HACIENDA

SOCIEDAD HIPOTECARIA FEDERAL

Oficio referencia: 2023 01 041 DTI

Ciudad de México, a 25 dc encro dc 2023

Mtro. Juan Jaime Molina Vélez.
Director General Adjunto de
Administración y Operaciones

RFCURSCi'3

La Dirección de Tecnologías de Información, ha resuelto con esta fecha adjudicar la presente contratación al proveedor que a continuación se indica; determinando conveniente realizar un procedimiento de excepción a la licitación pública para la Continuidad del Servicio Administrado dc Telecomunicaciones, por IO que solicito su apoyo para llevar a cabo su formalización de acuerdo con Io siguiente:

En términos de lo dispuesto por la fracción I del artículo 71 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, mc permito hacer de su conocimiento que los servicios a contratar deberán cubrir las siguientes especificaciones/datos técnicos y cantidades:

Ladescripción dc los servicios a contratar se detalla en el "Anexo Técnico", adjunto a esta solicitud.

Para tales efectos, los plazos para la prestación de los servicios serán los siguientes:

I,os servicios solicitados en el presente documento tendrán un periodo de vigencia a partir del día siguiente de la notificación de la adjudicación y hasta el 31 de diciembre de 2024.

Las condiciones para la entrega de los servicios serán las siguientes:

La entrega de los servicios deberá atender a Io establecido en la sección correspondiente en cl "Anexo Técnico", adjunto a esta solicitud.

Investigación de mercado.

Se adjunta documento con investigación de mercado correspondiente.

Procedimiento de contratación solicitado.

Adjudicación directa, bajo la modalidad de contrato abierto plurianual, con fundamento en Io dispuesto por cl artículo 41, fracción I II y 47 de la ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y con base en lo establecido en los artículos 72 fracción I II y 85 de su Reglamento, así como en el artículo 50 dc la Ley Federal de Presupuesto y Responsabilidad llaccndaria y 148 de su Reglamento.

Motivación del supuesto de excepción.

Actualmente se cuenta con un contrato de Servicio Administrado de Telecomunicaciones, que consiste en proporcionar servicios de voz, datos y video, a través dc los enlaces de comunicación e internet, utilizando mecanismos de seguridad y de administración de tráfico en la transmisión de la información, adjudicado a OPERBES S.A. de C.V.

Para la renovación de dichos servicios y después de analizar los contratos marco correspondientes a INTERNET CORPORATIVO y ARRENDAMIENTO DF. EQUIPO DE SEGURIDAD FIREWAI„I. Y NAC, emitidos por la Secretaría de Hacienda y Crédito Público y la Coordinadora de Estrategia Digital Nacional, la Dirección de Tecnologías de la Información de SEF (DTI) identificó por un lado, que los aspectos técnicos críticos que soportan los niveles óptimos de disponibilidad de nuestras operaciones y la redundancia de los mismos estarían comprometidos al no contar, el contrato marco de Internet Corporativo, con este diseño de arquitectura para mantener la disponibilidad, confidencialidad e integridad de los servicios del Banco, con Io que se podrían enfrentar penalizaciones por parte de los órganos reguladores como son CNBV, BANXICO e INDEVAL (en específico a lo que respecta a las operaciones que se realizan a través de los aplicativos SPEI y MEDUSA), y por el otro, que los servicios de seguridad perimetral y control de acceso a la red, incluidos en el contrato marco de Seguridad Firewall y NAC, cubrían sólo una parte de las especificaciones técnicas requeridas por SHF. Para ambos servicios no se contemplaba los servicios administrados necesarios.

Es por lo anterior que, al no contar con contratos marco que contemplen la totalidad dc los servicios requeridos y a fin de preparar la información que definiera con precisión las necesidades de la Institución en esta materia y realizar las gestiones necesarias para convocar la licitación correspondiente, la DTI gestionó una primera ampliación del Contrato con vigencia al 30 de noviembre de 2021.

Las gestiones realizadas para llevar a cabo la contratación del Servicio Administrado de Telecomunicaciones, mediante el procedimiento de Licitación Pública, a efecto de obtener las mejores condiciones de contratación para la Institución, se iniciaron a partir del mes de julio de 2021, mediante la realización del estudio de mercado, a través del cual se invitó a participar

principalmente a las empresas que participan en los contratos marco vigentes relacionados con la materia.

Como resultado de dicha investigación de mercado, se integró el expediente de contratación correspondiente, y con fecha 7 de septiembre del 2021, se presentó el Oficio 202109007DTl mediante el cual sc solicitó al Órgano Interno de Control la opinión favorable del Estudio dc Factibilidad, en el que se acompañó la Justificación dc Plurianualidad, a través dc la herramienta denominada Gestión de la Política TIC de Presidencia, obteniendo el Dictamen favorable mediante oficio OIC-SHF-064/ZOZI, de fecha 17 de septiembre de 2021.

Derivado de Io anterior, el lunes 20 de septiembre de 2021, la Dirección de Tecnologías de la Información solicitó, a través de la misma herramienta, el Dictamen Técnico por parte dc la Coordinación dc Estrategia Digital Nacional, la cual solicitó con fecha 11 dc octubre dc 2021, información adicional, para poder emitir la opinión favorable correspondiente.

Lo anterior resulta relevante, toda vez que, mediante oficio NO. 307-a.-1896, de fecha 01 de octubre del 2021, la Secretaría de Hacienda y Crédito Público hizo del conocimiento a las Unidades dc Administración y Finanzas de las Dependencias de la Administración Pública Federal las "Disposiciones Específicas para el cierre del ejercicio presupuestario 2021" (Disposiciones), en el que señaló que los ejecutores del gasto no podrán iniciar procedimientos de contratación después del 11 de octubre de 2021, conforme Io dispuesto en el numeral 6 del apartado "Fechas límite" de las referidas Disposiciones.

En ese orden de ideas, considerando la solicitud de información adicional por parte dc la Coordinación dc Estrategia Digital Nacional, dc fecha II de octubrc dc 2021, y toda vez que cl mismo 11 de octubre de 2021 fue la fecha límite para iniciar procedimientos de contratación, se determinó que ya no resultaba viable continuar con el proceso de contratación correspondiente, dada la restricción para iniciar un procedimiento de licitación pública.

No se omite señalar que con fecha 6 de septiembre de 2021, la Presidencia de la República publicó en el Diario Oficial de la Federación el "ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal" (Acuerdo), mediante el cual, entre otros temas, se modificó el procedimiento para la gestión de los pronunciamientos por parte de los Órganos de Control y Fiscalización dc las Instituciones y de la Coordinación de Estrategia Digital Nacional, y con ello, cl proceso para solicitar la emisión del Dictamen Técnico favorable.

Asimismo, mediante sesiones de trabajo, convocadas por la misma Coordinación de Estrategia Digital Nacional, se establecieron los períodos para el envío y visto bueno al POTIC 2022 (Portafolio de proyectos de Tecnologías de la Información y Comunicación), en las que se definió como fecha límite para la presentación de los proyectos a ejecutarse cn cl primer trimestre dcl ejercicio 2022,

el día 06 de octubre de 2021; y el 29 de octubre de 2021 para la presentación de los proyectos a ejecutarse a partir del segundo trimestre del ejcrcicio 2022.

Consecuentemente, y toda vez que resulta necesaria la obtención del Dictamen Técnico favorable por parte de la Coordinación de Estrategia Digital Nacional, para estar en posibilidad de llevar a cabo el procedimiento de contratación correspondiente, con las particularidades y especificaciones requeridas por SHF, y considerando que la prestación de dichos servicios no podrían ejecutarse en el primer trimestre del ejercicio 2022, se determinó instrumentar el procedimiento de contratación antes referido, en el segundo trimestre del ejercicio 2022.

Derivado de lo anterior, la Dirección de Tecnologías de la Información incluyó dentro del POTIC 2022, el procedimiento de contratación mediante licitación pública, a ejecutarse a partir del segundo trimestre del ejercicio 2022, el cual se registró en la Herramienta de Gestión, con el identificador SHF-2022-O-000077, que fue aprobado a través de la misma Herramienta, por lo que se iniciaron las acciones correspondientes a fin de elaborar un nuevo Estudio de Mercado y solicitar la aprobación del Dictamen Técnico, lo que implicaría un tiempo aproximado de 60 días, para posteriormente convocar al proceso de licitación que tomaría un tiempo aproximado de 45 días para contar con un proveedor adjudicado que podría entonces iniciar el proceso de implementación, el cual podría requerir entre dos y tres meses, por lo que de manera paralela sc ejecutaron las acciones necesarias para dar continuidad a los servicios mediante un proceso de adjudicación directa temporal.

Todo lo anterior resulta relevante, toda vez que, no obstante que se ejecutaron las acciones necesarias para realizar un procedimiento dc licitación pública para llevar a cabo la contratación de los servicios de telecomunicaciones, con las características, especificaciones y particularidades requeridas por SliF, se presentaron diversas situaciones, todas ellas ajenas a la SIIF, que imposibilitaron su instrumentación conforme las proyecciones y plazos estimados para tales efectos; i) Considerando la fecha en que se recibió la solicitud de información adicional por parte de la Coordinación de Estrategia Digital Nacional (II de octubre de 2021); ii) Considerando la restricción establecida por parte de la SHCP, para iniciar procesos de contratación para el ejercicio 2021, después del día II de octubre de 2021; y iii) Considerando que el día 06 de octubre dc 2021 fue el último día para registrar en el POTIC 2022, la presentación de los proyectos a ejecutarse en el primer trimestre del ejercicio 2022; situaciones todas ellas que obligaron a retrasar el proceso de contratación al segundo trimestre dc 2022.

En materia de continuidad operativa, en el Plan de Recuperación de Desastres (DRP) sc cstablcccn los procedimientos necesarios para recuperar los Servicios Críticos de Tecnologías de Información y Comunicaciones de una forma rápida y efectiva ante una interrupción de los mismos; motivo por cl cual, cs imprescindible contar con los servicios administrados de conectividad y seguridad, para estar en condiciones de brindar soporte al DRP al presentarse cualquier interrupción de los servicios críticos de TIC, a fin de garantizar el restablecimiento del correcto funcionamiento dc los

servicios de TIC necesarios para operar los procesos críticos de SHF, en el menor tiempo posible, ante cualquier eventualidad.

