinas Centrales y el Centro de Datos?

Respuesta: La convocante confirma que los servicios solicitados comprenden las Oficinas Centrales y el Centro de Datos, los cuales proporcionan servicio de internet en oficinas centrales por enlace MPLS y aplicativos internos en el Centro de Datos de Conagua en lo que respecta a 31 delegaciones. 4 sitios externos en la zona metropolitana y 1 en el estado de Aguascalientes – INEGI, se tiene un enlace MPLS al centro de datos de Conagua.

Pregunta 10

Pág. 39, descripción de los servicios, se indica hardware y software para lograr el esquema de seguridad que la SEMARNAT requiere para garantizar el óptimo funcionamiento de tos sistemas, preservar la seguridad de la información en su infraestructura tecnológica (enlaces de MPLS e Internet, routers y switches, equipo de filtrado web) ¿Puede confirmar que las tecnologías mencionadas están fuera del alcance de esta licitación en la cual se contemplará únicamente los Servicios de Seguridad Perimetral para Oficina Central y DataCenter, el Sistema de Contención de Ataques de Disponibilidad para Oficina Central y DataCenter y la mesa de servicio como se indica en la pág. 81 propuesta económica?

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Respuesta: La convocante solamente requiere los Servicios de Seguridad Perimetral tanto para Oficina Central como para Centro de Datos. Respecto a los Servicios de Contención de Ataques de disponibilidad solo se requieren para el Centro de Datos. Adicional a estos servicios deberá cumplir con los requerimientos técnicos para la prestación de la Mesa de Servicios.

Para la entrega de la propuesta económica, se solicita remitirse a la precisión 1

Pregunta 11

Página 39, Numeral 2 Procesos, indican que durante la implementación y operación de los servicios se deberán seguir los procesos y procedimientos definidos en el MAAGTICS, es de nuestro entendimiento que los procesos y procedimientos deben estar bajo las normas y estándares solicitados en el MAAGTICSI, como las descritas en su APÉNDICE IV. B MATRIZ DE METODOLOGÍAS, NORMAS Y MEJORES PRÁCTICAS APLICABLES A LA GESTIÓN DE LAS TIC, ¿es correcto nuestro entendimiento?

Respuesta: La licitante deberá ajustarse durante la implementación de los servicios al Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI)

Pregunta 12

Pág. 40, 8.1 Diseño e Implementación se indica Esta fase comprende la implementación-migración del servicio, debe tener una duración máxima de 4 semanas a partir del día hábil siguiente a la notificación del fallo. Dado que los equipos de seguridad solicitados requieren un permiso especial del gobierno para su exportación, cuyo trámite tarda hasta 4 semanas, se solicita a la convocante pueda extender el periodo de implementación al menos a 45 días naturales después del fallo.

Respuesta: El licitante deberá apegarse a lo establecido en el Anexo Técnico en el numeral 8.1 Diseño e Implementación.

Pregunta 13

Pág. 44, monitoreo, ¿puede confirmar si el monitoreo podrá realizarse vía remota utilizando herramientas propias del NOC del licitante mediante conexión segura por VPN?

Respuesta: La convocante confirma que los medios de conexión para la herramienta de monitoreo así como para la mesa de servicio, serán responsabilidad del licitante, cumpliendo en todo momento con las características mínimas requeridas para la prestación del servicio.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 14

Pág. 62, 16.1 Seguridad perimetral para Oficina Central de la SEMARNAT. ¿Puede confirmar que se deberá ofertar una solución en alta disponibilidad (2 equipos) para este servicio?

Respuesta: La convocante confirma que se requiere de una solución en alta disponibilidad con 2 equipos.

Pregunta 15

Pág. 62 y 66, se indica que el equipo debe contar con almacenamiento, firmware o bios redundante. ¿Es correcto entender que al indicar firmware o BIOS redundante se refiere a la posibilidad de almacenar 2 versiones de software (primario y secundario o standby) en el mismo equipo de manera que se tenga la posibilidad de arrancar con uno u otro para los casos en que se pueda producir una falla o corrupción en el software que esté operando?

Respuesta: Se indica a la licitante que al indicar Firmware o Bios redundante se refiere a la capacidad de resiliencia del dispositivo en conjunto con los demás componentes redundantes que se solicitan

Pregunta 16

Pág. 62 y 66 se solicitan 2 puertos de 10G, ¿puede confirmar si se deben incluir los gbic para dichas interfaces y si deben ser para corta distancia 10Gbase-SR?

Respuesta: La convocante confirma que no se requiere incluirlos, solo requiere la capacidad de los equipos propuestos para soportarlos.

Pregunta 17

Pág. 66, 16.2 Seguridad perimetral para el Data Center (Centro de Datos). ¿Puede confirmar que se deberá ofertar una solución en alta disponibilidad (2 equipos) para este servicio?

Respuesta: La convocante confirma que se requiere de una solución en alta disponibilidad con 2 equipos.

Pregunta 18

Pag 51, Indican que el licitante debe contar con una mesa de servicios certificada en ISO/IEC 20000, ¿es de nuestro entendimiento que esta mesa de servicios certificada debe estar en las instalaciones del licitante?

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Respuesta: Es correcta su apreciación, la convocante aclara que, tal y como se menciona en los requerimientos del Anexo Técnico para la prestación de los Servicios Administrados de Seguridad Perimetral, deberá estar certificado, preferentemente, con el estándar ISO/IEC 20000 o cualquier otro similar, la mesa de servicios deberá residir en las instalaciones del licitante, el método de conexión para el acceso a la misma depende de cada licitante.

Pregunta 19

Pág. 70, 16.3 Consola de Administración, Dado que este elemento no está listado en el formato de propuesta económica de la pág. 81, ¿puede confirmar en qué concepto del formato económico debemos integrar el costo de esta solución o en su defecto pueda modificar el formato para poder incluir este concepto?

Respuesta: La convocante confirma que el costo de la consola de administración forma parte integral de los servicios de seguridad perimetral solicitados tanto para la Oficina Central como para el Centro de Datos.

Pregunta 20

Pág. 71, 16.4 Sistema de Contención de Ataques de Disponibilidad, en el numeral 1, se indica que debe ser un equipo dedicado y enfocado a prevención de ataques de negación de servicio o que no mantengan el estado de la conexión. ¿Es correcto que para el cumplimiento de este numeral será suficiente demostrar que el equipo es de propósito exclusivo al 100% para prevención de DDoS/DoS y que no se trata de un equipo de tipo UTM, NGFW, NGIPS, NBA, etcétera?

Respuesta: Es correcta su apreciación.

Pregunta 21

Pág. 72, Sistema de Contención de Ataques de Disponibilidad, numeral 6, el fabricante de la solución deberá contar con algún sistema de inteligencia donde se esté monitoreando las amenazas de Internet a nivel mundial y podrá proporcionar información sobre: Botnets o DDoS, Scans, Phishing. Aunque estas características de reporte de scans y phising corresponden al sistema de inteligencia de fabricante, no a la solución de contención de ataques DDoS, ¿puede confirmar la convocante que el sistema de prevención DDoS únicamente deberá ser retroalimentado por el sistema de inteligencia global para los ataques que corresponden a una solución de DDoS debido a que scans y phising no son ataques en los que está enfocada esta solución?

Respuesta: La convocante confirma que para el cumplimiento de este requerimiento el fabricante de los equipos que conforman la solución ofertada deberá contar con algún sistema de inteligencia donde se esté monitoreando las amenazas de Internet a nivel mundial, documentado la existencia del mismo.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 22

Pág. 73, numeral 10. La solución deberá Descartar paquetes según puertos TCP o UDP específicos y payloads que coincidan o no con expresiones regulares configurables. Dado que el uso de expresiones regulares no es el único método por el cual se puede definir el tipo de tráfico a descartar y adicionalmente se requiere un conocimiento profundo de estas expresiones que no son necesariamente enfocadas a seguridad. ¿Puede confirmar la convocante que como opción al uso de expresiones regulares para definir los patrones del tráfico a descartar se podrá ofertar el método que el propio fabricante de cada solución haya definido para definir estas reglas, pudiendo ser vía comando o gráfica? Lo anterior en el entendido que el único responsable de realizar las configuraciones necesarias será el personal especializado del licitante lo que sería transparente para la convocante la forma en que se realice.

Respuesta: No se acepta su petición, ya que se requiere tener la capacidad de buscar cadenas de texto en los paquetes de TCP o UDP por medio de expresiones regulares que permitan el bloqueo de tráfico.

Pregunta 23

Pág. 73, numeral 17. El sistema podrá de identificar web crawlers y monitorear su uso. Dado que web crawler es un tipo específico de tráfico que no es malicioso a menos que empiece a rebasar umbrales definidos como aceptables. Se solicita que el término de "web crawler" pueda ser opcional, siempre que se demuestre que puede identificar el tráfico generado por estos y comparado con los umbrales que se hayan definido para evitar un problema de negación de servicio.

Respuesta: La convocante acepta la solicitud.

Pregunta 24

Pág. 75, numeral 6, se indica que las reubicaciones no deberán tener un costo extra. ¿Puede confirmar que el traslado/transporte de los equipos de un sitio a otro estaría a cargo de la convocante?

Respuesta: No es correcta su apreciación, el traslado o transporte de los equipos en caso de alguna reubicación deberá correr a cargo del licitante.

Pregunta 25

Pág. 76, primer viñeta se indica que se debe contar con El control por localización geográfica de llegadas y salidas de los ingenieros de campo. Se solicita a la convocante que esta funcionalidad pueda ser opcional dado que la localización geográfica de los ingenieros es un parámetro irrelevante para el servicio solicitado siempre que se cumpla con los SLAs definidos en bases.

Respuesta: La convocante acepta la solicitud.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 26

Pág. 76, se solicita, Para el control de los ingenieros de campo deberá contar con una aplicación accesible mediante cualquier dispositivo móvil tipo Smartphone (IOS, Windows, Android) mediante la cual se consultará el detalle del servicio a realizar y las actividades necesarias, realizar los informes de la llegada del personal al sitio, y la conclusión de cada actividad, y la notificación de observaciones y finalización del servicio en tiempo real. Se solicita a la convocante que esta funcionalidad pueda ser opcional dado que una herramienta en smartphone para el uso de los ingenieros de campo es una funcionalidad irrelevante para el servicio solicitado; siempre que se cumpla con los SLAs definidos en bases, el licitante debería poder definir los métodos de control de su personal como mejor convenga para cumplir los SLAs comprometidos. ¿Se acepta nuestra solicitud?

Respuesta: No se acepta su solicitud, la licitante deberá apegarse a las características técnicas solicitadas.

Pregunta 27

Pág. 78, numeral. 24.2 Deducciones, se indica que será del 1% por cada día natural sobre el importe de los servicios prestados en forma parcial o deficientemente. ¿Puede confirmar que el cálculo del 1% se realizará sobre el monto mensual del servicio?

Respuesta: La convocante confirma que el cálculo será del 1% sobre el monto mensual del servicio no prestado en forma parcial o deficiente.

Pregunta 28

Pag 85 MECANISMOS DE EVALUACIÓN A TRAVÉS OEL CRITERIO DE PUNTOS O PORCENTAJES, subrubro c, Dominio de Herramientas relacionadas con el servicio, para el recurso **Especialista en alineación de servicios**, es de nuestro entendimiento que lo que solicita la convocante son requisitos mínimos y podemos presentar una certificación en ITIL Expert que es mayor a las solicitadas por la convocante (Operational Support and Analysis (OSA) o Service Offerings & Agreements (SOA))

Respuesta: El licitante deberá apegarse a lo establecido en el Anexo Técnico.

Pregunta 29

Pág. 85 MECANISMOS DE EVALUACIÓN A TRAVÉS DEL CRITERIO DE PUNTOS O PORCENTAJES, rubro ii. Experiencia y Especialidad del Licitante pág. 87, indican que el objeto de los contratos sean de servicios administrados, es de nuestro entendimiento que los contratos y/o pedidos deben incluir soluciones de seguridad?

Respuesta: La convocante aclara que para el rubro "II.- EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE", los contratos para el rubro de experiencia deberán ser contratos cuyo objeto contenga Servicios de Seguridad Perimetral o similar y deberán de estar concluidos a la fecha de presentación de propuestas.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Los contratos para el rubro de Especialidad deberán contener la solución de firewall dentro de sus componentes y deberán de estar concluidos a la fecha de presentación de propuestas.

Pregunta 30

Pág. 87 MECANISMOS DE EVALUACIÓN A TRAVÉS DEL CRITERIO DE PUNTOS O PORCENTAJES, rubro ii. Experiencia y Especialidad del Licitante pág. 87, indican que el objeto de los contratos sean de servicios administrados, es de nuestro entendimiento que los contratos y/o pedidos deben incluir soluciones de seguridad similares a los solicitados por la convocante en el Anexo técnico del presente procedimiento?

Respuesta: La convocante aclara que para el rubro "II.- EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE", los contratos para el rubro de experiencia deberán ser contratos cuyo objeto contenga Servicios de Seguridad Perimetral o similar y deberán de estar concluidos a la fecha de presentación de propuestas.

Los contratos para el rubro de Especialidad deberán contener la solución de firewall dentro de sus componentes y deberán de estar concluidos a la fecha de presentación de propuestas.

Pregunta 31

Pág. 87 MECANISMOS DE EVALUACIÓN A TRAVÉS OEL CRITERIO DE PUNTOS O PORCENTAJES, rubro ii. Experiencia y Especialidad del Licitante pág. 87, indican que se pueden presentar contratos plurianuales, los cuales por su naturaleza aún pueden estar vigentes a la fecha de presentación y apertura de proposiciones de la presente licitación, ¿es correcto entender que en el caso los contratos plurianuales solo se computaran los años fiscales concluídos a la fecha de apertura?

Respuesta: Es correcto su comentario, para el rubro II. EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE, Relativo al inciso a) Experiencia, se aceptará la presentación de contratos y/o pedidos plurianuales en los que se haya pactado que las obligaciones del proveedor se consideran divisibles, a efecto de sean susceptibles de computarse los años, meses o fracciones de año de dichos contratos y/o pedidos, en los que se hayan concluido o finiquitado obligaciones.

Pregunta 32

PAG 88 MECANISMOS DE EVALUACIÓN A TRAVÉS OEL CRITERIO DE PUNTOS O PORCENTAJES, rubro METODOLOGÍA PARA LA PRESTACIÓN DEL SERVICIO, se indica que para obtener 6 Puntos el Licitante deberá entregar documentos en el cual exponga la metodología a utilizar en la Gestión de Incidentes, Gestión de Problemas y Cumplimiento de Solicitudes , ¿es correcto entender que un certificado del estándar ISO 20000 a nombre del licitante y vigente al acto de apertura, sería la manera de acreditar oficialmente la aplicación las metodologías solicitadas por la convocante?

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Respuesta: No es correcta su apreciación se requiere que detalle la metodología propuesta a utilizar en la Gestión de Incidentes, Gestión de Problemas y Cumplimiento de solicitudes.

Pregunta 33

Pág. 88 MECANISMOS DE EVALUACIÓN A TRAVÉS OEL CRITERIO DE PUNTOS O PORCENTAJES, rubro IV, Cumplimiento de Contratos, es correcto entender que los contratos presentados en este rubro, pueden ser los mismos presentado en el rubro ii. Experiencia y Especialidad del Licitante

Respuesta: No es correcta su apreciación. Podrán ser los mismos para el rubro de especialidad

SEGURIDAD EN LA NUBE, S.A. DE C.V.

Pregunta 1

Dice: Pág. 39 "El equipamiento a considerar por el Proveedor soporte al menos 200 mbps para la transferencia de información en oficinas centrales..."

Y en la página anterior dice: "El centro de datos cuenta con un enlace de 70 mbps para el acceso a internet y en sus oficinas centrales con capacidad de 250 mbps"

Pregunta: ¿Podría la convocante precisar si lo que se requiere proteger es el enlace de 250 mbps?

Respuesta: La convocante precisa que se requiriere de al menos 250 Mbps y para Centro de Datos de al menos 100 Mbps, el ofertar transferencia superior no será causal de desechamiento.

Pregunta 2

Dice: Punto 5, inciso C, Pág. 51 "El licitante deberá encargarse de contar con una mesa de servicios preferentemente certificada en el estándar ISO/IEC 20000"

Pregunta: Podría precisar la convocante, que el indicar "preferentemente" se refiere a que este requisito es opcional, ¿estamos en lo correcto?

Respuesta: Es correcta su apreciación, la convocante aclara que, tal y como se menciona en los requerimientos del Anexo Técnico para la prestación de los Servicios Administrados de Seguridad Perimetral, deberá estar certificado, preferentemente, con el estándar ISO/IEC 20000 o cualquier otro similar.

Pregunta 3

Dice: Pág. 61, Numeral 16 Especificaciones generales de la solución propuesta.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017
"Servicios administrados de seguridad perimetral"

Pregunta: ¿Podría la convocante definir si la solución "Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet" es requerida para ambos sitios mencionados (oficinas centrales y centro de datos) o solo uno de estos sitios?

Respuesta: La convocante aclara que con Respecto a los Servicios de Contención de Ataques de Disponibilidad solo se requieren para el sitio del Centro de Datos.

Pregunta 4

Dice: Pág. 61, Numeral 16.1 Seguridad perimetral para oficina central de la SEMARNAT.

Pregunta: "...Así como almacenamiento, firmware o BIOS redundante..." ¿Puede la convocante confirmar que este punto hace referencia a la capacidad de contar con 2 particiones que permitan guardar la integridad del software en casos de actualización del appliance?

¿Puede la convocante confirmar que la respuesta aplica para las localidades – DataCenter y Oficinas Centrales?