También se busca asegurar la capacidad de operación de los procesos críticos de SHF ante algún evento que interrumpa la operación normal; reducir la probabilidad de pérdidas para SIIF, a un mínimo de nivel aceptable y a un costo razonable, en caso de presentarse alguna contingencia o desastre, considerando la protección y conservación de los activos de TIC de SIIF de riesgos y asegurar que existan los controles de seguridad adecuados para reducir el impacto en caso de materializarse los riesgos a los que está expuesta SHF, cs de suma importancia para la Institución.

Los escenarios que contempla el DRP, están dirigidos a mantener los Servicios de TIC que soportan la operación crítica de SIIF, Seguro de Crédito a la Vivienda y el Fondo de Operación y Financiamiento Bancario a la Vivienda, como son los procesos de tesorería y mercado de dinero, derivados, crédito de corto y largo plazo, seguro de crédito a la vivienda y el de garantía por incumplimiento en caso de fallas en la tecnología, o por instalaciones principales inaccesibles o por destrucción o inoperatividad de las instalaciones principales o de pérdida de integridad o de la disponibilidad de la información, conforme al resultado del análisis de impacto al negocio y que fueron definidos por SHF.

Dada la importancia que representa para Sociedad Hipotecaria Federal la conectividad, seguridad perimctral y control de acceso a la red de internet, a fin de proteger los activos de informaciones institucionales y de esta forma evitar riesgos que afecten la continuidad de los planes y operaciones institucionales, es muy importante mantener los servicios actuales.

Cabe señalar que, de no llevarse a cabo la contratación de los Servicios Administrados de Telecomunicaciones, se generarían consecuencias graves a la operación general de la institución e incluso las áreas críticas tendrían un impacto cuantificable como se establece cn el Plan de Continuidad de Negocio en su Anexo 12.16. Estimación de Impactos, en el punto 8. Incidencias en el Negocio y fallos en los sistemas, Servicios informáticos y/o comunicaciones suspendidas sin reemplazo hasta por un promedio de 5.22 millones de pesos mensuales por cada uno dc los riesgos asociados a los 33 procesos críticos, por Io que en caso de materializarse este riesgo, el impacto estimado ascendería a un monto de 172.26 millones de pesos mensuales, pudiendo reflejarse además en faltas graves en los cumplimientos de metas, en entrega de información a entidades regulatorias y/o supervisoras, falta u omisión en dispersiones de flujos de efectivo o pagos comprometidos, etc.

Los procesos críticos identificados en el Plan de Continuidad de Negocio que se verían afectados son los siguientes:

Macro rocesos	Procesos	Sub rocesos	Dirección Subdirección
(-•rédito	Ct•édito Corto y l,,lrgo Plazo (Individual y :nte) Crédito Elltidades Financieras como Fiduciarias Sindicado	Adlllinistración - Dispersión de Recursos	SD de Mesa de Control de Crédito
		Adnlinistración Facturación	SI) de Operación) de Crédito SI) de Gestión de Cobranza SD de 'eraciones de 'l'esoret'ia
		Prepagos	SI) de ()peraciólll de C."édito SI) de O)eraclones de •l'esoreri,t

	Crédito Esquenta I	Devolución del Margen ,'i la Entidad Financiera	SI) de Gestión de

	Crédito Sinciicado	Gest!óti de Cobranza Conlisi0111Sta	SI) de Gestióll (le Cobranza
	Crédito Respaldos M Crédito Ret110delacicin Clí•dito FOVI Crédito FtiVl ler Ïu Casa y acción / para Re:lta l'iso	Autofi7ación para Ia devolucióll dei margen comisionista al desarrollador •	SI) de Gestion de Cobranza
	Garantías	Cobro de Prima	SI) de ()peraciótl de Seguros y Gar,lttti.is SI) de (;estiOn dc SI) de O »eracaottes •rcsoreria
		Reclamación de Ga l•antía	SI) de Operació'i de Seguros y de SI) de y Pérdidas SI) de Operac•ones de 'l'esol•eria
	Seguro de Crédit Vivienda	Administración Contraprestación Cobro	SI) de ()peraciót' de Seguros y titi.1S SI) de Gestion de Cobra 117.a SI) de ()per.iC1011es de 'l'esorcria
		Reclamación de Seguro	SI) de Reclalllaciolles y Mitigaü(in de Pérdidas SI) de Operaci011es de Tesot•eria
	Minintos. SWA UDIs SWAP Salarios	Control Ope Cobro de Intercambio ('perativo - Cálculo Cotnisión	SI) de Operacióll de Segul•os y (iarallti,is SI) de Gesti(in de Cobranza SI) de Operaciones de Tesorría
		Pt•oyecf'ión de Flujos	SI) de Estructlll•acióll y Derivados
		Valuación Cobertura y l.iquidación de Ia	SD de y Derivados de Aditiin:stración de Financieros SD de Operaciones de Tesoreri'l

Macto	Procesos	Sub)rocesos	Dirección Subdirecclón
	Tesoreria	i'.tectivo	SI) de Fin'tll' SD cle Inversiont.•s Dirección de Tesoretáa y Mercados Financieros de O eraci01tes Tesorerla
		Emisiones - Colocación de Deuda (PRLV'S) de 'l'itulos	SD de Filiancianuetlto SD de O 'eraciotli_", de Tesoreria

HACIENDA

		Emisiones – Coloc de Deuda (CEDE'S	Colocacióll de Títulos	SD de Financiamiento Dirección de Tesorería y Mercados Financieros SD de Operaciones de Tesorería
		Cliente', de	- Inversión	SD de Inversiones cle de Tesoreria
		Clientes Liquidación	de Tesoreria	de Operaciones de •re•sorevia
		at 'orles Tesoreria Mesa de l).nero -		S!) de Inversione:s)eraciones
		Operaciones Tesorería Mes Dinero - Operaciones a Plazo	Mesa de	SI) de Inversiones SI) de O)eraci011es
		Operaciones Dinero – Sa Money (MXN	Tesorería Mesa de Saldos Tardios y Call	SI) de Inversiones SI) de Oper.1ci01)es de
		Operaciones Tes Dinero - Subastas	Tesoreriii Mesa de	SI) de Inversiones
		()peraciones Tesorería Mesa de l)inet o	Incunlptiltuento de	SI) de Inversiones SI) de ()peraciolles 'lesorerla
		Money en Dólares		SI) de Tesorería Inter'iacion.il SI) de O 'eraciones de
		Divisas • Conlpraventa de Divisas Organismos Multilaterales	Financieros • Antottlzaclón	SD de Tesorería Internacional SD (le (i'jeraciones de Tesorería de •l•esoreria Intern SI) de 'eracioli'.•s de 'l'esoreria
		Concertación	de Operaciones	SI) (le Estructuración y ración de y Derivados SI) de Adnlinist Financieros SI) de C) leraciones de 'l'.•soreri'/
	Derivados	Operaciones	Extraordinarias	SD de Estructuración y Derivados SD de Administración de Financieros SD de Tesorería Internacional SD de Operaciones de Tesorería Dirección de Consultoría Jurídica Riesgos
		l.iqtl'd.wion de operaciones		(le Operaciones 'l•esorevia de Adtninistr
			en Electivo en Pesos y A:ltericalios	SI' de Operaciones de Tesorelia
		Entrega Gubernamentales	de valores conto Garantía	SI) Operaci011es de SD (ie lli%'ersi01ieS
Administración	Eitl,incieros	Pagos litvitucionales		Dirección de Administración SI) de Presupuesto de (:ontabilidad Unidad Fiduciaria y Fisca SI) de O Jetacione:, de Tesoret'ia
			rclinliellto de Operacióti Altet no ;'ara el seA'icio SI'EI	SI) de Operaciones de Tesoreri"

Ante esta situación, y con la finalidad de garantizar la continuidad de la operación de la Institución y no afectar los procesos críticos de la misma, resulta indispensable llevar a cabo la contratación de la prestación de los servicios que se propone, por un periodo de vigencia a partir del día siguiente de la notificación de la adjudicación y hasta el 31 de diciembre dc 2024, con la finalidad de: i) evitar la interrupción de la operación de la Institución; ii) evitar la afectación en los procesos críticos antes referidos con el riesgo incluso dc afectar el cumplimiento del objeto social de la Institución, sus objetivos y programas nacionales y sectoriales; iii) evitar las pérdidas y costos adicionales que podrían generarse con la interrupción del servicio; iv) evitar el riesgo de incumplir las distintas disposiciones en materia de seguridad de información emitidas por Banco de México, Indeval, Comisión Nacional Bancaria y de Valores y la Comisión Nacional de Seguros y Fianzas, v) ' ! continuar contribuyendo al fortalecimiento de control interno institucional.

Asimismo, como resultado de la Investigación de Mercado realizada, se determinó que por la naturaleza de la contratación y el plazo de los servicios que se propone, la empresa que actualmente presta el servicio es la que ofrece las mejores condiciones para la Institución y que cuenta con las posibilidades de brindar los servicios requeridos por SHF, misma que se mostró interesada en atender todos los requerimientos solicitados cn cl plazo que durará la presente contratación.

De igual forma, otro punto que se consideró para llevar a cabo la contratación es que el prestador de los servicios aceptó continuar con los mismos términos, características, especificaciones, condiciones, y en especial, los mismos precios a los establecidos dentro del actual contrato, y que se mantiene desde cl año 2013.

Adicionalmente, es importante destacar la relevancia para la Institución de contar con el Servicio Administrado de Telecomunicaciones, Io que radica en la necesidad de mantener comunicación constante con las diferentes entidades gubernamentales y no gubernamentales, como un medio. esencial en el accionar diario dc la Institución, a fin de atender todas y cada una dc las Disposiciones emitidas por las entidades regulatorias de carácter financiero, como por ejemplo, las señaladas por el Banco de México (BM) e Indeval, en relación con las Reglas para la realización de operaciones derivadas, así como en las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito, emitidas por la Comisión Nacional Bancaria y de Valores (CNBV) y la Comisión Nacional de Seguros y Fianzas (CNSF).

Para la operación de SHF, se requiere de la disponibilidad, capacidad de control y administración de los servicios prestados para la interacción con las dependencias financieras y normativas, a través de la vía de medios dc telecomunicaciones; así como para las transacciones realizadas por las áreas de finanzas, en su operar diario, pues en caso de no contar con este servicio, podría hacerse acreedora a fuertes sanciones económicas y quedar fuera del mercado financiero por el que fue creada y formalizada, ya que se afectarían las operaciones correspondientes al entorno financiero, provocando así pérdidas significativas a la Institución, además de las sanciones administrativas señaladas en la normatividad emitida por el BM, Indeval, CNBV y CNSF, como ya se ha señalado.

El Servicio Administrado de Telecomunicaciones es para brindar el soporte operativo requerido por parte de las áreas críticas en sus labores diarias y para el caso de posibles contingencias, bajo un esquema de servicios basado en una disponibilidad de 7*24*365 durante la vigencia del servicio a contratar, para el edificio principal de SHF y sus sitios alternos, lo que permite la operatividad continua y sin interrupciones para las áreas sustantivas dc Sociedad Hipotecaria Federal.

Por otro parte, también se pondría en riesgo la continuidad de las operaciones de la Institución mediante la recuperación de la información, ya que no se contaría con los medios tecnológicos necesarios para el traslado de información de respaldo al Centro de Datos Alterno, y en su caso,

estar en capacidad de reaccionar en el caso de que sc prescntc una contingencia o de un desastre que afecte al sitio principal.

Es importante señalar que la infraestructura tecnológica implementada en la Institución, dentro de la cual se encuentran los servicios administrados de telecomunicaciones que sc solicitan, los cuales contemplan servicios de voz, datos y video, a través de los enlaces de comunicación e internet, utili7.ando mecanismos de seguridad y de administración de tráfico en la transmisión de la información, son necesarios para operar los sistemas de información con los cuales sc soportan las funciones de negocio y administrativas institucionales, por Io que se requiere para muchos de los procesos críticos antes enlistados, de la adecuada interconexión, entre la SHF y las entidades normativas y financieras, la red de Intermediarios Financieros y otras más, con las que tiene estrecha relación.

Dicho recurso tecnológico es indispensable para contribuir al cumplimiento del objeto social de SIIF, que es impulsar el desarrollo de los mercados primario y secundario de crédito a la vivienda, mediante el otorgamiento de crédito y garantías destinadas a la construcción, adquisición y mejora de vivienda, preferentemente de interés social, así como al incremento de la capacidad productiva y cl desarrollo tecnológico, relacionados con la vivienda, sector que es un área prioritaria para el desarrollo nacional, aspectos que están plasmados en el Programa Institucional SHF 2020-2024, y que constituye la asunción de compromisos en términos de metas y resultados, mismo programa que está a su vez, alineado al Programa Nacional de Financiamiento al Desarrollo y considera acciones previstas en el Programa Sectorial de Desarrollo Agrario Territorial y Urbano y cn materia de Política Nacional de Vivienda al Programa Nacional de Vivienda y al Programa Nacional de Infraestructura.

Lo anterior, es de suma importancia, ya que, si los procesos críticos de SHF no pudieran funcionar de manera adecuada por la falta de los servicios de telecomunicaciones y seguridad ncccsarios, tanto los objetivos prioritarios como los compromisos establecidos en cl programa institucional, los cuales fueron alineados con los programadas nacionales y sectoriales, se verían seriamente afectados, mermando dc manera directa cl cumplimiento de la Misión de SIIF, que es "Impulsar el desarrollo del mercado de la vivienda bajo un enfoque social, económico y sustentable, ofreciendo soluciones financieras que faciliten su acceso y disponibilidad".

De manera directa o indirecta, todos los objetivos prioritarios establecidos en SHF podrían verse afectados por la falta de estos servicios, ya que para lograr "Mejorar el acceso y cobertura a soluciones de vivienda a nivel nacional", "Impulsar la disponibilidad de vivienda en el país", "Contribuir con soluciones financieras para abatir el rezago habitacional de la población" y "Contribuir al desarrollo urbano y vivienda sustentable", "Garantizar la solidez operativa y financiera de la SIIF y "Garantizar la solidez operativa y financiera de la SEIF", se requiere que la Institución cuente con la infraestructura tecnológica necesaria, a fin de que las aplicaciones implementadas para soportar los procesos de negocio críticos, operen de manera continua y eficiente, y que permita además, asegurar la confidencialidad, integridad y disponibilidad de la información

Fundamentación legal del supuesto de excepción.

De conformidad con los artículos 40, 41 fracción I I I y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 71, 72 fracción II I y 85 de su Reglamento, someto a su consideración, a efecto de que se sigan los trámites y procedimientos a que haya lugar, para la realización de un procedimiento de Adjudicación Directa, como excepción de una licitación pública, toda vez que derivado de la situación anteriormente descrita, he determinado lo siguiente:

A. Se evita un impacto cuantificable del orden de los SI '2,260,000.00 mensuales.
B. Se evitan riesgos de incumplir las distintas disposiciones en materia de seguridad de información emitidas por Banco de México, Indeval, Comisión Nacional Bancaria y de Valores y la Comisión Nacional de Seguros y Fianzas e C. Se continúa contribuyendo al fortalecimiento de control interno institucional
D. Se obtienen las mejores condiciones dc contratación para SHF, ya que la empresa propuesta para esta contratación ha mantenido los precios desde la licitación de 2013.
E. Sc considera que asignar la contratación de mérito a OPERBES, S.A. DE C.V., es la opción más viable, toda vez, que en su momento cumplió con todos los requerimientos administrativos y técnicos para resultar adjudicada en el proceso licitatorio de la Secretaría de Hacienda y Crédito Público.

Monto estimado de la contratación.

El monto máximo de la contratación es de $19,680,000.00 (Diecinueve millones seiscientos ochenta mil pesos 00/100 M.N.) antes de IVA, a ejercer en los ejercicios presupuestales 2023 y 202'1 de la siguiente manera:

AÑO	Partida Presupuestal	
	31602	33304
2023 2024		33.840.000.00
	36.000	
Total	$12,000,000.00	
	$19,680,000.00	

Forma de pago propuesta:

La forma dc pago será cn moneda nacional, a mes vencido, previa entrega y aceptación de los reportes correspondientes a entera satisfacción de SIIF, en un plazo no mayor de 20 días naturales contados a partir de la fecha en quc se haya recibido el entregable y presentado la factura respectiva, debidamente requisitada.

Penas Convencionales: Las penas convencionales están establecidas en la sección correspondiente del Anexo Técnico que se adjunta.

Persona (s) propuesta (s) para la adjudicación:

La contratación que se solicita se realizará con OPERBES, S.A. DE C.V.

Datos generales que se requieren:

Nombre o denominación social:	OPERBES, S.A. DE C.V.
Domicilio fiscal:	Av. Javier Barros Sierra número 540 Torre ll piso, Col. Lomas de Santa Fc, Álvaro Obregón, Ciudad de México.
Contacto:	Cesar Alejandro González González
Teléfono:	55 4000.2195
Correo electrónico del contacto:	agonzalezgon@bestel.com.mx
Representante legal:	Luis Alberto de la Garza Aguirre y César Gerónimo Jiménez Cervantes.

Acreditamiento de los criterios en que se funda la excepción.

El dictamen de excepción a la licitación pública se fundamenta en los criterios de economía, eficacia, eficiencia, imparcialidad y honradez y transparencia que establece el artículo 40 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público conforme a Io siguiente:

Economía

La propuesta recibida de la empresa OPERBES, S.A. DE C.V., cubre la totalidad de los servicios.

Adicionalmente, derivado dc la situación anteriormente expuesta, se evita un impacto cuantificable del orden de los $172,260,000.00 mensuales.

Eficacia

En este sentido, la realización de la contratación de mérito mediante el procedimiento de adjudicación directa permite optimizar los tiempos de contratación y asegura la disponibilidad dc los servicios demandados por la Institución, a través de un proveedor que cuenta con la capacidad y experiencia requeridas por SHF.

VILA

Eficiencia

Lacontratación del Servicio Administrado de Telecomunicaciones, se realizará con estricto apego a Io establecido en la Ley dc Adquisiciones, Arrendamientos y Servicios del Sector Público; por Io que con el cumplimiento de IO establecido en la Ley anteriormente citada y a la información contenida en este dictamen, se puede afirmar que con esta contratación, SHF estará en posibilidad de soportar las funciones y operaciones de negocio, basadas en los servicios de comunicaciones solicitados, de forma satisfactoria y sin interrupción alguna, lo que se traduce en el soporte a las funciones sustantivas del personal.

Imparcialidad y Honradez

La selección del procedimiento de contratación se realizó con estricto apego a las disposiciones establecidas cn la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y en la Ley Federal de Responsabilidades Administrativas dc los Servidores Públicos. Asimismo, después dc haber realizado un análisis minucioso de las condiciones existentes en el mercado, se determinó que el procedimiento de contratación que se solicita es la mejor opción disponible para la Sociedad Hipotecaria Federal, S.N.C., por lo que se ha dado cabal cumplimiento a los criterios de imparcialidad y honradez en la selección del procedimiento.

Transparencia

El criterio de transparencia se acredita fehacientemente, mediante el flujo de información que en todo momento fue accesible, claro, oportuno, completo y verificable, mismo que se encuentra disponible en los archivos correspondientes a la Subdirección de Ingeniería de Sistemas, mediante la cual se muestra que la información, documentación y demás soporte documental relativo a la contratación que nos ocupa está disponible para su consulta.

Asimismo, se ratifica que Io que se busca motivar con la presente solicitud de excepción a la Licitación Pública, es que se tenga la posibilidad de contratar el servicio en comento mediante la adjudicación directa, con las mejores condiciones económicas y de eficiencia para SHF, ya que prevalece el interés público, en tanto que la adjudicación propuesta se efectúa sin prejuicio ni prevención alguna, con la más absoluta transparencia en el presente caso.

Cabe señalar que, con base en los antecedentes y motivaciones descritos, se ha determinado que el precio señalado para la presente contratación se encuentra dentro de los rangos razonables de mercado y resulta adecuado para la Sociedad Hipotecaria Federal, S.N.C. en función de los beneficios que se obtendrán como resultado de llevar a cabo la contratación dc mérito.

2023 Francisco VILA

Existe suficiencia presupuestal para 2023
$6,000,000.00
(Servicios de Telecomunicaciones)
PARTIDA 31 602 $3,840,000.00
PARTIDA 3330'1 (Servicios de Mantrninliento (le Aplicaciones liliorntàtica:•)

SOCIEDAD HIPOTECARIA FEDERAL, S.N.C.
SUBDIRECCIÓN DE PRESUPUESTO
SE CUENTA CON SUFICIENCIA PRESUPUESTAL EN LA (S) PARTIDA (S): 31602, 33304

Vo.Bo. Suficiencia Presupuestal.