Respuesta: No es correcta su apreciación, es para contar con la capacidad de resiliencia. El requerimiento es aplicable para ambos sitios: DataCenter y Oficinas Centrales.

Pregunta 5

Dice: Pág. 62, Numeral 16.1 Seguridad perimetral para oficina central de la SEMARNAT.

Pregunta: ¿Podría la convocante definir el resultado técnico esperado para los conceptos de Firmware o BIOS redundante?

Respuesta: La convocante aclara que el resultado técnico se refiere a que el dispositivo debe ser resiliente.

Pregunta 6

Dice: Pág. 62, Numeral General

Pregunta: ¿Aceptaría la convocante que la solución requerida para el IPS, se encuentre integrada en el Firewall siempre y cuando cumpla sus especificaciones técnicas?

¿Puede la convocante confirmar que la respuesta aplica para las localidades – DataCenter y Oficinas Centrales?

Respuesta: Se acepta su petición siempre y cuando cumpla sus especificaciones técnicas solicitadas. El requerimiento es aplicable para ambos sitios: DataCenter y Oficinas Centrales.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 7

Dice: Pág. 63, Numeral 16.1.1 Firewall

Pregunta: La solución "Sandboxing" al ser una solución que realiza el análisis de código malicioso y emular el comportamiento de archivos desconocidos genera un elevado consumo de recursos que podrían afectaran indirectamente la operación de la convocante. ¿Podría la convocante permitir la propuesta de una solución tipo Sandboxing como servicios propósito especifico con interacción en la nube de la solución?

¿Puede la convocante confirmar que la respuesta aplica para las localidades – DataCenter y Oficinas Centrales?

Respuesta: Se acepta su petición ya que la propuesta de solución de sandboxing será de acuerdo a la integración de cada licitante, siempre y cuando cumpla con las características técnicas solicitadas. El requerimiento es aplicable para ambos sitios: DataCenter y Oficinas Centrales.

Pregunta 8

Dice: Pág. 63, Numeral 16.1.2 IPS y Prevención de intrusos

Pregunta: "Deberá contar con una eficiencia de 99% ... NSS Labs Breach Detection System" Debido a que es una tecnología de NGFW y de propósito específico, ¿Puede la convocante confirmar que al mencionar Breach Detection System se refiere a una tecnología de propósito sandboxing?

¿Puede la convocante confirmar que la respuesta aplica para las localidades – DataCenter y Oficinas Centrales?

Respuesta: La convocante hace la aclaración de que lo solicitado es que el fabricante cuente con las eficiencias solicitadas en dicho reporte. El requerimiento es aplicable para ambos sitios: DataCenter y Oficinas Centrales.

Pregunta 9

Dice: Pág. 63, Numeral 16.1.2 IPS y Prevención de intrusos

Pregunta: "... http, SMTP, IMAP, POP3, FTP, SMB" ¿Aceptaría la convocante que se tenga soporte como máximo 5 de los protocolos mencionados?

¿Puede la convocante confirmar que la respuesta aplica para las localidades – DataCenter y Oficinas Centrales?

Respuesta: La convocante confirma que los protocolos que deberán soportar deberán ser al menos los siguientes: HTTP, SMTP, IMAP, POP3, FTP, SMB o CIFS. El requerimiento es aplicable para ambos sitios: DataCenter y Oficinas Centrales.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES
Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017
"Servicios administrados de seguridad perimetral"

Pregunta 10

Dice: Pág. 70, Numeral 16.3 Consola de administración.

Pregunta: "Deberá ser capaz de crear un perfil de tráfico de la red para crear baselines del tráfico existente en la red"

¿Podría la convocante confirmar que esta funcionalidad se refiere a la creación de perfiles de tráfico por medio de políticas gestionables para la correcta administración del ancho de banda?

Respuesta: La convocante aclara que la consola deberá tener la capacidad de poder graficar el tipo de tráfico existente en la red, para cumplir con esta funcionalidad.

Pregunta 11

Dice: Pág. 13, Numeral 3. Se presentará en idioma español, así como todos y cada uno de los documentos que la integran.

Pregunta: ¿Acepta la convocante que la traducción simple al español se encuentre en la tabla de referencias cruzadas que haga referencia al requerimiento puntual solicitado por la convocante?

Respuesta: Se acepta su solicitud.

Pregunta 12

Dice: Pág. 40, Numeral 8.1 Diseño e Implantación.

Pregunta: ¿Aceptaría la convocante modificar el tiempo de implementación migración del servicio a 8 semanas? Debido a que los tiempos de entrega promedio de fabricantes son de 4-6 semanas.

Respuesta: No se acepta su solicitud, deberá apegarse al cronograma de actividades del Anexo Técnico.

SECURITY ONE S.A. DE C.V.

Pregunta 1

Firewall

Página 63, Dice: Las comunicaciones entre la consola de administración y los dispositivos administrador deberá ser cifrada (encriptada), esto al considerarse equipos perimetrales altamente críticos.

Pregunta: ¿Debemos entender que el acceso a dichos equipos sea por medio de HTTPS, tanto en los equipos de seguridad perimetral como en la consola de administración?, ¿Es correcta nuestra apreciación?

Respuesta: No es correcta su apreciación, las comunicaciones deberán ser cifradas entre la consola y los equipos de seguridad perimetral sobre SSL y la administración desde la consola

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

podrá ser ya sea por consola GUI o HTTPS siempre y cuando no hayan presentado vulnerabilidades de XSS.

Pregunta 2

Página 63. Dice: A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptan componentes de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE alimentadas por el NIST) que no hayas sido remediadas oportunamente en un plano no mayor a 12 días naturales.

Pregunta: ¿Debemos entender que se deberá entregar un reporte donde se pueda confirmar que la última versión de software disponible no haya tenido alguna vulnerabilidad crítica?, ¿Es correcta nuestra apreciación?

Respuesta: No es correcta su apreciación, se deberá entregar el reporte donde se valide que el fabricante ha remediado las vulnerabilidades presentadas en todas sus soluciones en un plazo no mayor a 12 días naturales en el último año.

Pregunta 3

Página 40 de 131.- Diseño e implementación.

Dice: "En su propuesta técnica el licitante debe proporcionar un programa de actividades a ejecutar para cumplir con los entregables que la SEMARNAT le solicita para esta fase"

Pregunta: para poder generar un programa de actividades lo más cercano a la realidad, podría la convocante especificar con que tecnología cuentan actualmente en todos los rubros solicitados, para poder dimensionar tiempos de migración e instalación.

Respuesta: La convocante aclara que los licitantes deberán de realizar un plan de trabajo estándar de acuerdo con su experiencia sin importar las tecnologías, para el plan de trabajo detallado lo realizará el licitante ganador en la primera fase del servicio deberá entregar a más tardar 1 semana después del día hábil inmediato después del fallo.

Pregunta 4

Página 39 de 131. Descripción de los servicios.

Dice: 1.- Tecnología: Proporcionara el aseguramiento en toda la infraestructura tecnológica (en los sitios de Ejercito Nacional, CONAGUA, 31 delegaciones, 4 sitios externos en la zona metropolitana y 1 en el estado de Aguascalientes –INEGI) hardware y software para lograr el esquema de seguridad que la SEMARNAT requiere para garantizar el óptimo funcionamiento de los sistemas, preservar la seguridad de la información en su infraestructura tecnológica (enlaces de MPLS e INTERNET, routers y switches, equipo de filtrado web), garantizando el óptimo uso de los recursos de telecomunicaciones.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta: Debemos entender que para los sitios de Ejercito Nacional, CONAGUA, 31 delegaciones, 4 sitios externos en la zona metropolitana y 1 en el estado de Aguascalientes –INEGI, un total de 38 sitios, se deberá proponer equipos en Alta Disponibilidad con las características mencionadas para el FW-IPS y DDOS), es correcta nuestra apreciación.

Respuesta: La convocante confirma que los equipos solicitados comprenden las Oficinas Centrales y el Centro de Datos (DDOS, solo para el centro de datos) los cuales proporcionan servicio de internet en oficinas centrales por enlace MPLS y aplicativos internos en el Centro de Datos de Conagua en lo que respecta a 31 delegaciones. 4 sitios externos en la zona metropolitana y 1 en el estado de Aguascalientes – INEGI, se tiene un enlace MPLS al centro de datos de Conagua.

Pregunta 5

En caso contrario, a la pregunta anterior se le pide a la convocantes especificar el requerimiento y mencionar el total de equipos que se tendrían que proponer, para el cumplimiento de los servicios, ya que es no es claro el dimensionamiento.

Respuesta: No es correcta su apreciación, solo son dos sitios donde se prestarán los servicios, en la Oficina Central de SEMARNAT y en el Centro de Datos ubicado en las instalaciones de CONAGUA, todos los demás sitios salen a través de estos dos sitios conectados por la MPLS.

Pregunta 6

Página 55 de 131- Cartas y Certificaciones.

Dice: 2.- El licitante, deberá presentar documento donde especifique que los equipos que proporcione no tengan anuncio de fin de vida, ni anuncio de fin de mantenimiento.