No adeudo de contribuciones fiscales.

De conformidad con las disposiciones en materia fiscal, adjunto a la presente solicitud, la opinión dc cumplimiento de obligaciones fiscales con el que se comprueba que se realizó la solicitud dc opinión prevista en la regla 2.1.31 de la Resolución Miscelánea Fiscal aplicable para el 2022 (o aquella que en el futuro la sustituya), y con el que se acredita que el proveedor propuesto no tiene adeudos fiscales firmes a su cargo.

Deigual manera, con finalidad dc dar cumplimiento al Acuerdo ACDO.SA1.HCT.101Z14/281.P.DlR y su Anexo Único, dictado por el H. Consejo Técnico, relativo a las Reglas para la obtención de la Opinión dc Cumplimiento de Obligaciones Fiscales en Materia de Seguridad Social; publicados el 23 de diciembre de 2014 y 27 de febrero de 2015, se adjunta la Opinión de Cumplimiento de Obligaciones Fiscales en Materia de Seguridad Social, en sentido positivo y vigente.

Asimismo, sc adjunta la Constancia de Situación Fiscal en Materia de Aportaciones Patronales y Entero de Descuentos, de conformidad con el Acuerdo del H. Consejo de Administración del

Instituto del Fondo Nacional de la Vivienda para los Trabajadores por el que se emiten las Reglas para la obtención de la constancia de situación fiscal cn materia de aportaciones patronales entero de descuentos.

2023
flúncis70

En términos de los Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios y de Obras públicas y servicios relacionados con las mismas, se precisa la siguiente información:

I. El domicilio en que habrá de entregarse el servicio y el horario correspondiente para ello; será en Av. Ejército Nacional No. 180 70. Piso, Col. Anzures, Alcaldía Miguel Hidalgo, C.P. 11590, Ciudad de México. en un horario de 9:00 a 18:00 horas.

11. Condiciones específicas de entrega del servicio;

Las solicitudes de soporte y/o mantenimiento deberán efectuarse y atenderse conforme a lo establecido en el punto "Niveles de Servicio"

111. El servidor público facultado para recibir los servicios, quien será el responsable de su aceptación a satisfacción, su devolución o rechazo y de determinar los incumplimientos en el caso de los servicios, así como de hacer cumplir los plazos que se establezcan para tales efectos de acuerdo con estos Lineamientos; será el Subdirector de Infraestructura Tecnológica y el Subdirector dc Seguridad Informática.

IV. El tipo de pruebas o verificación física a que se someterán los servicios de acuerdo con Io establecido en el artículo 29 fracción X de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, para ser recibidos a satisfacción, así como el responsable de llevarlas a cabo y el tiempo requerido para su realización, el cual no podrá exceder de diez días naturales contados a partir de la entrega del servicio en el domicilio a que sc refiere la fracción I de este lineamiento. Posteriormente al Servicio Administrado de Telecomunicaciones, personal de la Subdirección de Infraestructura Tecnológica y/o de la Subdirección de Seguridad Informática revisará el correcto funcionamiento de los servicios, en un periodo que no podrá exceder diez días naturales contados a partir de la prestación del servicio.

V. El procedimiento para la devolución o rechazo del Servicio Administrado dc Telecomunicaciones para determinar los incumplimientos en la prestación del servicio, lo cual solamente procederá por causas previstas en el contrato respectivo. En caso de incumplimiento, el servidor público facultado para recibir el servicio dará aviso al

2023
VILA

proveedor y a la Subdirección de Recursos Materiales y Servicios Generales en el caso de que se deban aplicar penas.

Garantías

De conformidad con el Artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el proveedor deberá garantizar los servicios mediante fianza expedida por una institución financiera autorizada, por el 10% del importe máximo del contrato antes del Impuesto al Valor Agregado.

Así mismo, se precisa que el costo que se genere por la emisión de las garantías que en su caso sc soliciten, correrá por cuenta del proveedor adjudicado.

Incumplimiento

El incumplimiento en la prestación del Servicio Administrado de Telecomunicaciones será comunicado al proveedor a más tardar en los cinco días hábiles siguientes a aquél en que éste sc determine, señalando las razones que Io motivaron, las cuales deberán estar vinculadas a las condiciones establecidas en el contrato, indicando el plazo para su reposición o corrección.

Comprobantes Fiscales Digitales por Internet.

I.Se deberán emitir los Comprobantes Fiscales Digitales por Internet (CFDI o como en el futuro la legislación fiscal de México le designe a los comprobantes fiscales), que dc conformidad con las disposiciones fiscales se requieran para comprobar los gastos y pagos realizados, los cuales deberán remitirse en archivos electrónicos XML y PDF(representación impresa) a las siguientes direcciones de correo electrónico: cfdsb@shf.gob.mx, emorales@shf.gob.mx y rquintcro@shf.gob.mx l l. El servidor público facultado para validar que los documentos que presente el proveedor para su pago cumplan con los requisitos de aceptación de la Continuidad del servicio administrado de telecomunicaciones, será el Subdirector de Infraestructura 'l'ecnológica y el Subdirector de Seguridad Informática.

En el caso de que se comunique al proveedor la existencia de errores o deficiencias en la factura o cl documento quc hubiere presentado, será responsabilidad del proveedor subsanarlos y presentar nuevamente la factura o el documento que reúna los requisitos fiscales correspondientes en el menor tiempo posible.

En ningún caso procederá la devolución de facturas o de los documentos presentados por cl proveedor, por errores que no afecten la validez fiscal del documento o por causas imputables a I dependencia o entidad.

Por otra parte, para dar cumplimiento de lo dispuesto en el artículo Décimo Segundo del Decreto de Austeridad y al lineamiento número 20 de los Lineamientos para la Aplicación y Seguimiento de las Medidas para el IJso Eficiente, Transparente y Efica7. de los Recursos Públicos, y las Acciones de Disciplina Presupuestaria en el Ejercicio del Gasto Público, así como para la Modernización de la Administración Pública Federal, solicito determine si la contratación de los servicios motivo de

la presente solicitud será consolidada. Sin detrimento de lo anterior, esta contratación se considera consolidada entre las unidades administrativas de SHF, de acuerdo con el Inciso I de dicho lineamiento.

Con base en lo anterior, le informo que dicha contratación es indispensable para la realización de las actividades de esta Dirección a mi cargo, por Io que le solicito nuevamente su apoyo para llevar a cabo el procedimiento de contratación respectivo.

Atentamente

Ing. Gregorio Linares Urenda
Director dc Tecnologías dc la Información

REQUISICIÓN DE BIENES Y/O SERVICIOS

SOCIEDAD HIPOTECARIA FEDERAL

DIRECCIÓN GENERAL DE ADMINISTRACIÓN Y OPERACIONES
DIRECCION DE ADMINISTRACIÓN
REQUISICIÓN DE BIENES Y SERVICIOS

2023 Francisco VILLA

HACIENDA

NOMBRE DE LA ENTIDAD: SOCIEDAD HIPOTECARIA FEDERAL, SOCIEDAD NACIONAL DE CRÉDITO.

ÁREA REQUIRENTE:
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

FECHA DE ELABORACIÓN: 22/01/2023

NO. DE REQUISICIÓN: 03/2023

FECHA REQUERIDA: AL DÍA SIGUIENTE DE LA NOTIFICACIÓN DE LA ADJUDICACIÓN

LUGAR DE ENTREGA: DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN; AV. EJÉRCITO NACIONAL NO. 180 7O. PISO 7, COL. ANZURES, ALCALDÍA MIGUEL HIDALGO, C.P. 11590

NO. DE PARTIDA	CUCOP	DESCRIPCIÓN DEL SERVICIO	CANTIDAD SOLICITADA	UNIDAD DE MEDIDA	PRECIO UNITARIO PROMEDIO	IMPORTE	
						Monto Mínimo	Monto Máximo
31602	31600001	CONTINUIDAD DEL SERVICIO ADMINISTRADO DE TELECOMUNICACIONES	1	SERVICIOS		$4,800,000.00	$ 12,000,000.00
33304	33300009	CONTINUIDAD DEL SERVICIO ADMINISTRADO DE TELECOMUNICACIONES	1	SERVICIOS		$ 3,072,000.00	$ 7,680,000.00
					SUBTOTAL	$ 7,872,000.00	$ 19,680,000.00
					I.V.A.	$ 1,259,520.00	$ 3,148,800.00

ANEXOS: SI

TIPO DE PROCEDIMIENTO DE CONTRATACIÓN: Adjudicación directa

OTROS GRAVÁMENES:	-	-
TOTAL:	$ 9,131,520.00	$ 22,828,800.00

ANTICIPO: NO

AUTORIZACIÓN DEL PRESUPUESTO: 213/2022 FECHA : 23/12/2022

EXISTENCIA EN ALMACÉN: No aplica

OBSERVACIONES: CONTINUIDAD DEL SERVICIO ADMINISTRADO DE TELECOMUNICACIONES, A TRAVÉS DE UN CONTRATO ABIERTO PLURIANUAL POR UN MONTO MÁXIMO DE $22,828,800.00 (VEINTIDOS MILLONES OCHOCIENTOS VEINTIOCHO MIL OCHOCIENTOS PESOS 00/100 M.N.); OFICIO DE AUTORIZACION DE PLURIANUALIDAD DGAAO-2022-235 DE FECHA 30 DE DICIEMBRE DE 2022.

REGISTRO SANITARIO: NO

NORMAS / NIVELES DE INSPECCIÓN: NO APLICA

CAPACITACIÓN: NO APLICA

PAÍS DE ORIGEN: MÉXICO

MÉTODO DE PRUEBA: NO APLICA

TIPO DE GARANTÍA: Cumplimiento indivisible	PORCENTAJE: 10	PLURIANUALIDAD: Si	MESES: 23
TIPO DE GARANTÍA:	PORCENTAJE: N/A	PENAS CONVENCIONALES: SI	PORCENTAJE: 2 AL MILLAR
TIPO DE GARANTÍA:	PORCENTAJE: N/A	TIEMPO DE FABRICACIÓN:	NO

CONDICIONES DE ENTREGA: CONFORME AL ANEXO TÉCNICO

ÁREA REQUIRENTE: ING. GREGORIO LINARES URENDA
DIRECTOR DE TECNOLIGÍAS DE LA INFORMACIÓN

AUTORIZA: LIC. CLAUDIA AMÉRICA ENRÍQUEZ VEGA
DIRECTORA DE ADMINISTRACIÓN

ANEXO A • ANEXO TÉCNICO

Continuidad del Servicio Administrado de Telecomunicaciones

INDICE

ESPECIFICACIONES TECNICAS Y ALCANCES DEL SERVICIO

1 Introduccion

Sociedad Hipotecaria Federal tiene la necesidad de mantener comunicación permanente entre los diversos nodos que la conforman, por lo que se requiere integrar una Red Telecomunicaciones, que permita la transmisión segura de datos y de voz, logrando la homologación tecnológica en materia de comunicaciones.

Actualmente la SHF cuenta con un esquema de conectividad para la transmisión de datos y voz entre un conjunto de nodos, cada uno de ellos identificado por un número (ID) y distribuidos geográficamente en el área metropolitana de la Ciudad de México y en diferentes localidades del país.

2 Alcances

2.1. Alcance del documento

El proposito del presente documento es establecer las especificaciones minimas y lineamientos técnicos minimos, para dar continuidad a los servicios actuales a través de la contratación de Continuidad del Servicio Administrado de Telecomunicaciones para la transmisión de datos y de voz, que incluyen los siguientes apartados: Servicio Administrado de Telecomunicaciones, Servicio de Acceso a Internet y Servicio de Seguridad, de acuerdo a los Niveles de Servicio que la SHF establezca.

2 20 Alcance del Servicto

Los servicios solicitados en el presente documento tendrán un periodo de vigencia a partir del día siguiente de la notificación de la adjudicación y hasta el 31 de diciembre de 2024.

"EL PROVEEDOR" integrará en su proposición la administración del proyecto, la operación, el mantenimiento y en general la administración de los servicios ofertados que se requieren en el presente documento.

"EL PROVEEDOR" deberá considerar el hardware, software, licenciamiento, infraestructura, medios, instalaciones y todo el personal necesario para soportar la operación y administración de los servicios solicitados; asimismo, todo el hardware y software quedará bajo su responsabilidad para cumplir los niveles de servicio solicitados por la SHF.

3 Cont.n"'dacf de los Servicios Administrados

A continuación, se describen las especificaciones que "El PROVEÉOOR- deberac•umpl" para proporcionar continuidad de los Servicios Administrados de acuerdo a la sc é.' a solicitud la SHE

3 1 Cont.nu.dad del servicio Administrado de Telecomumcaciones

Los servicios solicitados en el presente documento tendrán un de vigencia a vargr del día siguiente de la notificación de la adjudicación y hasta el 31 de diciembre de 7024

3 1 1 Continuidad dei servicio de LAN to LAN

Se debe dar continuidad a la operación a la SHF con menos con las siguientes características: ios dedicados punto a punto el detie cumpli

- Modo Wire
- Enlace Sincronc
- Debe entregarse en interfaz Ethernet (IEEE 802.3) con conectores el punto de demarcación del servicio. RJ4% en caca una de Sus puntas, siendo estos
- Realizar el transporte a nivel capa 2 del modelo OSI, es decir misma LAN de la SHF)
- Garantizar el ancho de banda siendo simétrico y bidireccional manteneonctt) el direccionamiento IP (extensión de la
- El PROVEEOC)R• ctefrerâ poder realizar incrementos ancho de banda solicitud de la Convocante y deberá egurar Cue CPE actual soporte dicho incremen'0
- Comunicación Full-Duplex llevada a cabo para desactivar la detección '30 colisiones y funciones de loopback
- tv Pocer transwonar diferentes VtANs con encapsulación do: 'G (IEEE 802.1Q) y transportar todo el tráfico de broadcast, unicas un;cast y mu/5cast entre los dos extremos del enlace
- La latencia máxima aceptada en enlace de ms
- Contar con una horramtenta t',e morutoroo y nedición de uso del enlace
- "El PROVEEDOR • det» considerar su proposjc;on el ancho de base inicial de 200 Mbps, con incrementos del Mpbs hasta 1 Gbps,

3.2 Continuidad del servicio administrado de Acceso a Internet

La SHF requiere d
a sus necesidades del Serve:i0 Oe Acceso a Internet, con serv'tctos de sequndad con de servicios de acuerd de

en el Ane'0 '-A *'Inmuebles y Requerimientos de Servicio e Infraes*

El ancho de banda solicitado se describe para SHF.

PROVEEDOR • deber considerar las squmntes

Para la prestación de este servicio, "EL P

contar cor, al monos dos conenonos STM.t6 a

1 y gararttzar que ia a internet en su Internaoonal_ esta '"formacion

dobera documentaria claramente en

b) EL PROVEEDOR• cebera manifestar por escrito. que cuenta con Acuerdos Peer•ngs con menos r.os W)'oveodores do internet de México con la finalidad do el dol entre 'os Proveedores do Internet

Paralos nocos debera OÇ.ierar con oatanceo de cargas en ambos emaces en casc taya deberánmiutar automatir.arnente el trafico al enlace que se encuentre operando correctamente

d) "EL PROVEEDOR" debera [illegible] por SHF. Esta solicitud permitirá cua homologadas, sin generar costos adic

pt090rconarun de 64 dilecciones EP homologar.%s acuerdo a cuando la SHF to requiera el incremento en dtrt%L€-ones

e) "EL PROVEEDOR" deberá poder reali asegurv que el CPE actual soporte di

asequr,v que poder realizar «v:remontcs de ancho do banc% a solec-'tud de ta Convocante y deberá dicho incremento

'i de Accese a internet, •EI_ PROVEEDOR• debe servvcg•y manera enuncuanva más no enlaces

considerar todos los elementos que requieran para limitativa podrán ser: router multiservicio, switches de este servicio no se aceptarán costos adicionales

to que Joara ta prestactor, se

q;' Se 'rnpiomentar y hab'lltar de datos en enlace AES-128 y algoritmo y d hashiry; SHA•â' o

3 2 M Caractensticas de seguridad que deberá tener ta continuidad del Servicio administrado de Acceso a Internet

uue «n la tnfraestructuea dei serv•Ci0 de tnternetde en forma el anómalo mitiqar mabc'0sa quo Presente como ataques de ta' poner»dc medio de L» actividad de gusanos o de ataques de t;po bntnots

tde "EL PROVEEDOR", se incluya un mecanismo del servicio y tener la capacidad de alertar a la SHF ataques de tipo Negación de Servicio Distribuido

tanto. el servao 'ntegrar sistema de gestion de amenazas que realito una Inspecc.:On at P'ovoedor de/ de manera e ias a s"uacon trate de agote',r o: ancho de franda o recursos de

El sistema debera realizar el análisis del flujo de tráfico buscando patrones de tráfico anormales que indiquen la presencia de un ataque tipo DDoS

Una vez que se ha detectado esta condición anómala, el tráfico debe ser filtrado y descartado todo el tráfico dañino dejando pasar solo el tráfico legítimo hacia las redes de la SHF para ser entregado a su destino final durante todo este proceso los servicios publicados en Internet deben permanecer siempre disponibles.

SHA-

El análisis del tráfico, la detección de anomalías y el proceso de mitigación de ataques de tipo DDoS se debe llevar a cabo en la infraestructurade "EL PROVEEDOR", el objetivo es que el proceso de mitigación del tráfico de ataque se realice antes de que pueda llegar a las redes de la SHF

La solución deberá permitir y operar al menos con las siguientes características

'as sgcentes

a) Mitigación y detección de amenazas
   - Detección de anomalías y mitigación de DDoS y DoS
   - Amenazas de día cero antes de que impacten en los servicios de SHF
b) Mitigación y detección de lo siguiente
   - Zombie Flexible
   - Zombis (con selecciones de umbrales en Mbps y pps desde el portal Web del cliente) para clasificar una IP como zombis y con la opción de conocer una lista de zombis activos detectados. Mitigación inteligente de botnets
   - Firmas de capas aplicativas
   - Mitigación contra ataques SSL
   - Ataques de SSL malformados
   - Visibilidad en tiempo real de los eventos de la mitigación
   - Visibilidad de todas las estadísticas de las mitigaciones andando
   - Selección de detalle y configuración de cada contra-medida usando la pizarra de mitigación
   - Captura simple de paquetes de datos "crudos" directamente desde la pizarra de mitigación
c) Ataques de saturación de recursos SSL Ingeniería de tráfico inteligente
   - Visibilidad escalable y análisis del tráfico con tecnología de "flujo" de la red
d) Interfaz Web que permita ofrecer por lo menos las siguientes características
   - Configuración de recursos definidos por rangos de las subredes (CIDR). Números de sistemas autónomos de BGP. Interfaces del router, comunidades de BGP, información de capa 3 y 4 de netflow (lenguaje basado en TCPDUMP)
   - Detección de ataques basado en la línea de base contra los recursos definidos, con opciones configurables por recursos que permitan filtrar la sensibilidad de la anomalía en paquetes por segundo y Mbps, disparando una alarma vía correo electrónico
   - Detección basada en la violación de un protocolo de por lo menos los siguientes
     - TCP Syn Flood/RST/NULL
     - ICMP Flooding
     - Tráfico total (Mbps y paquetes por segundo)
   - Detección del tráfico basado en lenguaje TCPDUMP con información definida en las capas 3 y 4
   - Ejecutar reportes en tiempo real y calendarizados que incluyan lo siguiente: Anomalías clasificadas por niveles de severidad acordada con SHF. Anomalías por tipo, incluyendo por lo menos las siguientes
     - Fragmentación de IP
     - Protocolo
     - Ancho de Banda
     - ICMP
     - TCP/SYN
     - Alertas y Mitigaciones
     - Distribución del ancho de banda
       - Por protocolo
       - Los hosts que más utilizan la red (Top Talkers)
       - Por aplicación
     - Tamaño del paquete
     - QoS
     - Un tabulador de gusanos
     - Por sitio y aplicaciones caídas

e SHV e'

atoqces y ae

me.•.l.aas oa'ö e' Para se oftecera ia

acceso tasaaas

PC' ment.s se acc-eso a ocu.•ndas meses ;nea te

A traves de msn* Web se 'a generaaer de Hue"as

a a:acue•. er 3 or

fo•mato ae manera aoe retrnitA on ataat'€• camr•e

J EL PROVEEOOR- J'