Pregunta: Debemos entender que la convocante no está solicitando equipos nuevos, para la prestación de los servicios, es correcta nuestra apreciación?

Respuesta: No es correcta su apreciación, la convocante solicita que los equipos deberán ser nuevos, de última generación y que no tengan anuncio de fin de vida, ni anuncio de fin de mantenimiento.

Pregunta 7

En caso de que la pregunta anterior sea afirmativa, ¿se le solicita a la convocante reconsiderar el requerimiento, ya que al no solicitar equipos nuevos, no se está en igualdad de condiciones que el proveedor actual y afecta la competitividad de los demás licitantes.

Respuesta: La convocante aclara que no se acepta la solicitud, así mismo se informa que actualmente la SEMARNAT no cuenta con ningún proveedor para estos servicios.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 8

Punto 14 Transferencia de conocimiento Página 26-53.

Dice: "El licitante para los servicios ofertados, deberá realizar la transferencia de conocimiento para 5 persona de la solución sin tener algún costo adicional para la secretaría, así como entregar el material necesario para la capacitación.

Pregunta: Debemos entender que esta capacitación será proporcionada por el propio personal que se encargó de la implementación de la soluciones y estará definida su duración por un número de horas o cantidad de días, es correcta nuestra apreciación?

Respuesta: Es correcta su apreciación, sin embargo, no necesariamente tiene que ser el mismo personal, podrá ser alguno otro personal que el Licitante designe con los conocimientos suficientes en la solución propuesta.

Pregunta 9

Punto 16.1 Seguridad perimetral para oficina central de la Semarnat 31-53.

Dice: "El servicio deberá considerar al menor de 10 Gbps de Throughput para el servicio de firewall, 10 Gbps de Throughput para el servicio de IPS y 10 Gbps de Throughput para el servicio de VPN.

Pregunta: ¿Podría la convocante aclarar si los 10GBs de Throughput para el servicio de VPN es IPSec VPN Throughput o SSL VPN Throughput?

Respuesta: La convocante aclara que se refiere a IPSec VPN Throughput.

TOTAL PLAY TELECOMUNICACIONES, S.A. DE C.V.

Pregunta 1

Pág. 1, Numeral General

Pregunta: Solicitamos amablemente a la convocante nos proporcione los anexos y toda la documentación que surja de la presente licitación y de la junta(s) de aclaraciones en un formato editable para su mejor interpretación y respuesta, ¿Se acepta nuestra solicitud?

Respuesta: Las bases de la presente licitación no se entregarán en formato "Microsoft Word".

Pregunta 2

Pág. 2, Pág. 76 de 131 punto 18 Cronograma de trabajo

Pregunta: Es correcto interpretar que el servicio entrara en operación al día siguiente del fallo, es decir el 1 de Julio de 2017.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Respuesta: Es correcta su interpretación.

Pregunta 3

Pág. 4, Pág. 81 de 131 Numeral 26 Propuesta Económica

Pregunta: Solicitamos amablemente a la convocante nos presente un ejemplo claro para realizar el llenado del formato económica ¿Se acepta nuestra solicitud?

Respuesta: La licitante deberá presentar su propuesta económica ajustándose al formato de la pág. 81 de 131, numeral 26, propuesta económica considerando su desglose por los costos mensuales de cada uno de los 4 servicios solicitados. Se solicita ver precisión 1.

Pregunta 4

Pág. 4, Numeral Pág. 97 de 131 Anexo 8

Pregunta: En el caso de que mi representada no se encuentre dentro de la estratificación mencionada, solicitamos a la convocante permita que este documento pueda ser de carácter opcional y que el no presentarla no será motivo de descalificación, ¿Se acepta nuestra solicitud?

RESPUESTA.- La presentación de este documento es optativa, por lo que no será causa de desechamiento.

Pregunta 5

Pág. 5, General

Pregunta: Solicitamos a la convocante nos indique el presupuesto asignado para dicho proyecto

Respuesta: La convocante aclara que no es posible proporcionarle el presupuesto asignado al proyecto.

Pregunta 6

Pág. 6, General

Pregunta: Solicitamos a la convocante no mencione el nombre de la empresa que actualmente provee el servicio solicitado

Respuesta: La convocante aclara que actualmente no se tiene ningún proveedor de servicio contratado.

Pregunta 7

Pág. 7, General

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta: Solicitamos amablemente a la convocante nos indique la renta mensual que actualmente está pagando por el servicio antes de impuestos

Respuesta: La convocante aclara que actualmente no se tiene ningún proveedor de servicio contratado.

Pregunta 8

Pág. 8, Pág. 6 de 131 Acto de Presentación y Apertura de Proposiciones

Pregunta: Solicitamos amablemente a la convocante nos proporcione al menos 15 días para la elaboración y entrega de la propuesta, ¿Se acepta nuestra solicitud?

Respuesta: No se acepta su solicitud, el tiempo establecido para la presentación de proposiciones, es conforme a lo establecido en el articulo 32 segundo párrafo de "La Ley",

PRODUCTOS Y SERVICIOS EN TIC, S.A. DE C.V.

Pregunta 1

Tema: General, Pág. 77 de 131, Numeral 19

Descripción: El periodo del servicio será a partir del día siguiente de la notificación del fallo y hasta el 31 de diciembre de 2017.

Pregunta: Al tratarse de un servicio el que solicita la convocante y por el corto periodo de este, se sugiere amablemente a la convocante que los servicios puedan ser proporcionados con equipos seminuevos pero que proporcionen las funcionalidades que solicitan, esto para poder proponer mejores condiciones a la convocante, se acepta nuestra propuesta?

Respuesta: La convocante solicita que los equipos deberán ser nuevos, de última generación y que no tengan anuncio de fin de vida, ni anuncio de fin de mantenimiento.

Pregunta 2

Tema: Seguridad perimetral para Oficina Central de la SEMARNAT, Pág. 62 de 131, Numeral 16.1

Descripción: El servicio deberá contar con dispositivos basados en Appliance de propósito específico los cuales deberán contar con sistema operativo propietario con un hardening comprobable, el mismo que debe ser desarrollado íntegramente por el fabricante de los dispositivos utilizados. Adicionalmente por la alta criticidad del nodo se deberá contar con Fuentes de poder redundantes Hot-Swap, así como almacenamiento, firmware o BIOS redundantes.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta: Es correcto entender que el contar con cualquiera de los dos: Firmware o Bios redundantes será suficiente para cumplir con este requisito?

Respuesta: No es correcta su apreciación deberá de cumplir con todos los requisitos que se enuncian: el servicio deberá contar con dispositivos basados en Appliance de propósito específico los cuales deberán contar con sistema operativo propietario con un hardening comprobable, el mismo que debe ser desarrollado íntegramente por el fabricante de los dispositivos utilizados. Adicionalmente por la alta criticidad del nodo se deberá contar con Fuentes de poder redundantes Hot-Swap, así como almacenamiento, firmware o BIOS redundantes.

Pregunta 3

Tema: Seguridad perimetral para Oficina Central de la SEMARNAT, Pág. 62 de 131, Numeral 16.1

Descripción: El servicio deberá brindar soporte en un mismo dispositivo los 3 servicios de al menos de 10Gbps Throughput de Firewall, 10Gbps de Throughput de IPS y 10 Gbps de Throughput de VPN.

Pregunta: Es correcto entender que el Throughput solicitado para Firewall, IPS debera ser el de NGFW en conjunto con la VPN.

Respuesta: No es correcta su apreciación, se deberá contar con el Throughput solicitado para cada rubro, como se indica en el anexo técnico.

Pregunta 4

Tema: Firewall, Pág. 62 de 131, Numeral 16.1.1

Descripción: La solución deberá contar con un Motor de Next Generation Firewall con la certificación "Recommended" por parte de NSS Labs en las pruebas de 2016.

Pregunta: Aceptaría la convocante poder brindar los reportes del MQ de Gartner de Enterprise Firewall del 2016?

Respuesta: No se acepta su solicitud, el fabricante de la tecnología deberá aparecer en el Overall Rating como "Recomended" y con el valor de "Block Percentage" mínimo de 98% de los reportes de NSS Labs en las pruebas de 2016.

Pregunta 5

Tema: Firewall, Pág. 63 de 131, Numeral 16.1.1

Descripción: Deberá brindar un mecanismo de protección a fallas en los dispositivos de la Infraestructura de Next Generation Firewall y Prevención de amenazas que permita de forma remota actualizar, administrar y/o monitorear el equipamiento en forma independiente de la interface de administración.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta: Podría la convocante aclarar a que se refiere con mecanismo de protección de fallas?

Respuesta: La convocante aclara que se refiere a un componente integrado en la solución que permita poder accesar a los dispositivos de la Infraestructura de Next Generation Firewall y Prevención de amenazas que permita de forma remota actualizar, administrar y/o monitorear el equipamiento en forma independiente de la interface de administración.