'nyecccr• de EGF'

F ac:os:• 'ACIs• de

so oata av-.ar:ar e; elemen•.o Woe esta

a PROVEEL)OR La m.t•oacor a ar'.:arse as'

rea ge Ce

J EL PROVE EtyOR 'as mogac.cnes

detaJes de y

acc.eso a' se r:ya

'EL PROVFEOOR en casc Oe ta*a ge i de nase ova ase•go'a'

Las *lectromcc, cesc:e

PROVEEOOR y D SHE ovc.cnes una e la a:

mencs las de SYN

ONS mal Eagado er con cnen:e G" y

Linea oase

Ce en '*tvs pa:a una IP can de conocr una

"Sta Ce

OQR' jnCtuyen a er ona esta os "'emen•.cs aue la •nteg•ar

tomo 'a anomm.as y ce atam.€•s

'EL PROVEEDOR' incluyen como parte del servicio propuesto, la solución de detección, gestión y mitigación de ataques DoS/DDoS que permitirá realizar inspección del tráfico de acceso a Internet y permitirá reducir de manera rápida e inteligente las amenazas a la seguridad y contra cualquier situación desconocida que trate de agotar el ancho de banda o los recursos de la red de SHF. La solución realiza el análisis del flujo de tráfico buscando patrones de tráfico anormales que indiquen la presencia de un ataque del tipo DoS/DDoS generado por medio de la actividad de gusanos o de ataques de tipo botnet.

El Centro de Operaciones de Seguridad (SOC) de 'EL PROVEEDOR' administrará la infraestructura relacionada con la solución de detección, gestión y mitigación de ataques DoS/DDoS permitiendo determinar en forma automática el comportamiento anómalo del servicio y tener la capacidad SHF de solicitar a 'EL PROVEEDOR' mitigar cualquier actividad maliciosa que se presente en forma de ataques de tipo Denegación de Servicio Distribuido.

'EL PROVEEDOR' tomaron en consideración que para la solución de detección, gestión y mitigación de amenazas no se considerará como válido equipo instalado en las instalaciones de SHF ni a través del equipo CPE propuesto, ni a través de infraestructura subcontratada o de un tercero, dicha solución estará implementada y operando en el backbone de 'EL PROVEEDOR'.

La solución realizará el análisis del flujo de tráfico buscando patrones de tráfico anormales que indiquen la presencia de un ataque tipo DoS/DDoS con base en netflow.

solución detección, gestión y mitigación de ataques DoS/DDoS detectará cualquier condición omala, el tráfico será filtrado y descartado todo el tráfico dañino, dejando pasar solo el tráfico legítimo

hacia la red de SHF para ser entregado a su destino final, durante todo este proceso los servicios publicados en Internet permanecerán siempre disponibles.

"EL PROVEEDOR" tomaron en consideración que el objetivo de incluir la solución de detección, gestión y mitigación de amenazas es que el proceso de mitigación del tráfico de los ataques se realice en una zona segura antes llegar a la infraestructura de red borde y/o segmentos internos de SHF.

La solución de detección, gestión y mitigación de ataques DoS/DDoS incluye:

Monitoreo pasivo para detectar eventos DoS/DDoS, sin afectar el tráfico de la red.

- Inyectar rutas de BGP para filtrar tráfico de ataques dirigidos a la red interna de SHF.
- Enrutar el tráfico bajo ataque hacia un sistema de filtrado inteligente que separa en tiempo real, al tráfico legítimo del tráfico malicioso.
- Usar técnicas para detectar anomalías, tales como ataques del tipo flooding (ICMP, TCP SYN, etc.).
- Representaciones gráficas de tasa de transferencia de datos, ataques, a través del tiempo para periodos de tiempo variable.
- Acceso a un a un portal web para que SHF pueda visualizar los reportes vía internet.
- La generación de reportes de las mitigaciones que fueron ejecutadas anteriormente, con detalles del tráfico que pasó y el tráfico que se descartó.
- Permitirá acceder a, por lo menos, los últimos 3 meses de las mitigaciones ocurridas (Reportes).
- Permitirá la generación de reportes de las mitigaciones ejecutadas, con detalles del tráfico que pasó y el tráfico que se descartó y estarán accesibles a SHF.

La solución de detección, gestión y mitigación de ataques DoS/DDoS acepta información de rutas BGP de todos los enrutadores monitoreados en la red, así como entiende la información de rutas y los AS_PATH completos, en un ambiente reflejado y/o de un espacio de SA privado y cuenta con reportes de análisis de tráfico de peering para cada peer, por prefijo IP y de cada objeto administrado por peer y por interface.

La solución de detección, gestión y mitigación de ataques DoS/DDoS brindará alertas cuando el proceso de recolección BGP de un enrutador monitoreado haya dejado de funcionar o presente algún problema así como es capaz de indicar por cuales interfaces se recibe el tráfico anómalo.

La solución de detección, gestión y mitigación de ataques DoS/DDoS se basa en hardware de propósito específico comercial especializado para la mitigación de Ataques DoS/DDoS. Dicha infraestructura cuenta con sus licencias de operación y soporte durante la vigencia del contrato. "EL PROVEEDOR" tomaron en consideración que no se aceptan soluciones basadas en open source (por sus siglas en inglés) o sistemas de código abierto, freeware, shareware o cualquier otra forma de software no comercial. De igual manera, que no se aceptan soluciones basadas en hardware tipo IPS y/o Firewall por no ser hardware especializado en la Mitigación de Ataques DoS/DDoS.

La arquitectura de la solución de detección, gestión y mitigación de ataques DoS/DDoS instalada en la infraestructura de "EL PROVEEDOR" monitoreará el tráfico con el fin de detectar los ataques DDoS desde su ingreso a la infraestructura de "EL PROVEEDOR" para que estas puedan detectar efectivamente los efectos del ataque desde el punto más cercano a la entrada donde son más dañinos por su magnitud en ancho de banda.

El SOC de "EL PROVEEDOR" entregará reportes de los incidentes ocurridos relacionados con ataques de DDoS. Dichos reportes contendrán al menos lo siguiente:

- Nombre de la alerta.
- Identificador del cliente.
- Dirección IP que fue atacada.
- Tiempo de Inicio y tiempo de término del ataque.
- Graficas de consumos de ancho de banda del ataque.
- Promedio de 1 y 5 minutos.
- Paquetes descartados.
- Paquetes permitidos.
- Paquetes totales que pasaron a través del equipo de mitigación.
    - Porcentaje total del tráfico.
    - Paquetes bloqueados en promedios de 1 y 5 minutos.

Con la finalidad de que SHF cuente con una seguridad perimetral que permita robustecer y protegerse contra ataques provenientes de internet, intranet y de otras redes; SHF requiere la continuidad de la infraestructura de seguridad necesaria para proteger las aplicaciones.

"EL PROVEEDOR" continuará ofreciendo los diferentes Servicios de Seguridad Perimetral con el objetivo de garantizar niveles de confianza para un control de acceso a las redes Internet e Intranet, así como la definición de políticas en zonas desmilitarizadas (DMZ) donde se alojarán los servicios y/o aplicaciones expuestas a Internet.

"EL PROVEEDOR" incluirá todos los elementos de hardware y software necesario para la correcta operac así como lo necesario para su montaje en gabinetes.

cuentacon servüos nencionados er sguento 'abia

COMPONENTE8	Nomenclatura
CONTENCtON OE A7AOUES EN EL PERIMETRO	CA p
MULTIFUNCIONAL	M FOPS
WAF	WAF
IPS	
PROTECCI N CONTRA MALWARE WEB	PCM
CORRELAC!ONAOOR OE EVENTOS	CE

Todos los equipos serán cajas con propósito específico y operar necesidades de SHF y a la criticidad de cada nodo de mane:a conjunta, alineándose a las

3 J Contsnuidad del servici0 de contenc•on de ataqucs en el perimetro de internet

La solución contará y operará al menos con las siguientes características:

a) Será una caja de propósito específico dedicado a proporcionar disponibilidad, por lo que no se aceptan soluciones que mantengan el estado de la conexión como cortafuegos, sistemas de prevención, detección y las variantes o combinaciones como UTM, NGFW, NGIPS ya que al conservar el estado de la conexión son por sí mismos susceptibles a DDoS.
b) Las capacidades mínimas de los equipos se consideraron con base a la siguiente tabla:

InspecciOn/ Throughput	Memoria	Conexiones por Segundo	Rendimiento para paquetes pequenos	Interfaces
Gb,-.s			1.5 Mpps	Fibra y Cobre segun las caracteristicas de los Enlaces

c) Si el rendimiento es mayor del 85% promedio durante 3 días hábiles consecutivos de operación normal "EL PROVEEDOR" remplazarán el equipo por la siguiente categoría, en un plazo no mayor a tres días hábiles.
d) El sistema tendrá embebido el bypass físico en cada interface para garantizar la disponibilidad y continuidad de los servicios activándose en los siguientes casos:
   - Pérdida de energía eléctrica.
   - Falla lógica en la interface de control.
   - Pérdida de conectividad con la tarjeta madre del dispositivo.
   - Colapso del sistema operativo.
e) El sistema al posicionarse en línea será completamente transparente, sin introducir ningún cambio de encapsulamiento, es decir, sin realizar modificación o alteración al tráfico que pase por dicha solución.

f) El sistema será capaz de soportar un modo de prueba "inactivo" 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"
g) El sistema soportará la implementación en modo "monitor" en el que no introduce ningún punto adicional de falla a la red
h) El sistema será capaz de capturar tráfico directamente desde un puerto espejo (SPAN) en un enrutador, switch o tap
i) El sistema soportará una configuración en donde no reenvíe el tráfico entre los puertos de protección al operar en modo espejo, SPAN, o tap de red, para evitar la inyección de tráfico duplicado
j) El sistema soportará redundancia completa para fuentes de alimentación
k) El sistema admitirá HotSwap de una fuente de alimentación degradada durante el funcionamiento normal del sistema

Para la administración de la solución propuesta se cumplirá al menos con lo siguiente:

a) El sistema proporcionará documentación en línea para consulta vía Web para ayudar a SHF a comprender las funciones de cada pantalla
b) "EL PROVEEDOR" proporcionará cuentas de solo lectura al sistema para la consulta y revisión de configuración. El acceso será vía Web y SSH
c) Incluirá un registro de cambios que reporte todos los eventos que podrían afectar la administración, incluyendo: los inicios de sesión de usuario, los cambios de configuración, comandos CLI y actualizaciones del sistema
d) El sistema proporcionará la capacidad para crear y exportar paquetes de diagnóstico que contienen información del estado y configuración a utilizarse para resolver problemas
e) El sistema proporcionará una opción de SYSLOG, SNMP v3 o notificaciones SMTP para las alertas del sistema, los cambios de modo de despliegue (activo/inactivo) y cambios de nivel de protección
f) El sistema admitirá el control de su estado general a través de SNMP v3
g) El sistema proporcionará controles de acceso a nivel de usuario basados en tokens que pueden asignarse a usuarios o grupos de usuarios para aplicar la separación de privilegios
h) El sistema proporcionará listas de control de acceso IP para todos los servicios remotos que estén accesibles
i) El sistema proporcionará Acceso, Autentificación y Auditoría a los usuarios a través de una base de datos de usuario local, RADIUS, TACACS+ o la configuración combinada de métodos
j) El sistema proporcionará 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 de la CPU y memoria de sistema
k) El sistema mostrará una lista de protecciones activas en conjunto con estadísticas resumidas de la cantidad de tráfico permitido y bloqueado para cada grupo de protección configurado
l) El sistema proporcionará estadísticas detalladas y gráficos para cada protección, mostrando su impacto en el tráfico durante los últimos 5 minutos, 1 hora, 24 horas, 7 días o un intervalo personalizado especificado durante toda la vigencia del Contrato
m) El sistema mostrará estadísticas de protección en tiempo real sobre tráfico permitido y bloqueado en bytes y paquetes, con estadísticas en bps y pps
n) Proporcionará estadísticas detalladas y gráficos para mínimo los siguientes grupos de protección
   - Servidores de Aplicaciones
   - servidores Web
   - servidores DNS
   - servidores VoIP
o) Las Estadísticas detalladas incluirán información sobre
   - Tráfico total
   - Tráfico total permitido y bloqueado
   - Número de hosts bloqueados
   - Estadísticas sobre cada tipo de prevención
   - Tráfico por URL
   - Tráfico por dominio
   - Información de ubicación IP
   - Distribución de protocolos
   - Distribución de servicios
   - Principales hosts bloqueados
p) El sistema admitirá la generación de informes PDF y generación de reportes vía correo electrónico con las estadísticas detalladas y gráficos para cada grupo de protección

Como parle do la solucion la mitigación en la NubO dc internet do "EL PROVEEOOR•• operará do la

siguenteforma

siguiente forma:

a) El sistema solicitará a través de un protocolo de señalización en la nube
b) La funcionalidad del sistema de "señalización en la nube de "EL PROVEEDOR"" soportará la solicitud de mitigación ascendente en la nube que proporciona la conectividad a Internet
c) El sistema podrá disparar la solicitud para una mitigación de nube ascendente, ya sea manual o automáticamente a través de la configuración de umbrales de tráfico
d) El sistema automáticamente reportará el estado y estadísticas durante una mitigación en la nube iniciada por "EL PROVEEDOR" sin necesidad de una solicitud explícita de SHF
e) El sistema será capaz de informar la cantidad de tráfico bloqueado en bps y pps durante una mitigación en la nube en curso
f) El sistema será capaz de informar la cantidad de tiempo que una mitigación de nube lleva ejecutándose
g) El sistema será capaz de informar el estado actual de una solicitud de mitigación de nube, informando si se ha activado correctamente o no
h) El sistema enviará notificaciones acerca de cualquier cambio de la mitigación
i) El sistema será capaz de reportar el estado de la conexión de señalización en la nube con el sistema del SOC de "EL PROVEEDOR", mostrando el estado, errores de conexión y cuando haya sido deshabilitado
j) El sistema podrá proporcionar la capacidad para manualmente disparar una prueba de conexión de señalización en la nube con el SOC del Licitante

la prevencion de ataques soportara y operara de la siguiente manera:

la prevencionde ataques soportara y operarade la siduiente

a) Bloqueará paquetes que no son válidos y proporcionará estadísticas para los paquetes descartados considerando lo siguiente
   - Controles de encabezados IP malformados
   - Fragmentos incompletos, checksum IP erróneos
   - Fragmentos duplicados
   - Fragmentos muy largos
   - Paquetes pequeños
   - Paquetes TCP pequeños
   - Paquetes UDP pequeños
   - Paquetes ICMP pequeños
   - Checksums TCP/UDP erróneos
   - Banderas TCP inválidas
   - Números ACK inválidos
b) Permitirá la configuración de listas de filtros que contengan expresiones FCAP para permitir o bloquear tráfico
c) Detectará fuentes 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)
d) Descartará paquetes según puertos TCP / UDP específicos y payloads que coincidan o no con expresiones regulares configurables
e) Prevención de inundación suplantada de SYN's TCP que autentifiquen conexiones TCP desde los host origen
f) Prevención de inundación suplantada de SYN s TCP será capaz de especificar los puertos TCP origen y destino a ser ignorados
g) Prevención de inundación suplantada SYN s TCP proporcionará una forma de no impactar sesiones de usuarios legítimos HTTP a través de redirección HTTP subsecuente
h) Prevención de inundación suplantada de SYN's TCP proporcionará opciones de mecanismos fuera de secuencia ACK para la autentificación de la conexión de las aplicaciones basadas en TCP que son sensitivas a envío de TCP RST a los clientes
i) Eliminación de sesiones TCP inactivas si SHF no envía una cantidad de datos configurable por "EL PROVEEDOR" dentro de un periodo de tiempo
j) Soportará la capacidad de poner en listas negras a los host después de un número de conexiones TCP consecutivas inactivas configurables por "EL PROVEEDOR"
k) Soportará el bloqueo de solicitudes DNS malformadas en el puerto 53 que no cumplan con el estándar RFC
l) Autentificará solicitudes DNS desde el host origen y eliminar aquellas que no puedan ser autentificadas dentro de un tiempo específico
m) Limitará el número de consultas DNS por segundo a una velocidad configurable por el Licitante
n) Bloqueará el tráfico desde cualquier host que genere más solicitudes DNS fallidas consecutivas del límite configurado y poner al host origen en una lista negra

o) Configurará expresiones regulares para suprimir el tráfico DNS específico con los encabezados que coincidan con las expresiones
p) Detectará y eliminará 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
q) Bloqueará hosts que excedan un umbral configurable para el número total de operaciones por segundo por servidor destino
r) Suprimirá paquetes HTTP específicos según los encabezados HTTP coincidentes con hasta 5 expresiones regulares configurables
s) Normalizará el tráfico que coincida con una expresión FCAP específica, y suprimir el tráfico que exceda la tasa configurada. Las expresiones FCAP soportará la selección de los campos de encabezado IP y campos de los encabezados en capa 4 (UDP y TCP)
t) Detectará y bloqueará las inundaciones de SYN's TCP por encima de la tasa configurada
u) Detectará y bloqueará las inundaciones ICMP por encima de la tasa configurada
v) Bloqueará el tráfico procedente de fuentes que interrumpen reiteradamente solicitudes HTTP
w) Bloqueará el tráfico originado por BOT's según las firmas proporcionadas por el sistema
x) Activará las nuevas técnicas de defensa actualizando las firmas que serán mantenidas por el equipo de investigación del fabricante 24x7
y) Actualizará automáticamente sus firmas de protección de ataques periódicamente a intervalos configurables o de forma manual
z) Actualización de firma de protección de ataques a través de servidores proxy
aa) Configuración de protecciones predefinidas asociadas con servicios específicos, como Web, DNS, VoIP o un servidor genérico
bb) El sistema permitirá que los parametros de protección sean cambiados mientras la proteccion esta corriendo
cc) El sistema podrá bloquear tráfico por país de origen

3 2 Continuidad del Servicio Multifuncional do Segundad

Se requiere dar continuidad a la solución de protección de los servicios de la SHF multifuncional (UTM) el cual incluya servicios de Firewall, VPN, filtrado de co Aplicaciones y Control de Ancho de Banda características de un equipo Web, IPS, DLP, Control de con ias de conten.do

Se requieren 3 sistemas independientes:

1 Clúster de Firewalls (UTM) configurados en HA para protección de Internet, instalados en el nodo principal de la SHF

1 Cluster de Firewalls (UTM) configurados en HA para protección de la red interna de la SHF, instal el nodo principal de la SHF

1 Firewall standalone para protección de la conexión a Internet, instalado en el sitio DRP de la S ORP

1 Firewall standalone para protección de la conexión a Internet, instalado en el sitio PCN de la SHF

La administración de los equipos será realizada por la SHF, sin embargo, "EL PROVEEDOR" deberá continuar proporcionando los siguientes servicios de aprovisionamiento y soporte, los cuales deberán estar incluidos en el costo mensual del servicio:

- Aprovisionamiento de los equipos UTM en un esquema de cobro mensual fijo basado en servicios
- Instalación. Los servicios auxiliares como rack, energía eléctrica, tierra física, etc., serán proporcionados por la SHF
- Pruebas y puesta en producción. La SHF proporcionará la configuración inicial de los equipos y en conjunto con "EL PROVEEDOR" se realizarán las pruebas previas al paso a producción
- Mesa de ayuda para soporte técnico remoto y/o en sitio para resolución de problemas, ayuda en la aplicación de configuraciones o dudas técnicas en un esquema 7*24*365
- Mantenimiento preventivo, uno anual
- Mantenimiento correctivo y reemplazo de equipo en caso de falla
- Se deberán almacenar y registrar las bitácoras de eventos de los componentes que formen parte de la solución en un repositorio por un tiempo mínimo de 6 meses

- Se deberán almacenar los respaldos de configuración de los componentes que formen parte de la solución en un repositorio por un tiempo mínimo de 6 meses

debera implementar y habilitar un mecanismo de autenticación, autorización y registro de cambios (Accounting) en dispositivos que formen parte de la solución

En caso de una indisponibilidad total o parcial del servicio, se cobrará una pena de 5 al millar sobre el costo del servicio afectado, por cada hora de indisponibilidad mensual