Pregunta 6

Tema: Firewall, Pág. 63 de 131, Numeral 16.1.1

Descripción: Deberá brindar un mecanismo de protección a fallas en los dispositivos de la Infraestructura de Next Generation Firewall y Prevención de amenazas que permita de forma remota actualizar, administrar y/o monitorear el equipamiento en forma independiente de la interface de administración.

Pregunta: Podría la convocante aclarar si este componente se refiere a un OOBM (Out of Band Management)?

Respuesta: La convocante aclara que no es únicamente un mecanismo de Out-of-Band Management, sino que deberá ser un mecanismo de protección a fallas en los dispositivos de la Infraestructura de Next Generation Firewall y Prevención de amenazas que permita de forma remota actualizar, administrar y/o monitorear el equipamiento en forma independiente de la interface de administración.

Pregunta 7

Tema: Firewall, Pág. 63 de 131, Numeral 16.1.1

Descripción: A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptaran componentes de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE alimentadas por el NIST) que no hayan sido remediadas oportunamente en un plazo no mayor a 12 días naturales.

Pregunta: Aceptaría la convocante que el plazo de remediación de una vulnerabilidad crítica o de alto riesgo pueda ser en un plazo no mayor a 30 días, esto para no limitar la libre participación.

Respuesta: No se acepta su solicitud, se deberá entregar el reporte donde se valide que el fabricante ha remediado las vulnerabilidades presentadas en todas sus soluciones en un plazo no mayor a 12 días naturales en el último año.

Pregunta 8

Tema: IPS, Pág. 64 de 131, Numeral 16.1.2

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Descripción: Deberá contar el módulo de IPS con una eficiencia comprobada de un mínimo de 98% de eficiencia por parte NSS Labs de acuerdo a las pruebas de Next Generation Intrusion Prevention System de 2016.

Pregunta: Aceptaría la convocante que el el Modulo de IPS pueda contar con una eficiencia mínima del 95% por parte de NSS Labs de acuerdo a las pruebas de Next Generation Intrusion Prevention System de 2016.

Respuesta: No se acepta su solicitud, el fabricante de la tecnología deberá aparece en el Overall Rating como "Recomended" y con el valor de "Block Percentage" mínimo de 98% de los reportes de NSS Labs en las pruebas de 2016, solicitadas en el anexo técnico.

Pregunta 9

Tema: Seguridad perimetral para el Data Center (Centro de Datos), Pág. 66 de 131, Numeral 16.2

Descripción: El servicio deberá contar con dispositivos basados en Appliance de propósito específico los cuales deberán contar con sistema operativo propietario con un hardening comprobable, el mismo que debe ser desarrollado íntegramente por el fabricante de los dispositivos utilizados. Adicionalmente por la alta criticidad del nodo se deberá contar con Fuentes de poder redundantes Hot-Swap, así como almacenamiento, firmware o BIOS redundantes.

Pregunta: Es correcto entender que el contar con cualquiera de los dos: Firmware o Bios redundantes será suficiente para cumplir con este requisito?

Respuesta: No es correcta su apreciación deberá de cumplir con todos los requisitos que se enuncian: el servicio deberá contar con dispositivos basados en Appliance de propósito específico los cuales deberán contar con sistema operativo propietario con un hardening comprobable, el mismo que debe ser desarrollado íntegramente por el fabricante de los dispositivos utilizados. Adicionalmente por la alta criticidad del nodo se deberá contar con Fuentes de poder redundantes Hot-Swap, así como almacenamiento, firmware o BIOS redundantes.

Pregunta 10

Tema: Seguridad perimetral para el Data Center (Centro de Datos), Pág. 66 de 131, Numeral 16.2

Descripción: El servicio deberá brindar soporte en un mismo dispositivo los 3 servicios de al menos de 10Gbps Throughput de Firewall, 10Gbps de Throughput de IPS y 10 Gbps de Throughput de VPN.

Pregunta: Es correcto entender que el Throughput solicitado para Firewall, IPS debera ser el de NGFW en conjunto con la VPN.

Respuesta: No es correcta su apreciación, se deberá contar con el Throughput solicitado para cada rubro, como se indica en el anexo técnico.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 11

Tema: Firewall, Pág. 66 de 131, Numeral 16.2.1

Descripción: La solución deberá contar con un Motor de Next Generation Firewall con la certificación "Recommended" por parte de NSS Labs en las pruebas de 2016.

Pregunta: Aceptaría la convocante poder brindar los reportes del MQ de Gartner de Enterprise Firewall del 2016?

Respuesta: No se acepta su solicitud, el fabricante de la tecnología deberá aparece en el Overall Rating como "Recomended" y con el valor de "Block Percentage" mínimo de 98% de los reportes de NSS Labs en las pruebas de 2016 solicitadas en el anexo técnico.

Pregunta 12

Tema: Firewall, Pág. 63 de 131, Numeral 16.2.1

Descripción: Deberá brindar un mecanismo de protección a fallas en los dispositivos de la Infraestructura de Next Generation Firewall y Prevención de amenazas que permita de forma remota actualizar, administrar y/o monitorear el equipamiento en forma independiente de la interface de administración.

Pregunta: Podría la convocante aclarar a que se refiere con mecanismo de protección de fallas?

Respuesta: La convocante aclara que se refiere a un componente integrado en la solución que permita poder accesar a los dispositivos de la Infraestructura de Next Generation Firewall y Prevención de amenazas que permita de forma remota actualizar, administrar y/o monitorear el equipamiento en forma independiente de la interface de administración.

Pregunta 13

Tema: Firewall, Pág. 67 de 131, Numeral 16.2.1

Descripción: Deberá brindar un mecanismo de protección a fallas en los dispositivos de la Infraestructura de Next Generation Firewall y Prevención de amenazas que permita de forma remota actualizar, administrar y/o monitorear el equipamiento en forma independiente de la interface de administración.

Pregunta: Podría la convocante aclarar si este componente se refiere a un OOBM (Out of Band Management)?

Respuesta: La convocante aclara que no es únicamente un mecanismo de Out-of-Band Management, sino que deberá ser un mecanismo de protección a fallas en los dispositivos de la Infraestructura de Next Generation Firewall y Prevención de amenazas que permita de forma remota actualizar, administrar y/o monitorear el equipamiento en forma independiente de la interface de administración.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 14

Tema: Firewall, Pág. 67 de 131, Numeral 16.2.1

Descripción: A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptaran componentes de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE alimentadas por el NIST) que no hayan sido remediadas oportunamente en un plazo no mayor a 12 días naturales.

Pregunta: Aceptaría la convocante que el plazo de remediación de una vulnerabilidad críticas o de alto riesgo pueda ser en un plazo no mayor a 30 días, esto para no limitar la libre participación.

Respuesta: No se acepta su solicitud, se deberá entregar el reporte donde se valide que el fabricante ha remediado las vulnerabilidades presentadas en todas sus soluciones en un plazo no mayor a 12 días naturales en el último año.

Pregunta 15

Tema: IPS, Pág. 68 de 131, Numeral 16.2.2

Descripción: Deberá contar el módulo de IPS con una eficiencia comprobada de un mínimo de 98% de eficiencia por parte NSS Labs de acuerdo a las pruebas de Next Generation Intrusion Prevention System de 2016.

Pregunta: Aceptaría la convocante que el Modulo de IPS pueda contar con una eficiencia mínima del 95% por parte de NSS Labs de acuerdo a las pruebas de Next Generation Intrusion Prevention System de 2016.

Respuesta: No se acepta su solicitud, el fabricante de la tecnología deberá aparece en el Overall Rating como "Recomended" y con el valor de "Block Percentage" mínimo de 98% de los reportes de NSS Labs en las pruebas de 2016.

Pregunta 16

Tema: Consola de Administración, Pág. 70 de 131, Numeral 16.3, Punto 2

Descripción: Deberá estar basada en software, compatible para su instalación en ambientes virtualizados o servidores dedicados, mediante el cual se lleva a cabo la administración de la seguridad y reporteo de la infraestructura de los Next Generation Firewalls, de la solución perimetral, y centro de datos. Deberá centralizar la configuración y monitoreo de los dispositivos de seguridad, así como todas sus funciones de protección de red.

Pregunta: Podría la convocante aclarar qué tipo de ambientes virtualizados deberán ser soportados para la consola de Administración.

Respuesta: La convocante aclara que se deberá entender por ambientes virtualizados a las tecnologías que cuenten con Hipervisor y que son: Vmware, Hyper-V, KVM u Openstack.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 17

Tema: Consola de Administración, Pág. 70 de 131, Numeral 16.3, Punto 6

Descripción: Las comunicaciones entre la consola de administración y los dispositivos administrados deberán ser cifradas por medio de una GUI. Se podrán ofertar soluciones que usen WebUI sobre HTTPS debido a las vulnerabilidades reportadas de Cross-site-scripting (XSS), de diversos fabricantes que pueden poner en riesgo la seguridad de la Secretaría.

Pregunta: Es correcto entender que aun cuando la solución de WebUI ofertada sobre HTTPS no deberá tener reportadas vulnerabilidades medias, altas o criticas de Cross-site-scripting (XSS)

Respuesta: Es correcta su apreciación, la solución en cualquiera de sus versiones de WebUI ofertada sobre HTTPS para la administración no deberá tener reportadas vulnerabilidades medias, altas o criticas de Cross-site-scripting (XSS).

Pregunta 18

Tema: Consola de Administración, Pág. 70 de 131, Numeral 16.3, Punto 16

Descripción: A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptaran componentes de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE alimentadas por el NIST) que no hayan sido remediadas oportunamente en un plazo no mayor a 12 días naturales.

Pregunta: Aceptaría la convocante que el plazo de remediación de una vulnerabilidad criticas o de alto riesgo pueda ser en un plazo no mayor a 30 días, esto para no limitar la libre participación.

Respuesta: No se acepta su solicitud, deberá entregar el reporte donde se valide que el fabricante ha remediado las vulnerabilidades presentadas en todas sus soluciones en un plazo no mayor a 12 días naturales en el último año.

Pregunta 19

Tema: Sistema de Contención de Ataques de Disponibilidad en el Perímetro de Internet (Mitigación en Sitio) para la Oficina Central y para el Centro de Datos, Pág. 72 de 131, Numeral 16.4

Descripción: La solución deber incluir plantillas de políticas pre-configuradas para mitigar amenazas de disponibilidad de servicios.

Pregunta: Es correcto entender como por "Planilla" a configuraciones Predefinidas o bien Out-of-the-Box?

Respuesta: Es correcta su apreciación.

Pregunta 20

Tema: Capacidad y Rendimiento, Pág. 72 de 131, Numeral 16.4.1

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Descripción: El equipo deberá de tener embebido el bypass físico interno en pares de interfaces y/o en cada interface para garantizar la disponibilidad y continuidad de los servicios activándose en los siguientes casos:

- Perdida de energía eléctrica y/o
- Falla lógica en la interface de control y/o
- Pérdida de conectividad con la tarjeta madre del dispositivo y/o
- Colapso del sistema operativo.

Pregunta: Es correcto entender que el Bypass físico interno es aplicable exclusivamente a pares de interfases?

Respuesta: Es correcta su apreciación, el Bypass físico deberá contar con la capacidad de poder garantizar el flujo de tráfico (sin la protección de DDoS) en los posibles escenarios de falla mencionados en el anexo técnico.

Pregunta 21

Tema: Capacidad y Rendimiento, Pág. 72 de 131, Numeral 16.4.1

Descripción: Contar los recursos suficientes para cubrir los parámetros óptimos de operación.

Pregunta: Es correcto entender que la solución sea capaz de poder incrementar su Throughput de protección por medio de licenciamiento utilizando los recursos máximos del equipo?

Respuesta: Es correcta su apreciación, la solución deberá contar con los recursos suficientes para cubrir los parámetros óptimos de operación y que cuente con la capacidad de incrementar el Throuhput de inspección por medio de licenciamiento o crecimiento de HW.

Pregunta 22

Tema: Capacidad y Rendimiento, Pág. 72 de 131, Numeral 16.4.1

Descripción: El equipo de seguridad deberá venir respaldado con investigación y análisis global del tráfico, para poder mitigar las amenazas y vectores de ataque actuales. Por lo que el fabricante de la solución deberá contar con algún sistema de inteligencia donde se esté monitoreando las amenazas de Internet a nivel mundial y podrá proporcionar información sobre:

Botnets oDDoS

- Scans
  Phishing

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta: Es correcto entender que la solución deberá contar con la capacidad de poder ser integrada con diversas fuentes de inteligencia que se encuentre continuamente investigando y analizando el trafico global?

Respuesta: Es correcta su apreciación.

Pregunta 23

Tema: Capacidad y Rendimiento, Pág. 73 de 131, Numeral 16.4.1

Descripción: La solución propuesta deberá contar con bloqueo de tráfico malformado DNS, SIP y HTTP, Detección de fragmentación de paquetes e inundación de ICMP, Detección de inundación UDP, soporte TLS, Detección de inundación TCP SYN y/o SYN suplantados, reseteo de conexiones TCP, límite de conexiones TCP, bloqueo de tráfico basado en umbrales prevención de botnets y filtrado mediante listas para inspeccionar y bloquear tanto tráfico entrante como saliente.

Pregunta: Es correcto entender que las funcionalidades de bloqueo se refiere a que la solución deberá brindar protecciones de inundación de tráfico para la Red, Servidores y aplicaciones?

Respuesta: Es correcta su apreciación, deberá entender como bloqueo de tráfico malformado DNS, SIP y HTTP a protecciones de Aplicaciones, Detección de fragmentación de paquetes e inundación de ICMP, Detección de inundación UDP a protecciones de Red, soporte TLS como protección de Aplicación, Detección de inundación TCP SYN y/o SYN suplantados, reseteo de conexiones TCP, límite de conexiones TCP, bloqueo de tráfico basado en umbrales prevención de botnets como protecciones de Red. La solución deberá brindar protecciones para Trafico de la Red, Servidores y Aplicaciones.

Pregunta 24

Tema: Capacidad y Rendimiento, Pág. 73 de 131, Numeral 16.4.1

Descripción: El sistema deberá soportar TLS

Pregunta: Es correcto entender que el soporte a TLS se refiere a la prevención de inundación de tráfico por medio de este protocolo y que pueda ser integrado en las protecciones de Red y Aplicaciones.

Respuesta: Es correcta su apreciación.

Pregunta 25

Tema: Capacidad y Rendimiento, Pág. 74 de 131, Numeral 16.4.1

Descripción: La solución deberá contar con la capacidad de enviar eventos hacia la Consola de Administración de los dispositivos Perimetrales y DataCenter para poder correlacionar eventos.

Pregunta: Es correcto entender que la Consola de Administración de los dispositivos Perimetrales y DataCenter cuente con la capacidad de correlacionar eventos de DDoS y que puedan estar en una vista?

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Respuesta: La convocante aclara que se deberá contar con la capacidad de integrar todos los eventos de seguridad en una misma consola, de igual forma los reportes de DDoS.

Pregunta 26

Tema: Capacidad y Rendimiento, Pág. 74 de 131, Numeral 16.4.1

Descripción: A raíz de los últimos reportes de vulnerabilidades de distintos fabricantes de seguridad, se deberá entregar un reporte de las mismas que hayan identificadas el último año; no se aceptaran componentes de fabricantes que hayan tenido vulnerabilidades de mediano a alto riesgo (reportadas en SANS o CVE alimentadas por el NIST) que no hayan sido remediadas oportunamente en un plazo no mayor a 12 días naturales.

Pregunta: Aceptaría la convocante que el plazo de remediación de una vulnerabilidad críticas o de alto riesgo pueda ser en un plazo no mayor a 30 días, esto para no limitar la libre participación.

Respuesta: No se acepta su solicitud, se deberá entregar el reporte donde se valide que el fabricante ha remediado las vulnerabilidades presentadas en todas sus soluciones en un plazo no mayor a 12 días naturales en el último año.

Pregunta 27

Tema: Arquitecto líder de la solución, Pág. 56 de 131, Numeral 13

Descripción: El Arquitecto líder de la solución, deberá demostrar experiencia de al menos 5 años y contar con al menos una de las siguientes certificaciones vigentes:

Certified Incident Handler (GCIH).

- Certified Information Systems Security Professional (CISSP)
- Máxima certificación por parte del fabricante de la solución

Pregunta: Es correcto entender que el contar con cualquiera de las certificaciones será suficiente?

Respuesta: No es correcta su apreciación, deberá comprobar al menos 1 de las certificaciones mencionadas, en el caso de presentar la certificación del fabricante esta deberá garantizar un nivel de experto.

Pregunta 28

Tema: Arquitecto líder de la solución, Pág. 56 de 131, Numeral 13

Descripción: El Arquitecto líder de la solución, debera demostrar experiencia de al menos 5 años y contar con al menos una de las siguientes certificaciones vigentes:

- Certified Incident Handler (GCIH).

• Certified Information Systems Security Professional (CISSP)
• Maxima certificacion por parte del fabricante de la solucion

Pregunta: Debido a que cada fabricante maneja de diferente manera sus certificaciones, es correcto entender que para cumplir con este requisito se podrá presentar certificado del fabricante para este recurso?

Respuesta: No es correcta su apreciación, deberá comprobar al menos 1 de las certificaciones mencionadas, en el caso de presentar la certificación del fabricante esta deberá garantizar un nivel de experto.

Pregunta 29

Tema: Arquitecto lider de la solución, Pág. 56 de 131, Numeral 13

Descripción: El recurso especialista deberá demostrar experiencia de al menos 5 años y contar con al menos una de las siguientes certificaciones:

• Operational Support and Analysis (OSA).
• Service Offerings & Agreements (SOA).

Pregunta: Es correcto entender que las certificaciones solicitadas son de ITIL y que contar con cualquiera de las certificaciones de esta será suficiente?

Respuesta: La convocante solicita que el recurso especialista propuesto por el licitante deberá contar con al menos una de las dos certificaciones mencionadas en la Pág. 56 de 131, Numeral 13.

Pregunta 30

Tema: Arquitecto lider de la solución, Pág. 56 de 131, Numeral 13

Descripción: El recurso especialista deberá demostrar experiencia de al menos 5 años y contar con al menos una de las siguientes certificaciones:

• CISA, emitido por Information Systems Audit and Control Association (ISACA), centro de educación acreditado o equivalente.

• ISO/IEC 27001, emitido por Internacional Standard Organization (ISO/IEC), centro de educación acreditada o equivalente.

Pregunta: Es correcto entender que el contar con cualquiera de las certificaciones será suficiente?

Respuesta: La convocante solicita que el recurso especialista propuesto por el licitante deberá contar con al menos una de las dos certificaciones mencionadas en la Pág. 56 de 131, Numeral 13.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

INDRA SISTEMAS MEXICO, S.A. DE C.V.

Pregunta 1

Tema: GENERAL. g) Propuesta técnica (ANEXO 1 "Especificaciones Técnicas"), inciso 4. Página 13

Pregunta: ¿Es correcto entender que la traducción simple indicada por la convocante, deberá ser solamente del apartado en donde se esté haciendo referencia a una característica técnica de la propuesta del licitante y no de todo el documento?

Respuesta: Es correcta su apreciación.

Pregunta 2

Tema: GENERAL. 8.1.1 Actividades de la fase de Diseño e Implementación Planeación y Diseño, párrafo 1. Página 41

Pregunta: ¿Es correcto interpretar que los procesos se realizaran en conjunto con el personal de la Convocante en mesas de trabajo antes de tomar la operación, con el fin que estos procesos estén alineados?

Respuesta: Es correcta su apreciación.

Pregunta 3

Tema: GENERAL. 8.1.1 Actividades de la fase de Diseño e Implementación, bullet Configuración, sub bullet Entregables. Página 42

Pregunta: Se indica el entregable "Memoria técnica de la solución implementada" ¿Es correcto entender que la licitante hará entregara de la plantilla que debe utilizar el licitante para este entregable, así como el contenido que explícitamente debe contener el documento? o bien el formato y contenido es libre.

Se solicita a la convocante indicar si la respuesta anterior aplicará para todos los documentos mencionados en el presente documento de bases de licitación

Respuesta: El licitante deberá apegarse a lo establecido en el Anexo Técnico, punto 10 "Solución Requerida", numeral 10, así mismo se informa que el formato podrá ser libre así como el formato de todos los documentos solicitados en las bases de este documento.

Pregunta 4

Tema: GENERAL. 8.1.1 Actividades de la fase de Diseño e Implementación, bullet Pruebas y Validación, sub bullet Entregables. Página 43

Pregunta: ¿Es correcto interpretar que el licitante ganador deberá notificar vía correo electrónico a la cuenta o lista de distribución que la Convocante proporcione como oficial?

Respuesta: No se entiende la pregunta, favor de replantearla.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 5:

Tema: GENERAL. 8.1.1 Actividades de la fase de Diseño e Implementación, bullet Afinación y estabilización. sub bullet Entregables. Página 44

Pregunta: ¿Es correcto entender que la Convocante nos hará entregara de la plantilla que debe utilizar el proveedor, así como el contenido que requiere explícitamente? o bien el formato y contenido es libre.

Respuesta: El licitante podrá entregar un formato libre los documentos solicitados, sin embargo deberá estar alienado al objetivo del contenido solicitado.

Pregunta 6

Tema: GENERAL. 8.1.1 Actividades de la fase de Diseño e Implementación, bullet Afinación y estabilización. sub bullet Notificación. Página 44

Pregunta: Para sub bullet Notificación ¿Es correcto entender que el licitante ganador debe notificar vía correo electrónico a la cuenta o lista de distribución de la Convocante que indiquen como oficial?

Respuesta: La No se entiende la pregunta, favor de replantearla.

Pregunta 7:

Tema: GENERAL. 8.3.1 Actividades de la fase de Operación, bullet Administración, párrafo 1. Página 44

Pregunta: Se solicita amablemente a la convocante, indique cuál es el horario laboral con el que opera la Convocante

Respuesta: La convocante indica que el horario laboral es acorde a las necesidades de los usuarios de la Secretaria, sin embargo el soporte que se deberá proporcionar será 7X24

Pregunta 8:

Tema: GENERAL. 8.3.1 Actividades de la fase de Operación, bullet Administración, párrafo 2. Página 45

Pregunta: ¿Es correcto interpretar que la Convocante fungirá como el primer nivel de soporte para todos los sitios y será quien escale con la Licitante los problemas y afectaciones del servicio correspondientes al 2o y 3er nivel? En caso contrario, favor de acotar

Respuesta: Es correcta su apreciación.

Pregunta 9:

Tema: GENERAL. 11 Niveles de servicio, 11.1 Atención a incidentes, Tabla 1. Página 52

Pregunta: ¿Es correcto interpretar que los niveles de severidad deben de considerarse con base a los tiempos de atención/resolución, indicados en la tabla de la página 53 correspondiente al punto 11.3 Administración de Incidentes Reportes de fallas?

Respuesta: Es correcta su apreciación.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES
Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017
"Servicios administrados de seguridad perimetral"

Pregunta 10:

Tema: GENERAL. 11 Niveles de servicio, 11.1 Atención a incidentes, Tabla 1

Pregunta: Se solicita a la Convocante pueda explicar con detalle la actividad de "Solicitud de requerimiento", ya que en la tabla de la página 52 se le asigna un valor de Severidad 1 a esta actividad y en la tabla de la página 53, se le asigna un valor de Severidad 4. Página 52

Respuesta: La convocante aclara que los niveles de severidad deberán de ser asignados de acuerdo a lo expresado en la tabla de la página 53.

Pregunta 11:

Tema: GENERAL. 11.3 Administración de Incidentes, Reporte de fallas. Página 53

Pregunta: ¿Es correcto entender que el tiempo de detección/notificación y el tiempo de atención/resolución se suman para obtener el tiempo total del ciclo de vida del ticket y con ello el SLA total?

Se solicita a la convocante pueda proporcionar un ejemplo con Severidad 1.

Respuesta: Es correcta su apreciación, el incidente de severidad 1 será cuando el servicio deje de proporcionar conexión a internet a todos los usuarios de la RED.

Pregunta 12:

Tema: GENERAL. 13. Cartas y Certificaciones, tablas de perfiles especializados, Especialista en alineación de servicios. Página 56

Pregunta: Solicitamos amablemente a LA CONVOCANTE, si se acepta que se pueda presentar la certificación Itil v3 Expert, siendo está de mayor nivel a las solicitadas por LA CONVOCANTE?

Respuesta: El licitante deberá apegarse a lo establecido en el Anexo Técnico.

Pregunta 13:

Tema: GENERAL. 13. Cartas y Certificaciones, tablas de perfiles especializados, Especialista gobierno de la seguridad de la información en ASI, OPEC de MAAGTICSI. Página 57

Pregunta: Se propone a la convocante que la demostración de certificación pueda provenir de personal perteneciente a la plantilla de trabajadores de la Licitante. ¿Se acepta la propuesta?

Respuesta: Se acepta su propuesta, la demostración de certificación podrá provenir de personal perteneciente a la plantilla de trabajadores de la Licitante

Pregunta 14:

Tema: FIREWALL 16.1 Seguridad Perimetral para oficina Central de la Semarnat, bullet 1. Página 62

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta: Considerando que la infraestructura solicitada se encontrará configurada en un esquema de alta disponibilidad, ¿Es correcto interpretar que el almacenamiento, firmware o BIOS redundante hace referencia al esquema de conectividad en Alta Disponibilidad y que la convocante no se refiere a características individuales? Favor de comentar

Respuesta: No es correcta su apreciación, se requieren las funcionalidades descritas de Fuentes de poder redundantes Hot-Swap, almacenamiento redundante y Firmware o BIOS redundante por cada dispositivo propuesto.

Pregunta 15:

Tema: IPS Y PREVENCION DE AMENAZAS 16.1.2 IPS y Prevención de amenazas, bullet 4. Página 64

Pregunta: Se solicita a la convocante, permita realizar una propuesta de equipamiento que no incluya el análisis del protocolo SMB. ¿Se acepta la propuesta?

Respuesta: Los protocolos que deberán soportar deberán ser al menos los siguientes: HTTP, SMTP, IMAP, POP3, FTP, SMB o CIFS.

Pregunta 16:

Tema: CONSOLA DE ADMINISTRACIÓN. 16.3 Consola de Administración, bullet 3. Página 70

Pregunta: Se solicita amablemente a la convocante, proporcione una breve descripción respecto al punto referido, a fin de contar con una mejor perspectiva sobre funcionalidad solicitada

Respuesta: La convocante aclara que la consola deberá tener la capacidad de poder graficar el tipo de tráfico existente en la red.

Pregunta 17:

Tema: CONSOLA DE ADMINISTRACIÓN. 16.3 Consola de Administración, bullet 6. Página 70

Pregunta: La consola propuesta por Indra se maneja cifrada por medio de una GUI, la cual no cuenta con administración Web por HTTPS, sino que funciona por medio de Java. ¿Se acepta la propuesta?

Respuesta: No se acepta su propuesta, la consola podrá estar basada en cualquier lenguaje de programación, aclarando que la convocante no aceptara soluciones de fabricantes que presentaron vulnerabilidades de XSS (Cross-Site Scripting).

Pregunta 18:

Tema: PROTECCIÓN CONTRA DDoS. 14. Sistema de contención de ataques de disponibilidad en el Perímetro de Internet (mitigación en sitio) y para el Centro de Datos. Página 71

Pregunta: Se solicita a la Convocante indicar si en alguno de los sitios será necesario considerar un esquema de alta disponibilidad, si las condiciones de infraestructura así lo permiten

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES
Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017
"Servicios administrados de seguridad perimetral"

Respuesta: La convocante aclara que no se requiere.

Pregunta 19:

Tema: PROTECCIÓN CONTRA DDoS. 14. Sistema de contención de ataques de disponibilidad en el Perímetro de Internet (mitigación en sitio) y para el Centro de Datos. Página 71

Pregunta: Se solicita amablemente a LA CONVOCANTE indicar sí es posible que la misma solución de Firewall e IPS pueda brindar la funcionalidad de Protección contra DDoS, o si está se debe proponer de propósito específico?

Respuesta: La convocante aclara que el Sistema de Contención de Ataques de Disponibilidad en el perímetro de internet deberá ser una solución de propósito especifico.

Pregunta 20:

Tema: PROTECCIÓN CONTRA DDoS. 16.4.1 Capacidad y Rendimiento, bullet 23. Página 74

Pregunta: ¿Es correcto interpretar que la Convocante cuenta actualmente con equipamiento de correlacionador de eventos en operación y que será a este equipamiento hacia donde se enviarán los logs de los equipos de protección DDoS? En caso contrario, favor de acotar.

Respuesta: No es correcta su apreciación, se refiere a la consola de administración de los servicios solicitados en este anexo.

Pregunta 21:

Tema: GENERAL 17 Lugar, tiempo y Control de entrega de los Servicios, bullet 6. Página 75

Pregunta: Se solicita amablemente a la convocante, indique si cuenta con un pronóstico de reubicaciones que tenga programadas para reubicación de domicilio de alguno de los sitios que componen la presente Convocatoria.

Respuesta: No se cuenta por el momento con alguna reubicación programada.

Pregunta 22:

Tema: GENERAL 17 Lugar, tiempo y Control de entrega de los Servicios, bullet 7. Página 75

Pregunta: ¿Es correcto interpretar que la herramienta indicada deberá ser operada exclusivamente por la Licitante y la Convocante solo tendrá reportes mensuales de las actividades registradas? En caso contrario, favor de acotar.

Respuesta: Es correcta su apreciación.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 23

Tema: 17 Anexo Técnico. Página 49

Pregunta: ¿Cuál es el alcance del programa de evaluaciones del SGSI de SEMANRNAT?

Respuesta: El programa será presentado al licitante ganador y está alineado a lo establecido en MAAGTICSI

Pregunta 24

Tema: 17 Anexo Técnico. Página 49

Pregunta: ¿Qué compone el catálogo de activos de información e infraestructura clave de SEMARNAT?

Respuesta: El catalogo será presentado al licitante ganador y está alineado a lo establecido en MAAGTICSI

Pregunta 25

Tema: 17 Anexo Técnico. Página 49

Pregunta: ¿Cuál es el alcance considerado para la evaluación de riesgos?

Respuesta: Deberá estar considerado de acuerdo a lo establecido en MAAGTICSI

Pregunta 26

Tema: 17 Anexo Técnico. Página 50

Pregunta: ¿Qué metodología o marco de seguridad informática se deberá de considerar en los procesos y guías de operación para la atención de incidentes de seguridad perimetral?

Respuesta: Deberá apegarse a lo establecido en el MAAGTICSI

SCITUM S.A. DE C.V.

Pregunta 1

Tema: General,

Pregunta: Se solicita a la convocante, comparta el archivo de esta licitación en formato Word, con el objetivo de facilitar a los licitantes las actividades de referenciación y de lectura del mismo.

Respuesta: Las bases de la presente licitación no se entregarán en formato "Microsoft Word".

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 2

Tema: General,

Pregunta: Se solicita a la convocante, comparta la tabla de los mecanismos de evaluación de puntos y porcentajes en formato Word ya que no se aprecia la lectura.

Respuesta: Las bases de la presente licitación no se entregarán en formato "Microsoft Word".

Pregunta 3

Tema: General,

Pregunta: Solicitamos a la convocante explique y aclare lo siguiente:

En el supuesto de que algún participante, al no contar con trabajadores, no se ubique en el supuesto señalado por el artículo 15 de la Ley del Seguro Social y sus correlativos del reglamento sustantivo, y consecuentemente no se considere como sujeto obligado para efectos de ninguno de los supuestos señalados en Acuerdo ACDO.SA1.HCT.101214/281.P.DIR y, aunado a lo anterior, el participante cuente con opinión emitida por el IMSS respecto a la improcedencia del tema materia del presente cuestionamiento, precisando que podrá presentarse la acreditación ante el IMSS por parte de un tercero que no sea subcontratación, solicitamos a la convocante señale como procederá para facilitar la suscripción contractual en la hipótesis comentada.

RESPUESTA.- Deberá presentar la opinión de cumplimiento de obligaciones en sentido favorable de que se encuentra al corriente en sus obligaciones en MATERIA DE SEGURIDAD SOCIAL de la empresa que tiene contratado al personal.

Pregunta 4

Tema: General,

Pregunta: Se solicita a la convocante precise y aclare a ¿qué se refiere con LPP en la tabla de mecanismos de evaluación a través del criterio de evaluación de punto y porcentajes?

Respuesta: La convocante menciona que LPP es el Administrador del Proyecto del licitante.

Pregunta 5

Tema: General,

Pregunta: Debido a que el objeto de esta licitación es un servicio administrado, ¿puede la convocante confirmar que el licenciamiento, software, hardware, pólizas de soporte y mantenimiento de todos los componentes que integremos en nuestra propuesta, podrá estar a nombre del licitante ganador?, ¿y que no será necesario que este a nombre de la convocante?

Respuesta: Los servicios solicitados se requieren como servicios administrados, se aclara a la convocante que el modelo de requerimiento solicitado es de servicios administrados por lo que la SEMARNAT recibirá únicamente los servicios que se generen.

SEMARNAT
SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

DIRECCIÓN DE ADQUISICIONES Y CONTRATOS

ACTA DE REINICIO DE LA JUNTA DE ACLARACIONES

Licitación Pública Nacional Electrónica
No. LA-016000997-E51-2017

"Servicios administrados de seguridad perimetral"

Pregunta 6

Tema: Página 40 Fase de habilitación del servicio

Pregunta: Se solicita a la convocante amplíe el tiempo de la fase de diseño e implementación a por lo menos 8 semanas, debido a que el tiempo de entrega de los fabricantes en equipos nuevos es de 4 a 6 semanas y no se alcanzaría a cubrir la implementación.

Respuesta: El licitante deberá apegarse a lo establecido en el Anexo Técnico.

Pregunta 7

Tema: Página 43 Punto 8.2

Pregunta: ¿Es correcto interpretar que para la fase de transición y estabilización se refiere a una semana adicional a la fase diseño e implementación?, ya que en tabla de la página 77 Cronograma de Trabajo solo se marcan 4 semanas para estas 2 fases.

Respuesta: La convocante aclara que la fase de transición y estabilización deberá ser ejecutada en la semana 4 en paralelo a la última semana de la fase de diseño e implementación.

Pregunta 8

Tema: Página 48 Punto 10.1 Alineación a Normatividad y Procesos, Para el proceso ASI

Pregunta: Es correcto interpretar que la persona especialista en gobierno de seguridad de la información en ASI y OPEC de MAAGTICSI es la misma persona que se solicita en Página 55 LA TABLA DE PERFILES ESPECIALIZADOS "Especialista en gobierno de seguridad de la información en ASI OPEC de MAAGTICSI.

Respuesta: Es correcta su apreciación.

Pregunta 9

Tema: Página 55 Punto 13 Cartas y Certificaciones

Pregunta: Debido a que el representante legal de las marcas para los servicios solicitados no están en México y el proceso de firmas tarda hasta 3 semanas, se solicita a la convocante acepte que las cartas sean firmadas por el representante comercial o representante de la marca en México. ¿Se acepta nuestra propuesta?

Respuesta: La convocante aclara que deberá apegarse al punto 13 Cartas y Certificaciones del presente documento.

Pregunta 10

Tema: Página 74 Punto 16.5 Mesa de servicios