En caso de requerir algún tipo de soporte a la mesa de ayuda, ésta deberá ser atendida en un plazo máximo de 24 horas, después de su notificación. Se cobrará una pena de 5 al millar sobre el costo mensual del servicio afectado, por cada día adicional sin atención del requerimiento

Se
OS

Los equipos deberán ser instalados, configurados y puestos en operación al 100% para iniciar el pago d servicios. El tiempo máximo para estas actividades será de 45 días a partir del fallo

anc srensab.e te:r.olog.a to:almente adac,table a «as neces%laaes de la
en su total<ac centtaaradame"te desde ura cansoia con .a 3': ta y
soorec,vga operactona:

Dicha solución debe ser sumamente flexible, permitiendo que se añadan nuevos módulos de seguridad sin la necesidad de agregar nuevo hardware / software o complejidad a la administración. La tecnología debe contemplar al menos los siguientes módulos de seguridad y administración: Firewall, VPN, IPS, Filtrado web, control de aplicaciones, control de ancho de banda, antimalware y antispyware y protección a fuga de información, todas ellas con la capacidad de instalarse en un solo dispositivo sin la necesidad de usar hardware, software o herramientas de terceros para su funcionamiento. La tecnología deberá incluir y operar al menos con las siguientes características:

a) Debera de integrar el soporte a la tecnología de aceleración por hardware
b) Deberá soportar Alta disponibilidad en sus modos Activo-Activo o Activo-Pasivo
c) La solución deberá contar con las siguientes certificaciones:
   - ICSA
   - Common Criteria EAL4 o superior
   - FIPS 140 –Level 2 o superior
d) Estar en el cuadrante de líderes o retadores de Gartner para el rubro de UTM por sus siglas en inglés, el más reciente divulgado a la firma del contrato
e) Deberá soportar y operar con al menos las siguientes tecnologías de red: Ethernet, Fast Ethernet, Gigabit Ethernet y 10G Ethernet
f) La siguiente tabla muestra las capacidades que se deben considerar para dimensionar dicha tecnología:
   - 12 interfaces 10/100/1000 (RJ45)
   - Firewall Throughput 12 Gbps
   - Sesiones concurrentes 3,000,000

Modufo Firewall

nódulo deberá incluir y operar al menos con las siguientes características:

a) Tecnología de QoS basada en colas inteligentes, Diffserv, TOS.
b) Monitoreo gráfico en tiempo real del tráfico de QoS que está circulando por el equipo.
c) Modificar el MTU para evitar problemas de fragmentación de paquetes encriptados.
d) Soportar valores de MTU mayores a 1500 bytes, para incrementar el rendimiento de interfaces gigabit, permitiendo modificar el MSS.
e) Detección de ataques de red y nivel aplicativo, protegiendo al menos los siguientes servicios: Aplicaciones Web, Servicios de correo (E-mail), DNS, FTP, servicios de Windows (Microsoft Networking), Voz sobre IP (H.323, SIP, MGCP y SCCP/Skinny) y Servicios de Videoconferencia.
f) Detección y rechazo de ataques conocidos y desconocidos, protegiendo al menos de los siguientes:
   - Suplantación de IP (IP Spoofing)
   - Inundación de paquetes con SYN (SYN Flooding)
   - Rastreo de puertos abiertos (Port Scanning)
   - Ping de la muerte
   - Inundación de ICMP (ICMP Flood)

El
   - Cross-Site-Scripting
   - Además de gusanos como Code Red, Nimda, bugbear, Slammer y otros.

g) Los ataques contra los que se protege deberán ser actualizables en línea (vía Internet) y esta capacidad debe estar incluida e integrada dentro del mismo Firewall.
h) Dentro del mismo Firewall contar con detección de ataques de tipo:
   - Servidores Web
   - Servidores de correo
   - DNS evitando la ejecución de código malicioso
   - Ataques basados en fragmentación de paquetes
   - Inserción de scripts
   - Robo de información y credenciales
   - Ataques HTTP provocados por gusanos y malware
   - Método para bloqueo sobre mensajería instantánea de al menos las siguientes opciones:
     a. Video
     b. Voz
     c. Aplicaciones compartidas
     d. Transferencia de archivos
     e. Asistencia remota
i) Proteger a los clientes de ataques IP-spoofing.
j) Basado en la tecnología conocida como "Stateful Inspection".
k) Proteger implementaciones de VoIP, soportando en todas sus versiones: SIP, MGCP, SCCP y servicios de Videoconferencia.
l) Contar con el licenciamiento necesario para la activación de los siguientes protocolos de enrutamiento en IPv4 e IPv6: RIP, OSPF, BGP y MULTICAST para IPv4.
m) Capacidad de enrutar selectivamente tráfico hacia Internet para ambientes Multihoming (dos ISPs).
n) Protocolos LAN: 802.3ad, 802.1q.
o) Tecnología IPv6: Dual Stacking firewall y VPN, Túneles IPv4 desde IPv6.
p) La solución deberá contar con terminadores de túneles VPN y traducción de direcciones (NAT, PAT).
q) Implementar y operar reglas aplicadas a intervalos de tiempo específicos.
r) Controlar los accesos por medio de políticas específicas.
s) Almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
t) Integrar la solución con Directorio Activo u Open LDAP para crear reglas de control de aplicaciones en usuarios, grupos de usuarios, máquinas, dirección IP, redes y todas las opciones combinadas.
u) Conectarse en modo transparente (bridged mode).
v) Controlar el acceso a archivos compartidos de Microsoft usando CIFS.
w) Poner en cuarentena a equipos que se consideren maliciosos a través de la política del firewall.
x) Mecanismos de alarmas y avisos, ante violaciones a políticas o eventos del sistema.

Modulo de Filtrado do Contonido Web

El módulo deberá incluir y operar al menos con las siguientes características

a) Basado en categorías y debe poderse incluir como un bloque más
b) Permitir únicamente el tráfico explícitamente autorizado por la SHF hacia Internet
c) 100 millones de sitios web distribuidos en 70 categorías preconfiguradas, incluidas las siguientes:
    - Banners y publicidad
    - Narcóticos
    - Sitios de almacenamiento personal de archivos y datos
    - Sitios de armas y municiones
    - Sitios de chateo por Internet
    - Sitios de compartido de archivos P2P
    - Sitios de compras y subastas
    - Sitios de contenido adulto o sexual
    - Sitios de descarga de audio
    - Sitios de descarga de software gratis o pago
        - Sitios de hackers
        - Sitios de ilegales
        - Sitios de juegos o apuestas en línea
        - Sitios de proxies públicos usados para evitar proxies corporativos (Proxy avoidance)
        - Sitios de radio y televisión en línea
        - Sitios hacia los cuales los spyware, addware y keyloggers envían los datos recolectados de las víctimas
        - Sitios o páginas de correo electrónico vía Web
        - Sitios personales y bloggers
        - Sitios que contienen video o audio (streaming), aunque pertenezcan a otra categoría, tal como noticias, deportes, en base a filtrado por tipo de archivo
        - Sitios sobre alcohol y tabaco
        - Sitios sobre violencia y terrorismo
d) Mecanismo que permitan al administrador, negar o permitir URLs específicos, que no necesariamente están definidos en una categoría, para poder ser utilizados en la definición de nuevas reglas
e) Bloqueo de páginas que pertenezcan a categorías permitidas, pero cuya URL posea ciertas palabras clave
f) Acceso a páginas de ciertas categorías, pero bloquear el intento de ciertos tipos de archivo (tales como video, audio, archivos comprimidos, ejecutables, documentos u otros) desde dichas páginas
g) Técnicas para detectar código malicioso en archivos que se estén descargando y cancelar la descarga, informándolo al usuario
h) El servicio de navegación segura deberá contener el análisis dinámico (en tiempo real) de contenido de sitios web
i) Opción de modificar la notificación de bloqueo y redireccionar al usuario a otra página
j) Bloquear granularmente sitios basados en Web 2.0
k) Identificar y bloquear herramientas de 'proxy bypass' sobre protocolos estándar y no estándar (sin la necesidad de instalar un agente en los hosts o licencias adicionales)
l) Bloquear Malware sobre sitios Web
m) Método dinámico en la nube para la categorización de los sitios Web existentes y nuevos sitios emergentes
n) Inspeccionar el tráfico HTTPS haciendo un man in the middle entre los usuarios internos e Internet, para hacer inspección del contenido en texto claro, sin la necesidad de utilizar herramientas de terceros, servidores, licencias adicionales o agentes
o) Cifrar las autenticaciones de usuarios con LDAP y AD

Modulo de IPS

a) Opción de permitir el paso del tráfico en el segmento de red sin afectar el funcionamiento de la red (Bypass)
b) Actualizaciones periódicas durante la vigencia del contrato de nuevas definiciones para protección contra spyware y virus, las actualizaciones deberán realizarse de forma automática programada por fecha y hora
c) La actualización de las nuevas definiciones de spyware, virus y variantes deberá aplicarse sin interferir en la operación del equipo y sin necesidad de reiniciarlo
d) Realizar un monitoreo transparente para los usuarios donde de forma automática bloquee ataques maliciosos y preservando la disponibilidad del ancho de banda de red
e) Filtros/firmas en modo bloqueo sin necesidad de periodos de aprendizaje ni afinación por parte del operador
f) Inspección de tráfico IPv4 en dispositivos Móviles (2G/3G/4G)
g) Detectar y bloquear tráfico peer-to-peer incluso si la aplicación utiliza cambio de puertos
h) Detectar y bloquear aplicaciones que realicen control remoto incluyendo aquellas capaces de hacer Tunneling
i) Funcionamiento activo semejante al de prevención en línea, pero sin bloquear tráfico. Sólo alerta que eventos serían bloqueados
j) Creación de reglas y filtros de acceso por Adaptador, VLAN, Protocolo, Origen y Destino
k) Protección con base en servicios de reputación IP y de DNS para eliminar conexiones de origen maliciosas de Internet personalizadas por el usuario, ejército de bots, malware, atacantes conocidos y exploits
l) Protección para servidores Web contra ataques de inyección de SQL
m) Tecnología de detección de Reputación de Archivos, IP, aplicaciones y protocolos

n) Detección de ataques independiente del sistema operativo
o) Tener la información de contacto de los usuarios que están siendo atacados
p) Los eventos de seguridad mostrados deberán mostrar el usuario que está generando o recibiendo el ataque y generar una alerta o tomar acciones en base al perfil del usuario en cuestión
q) Tecnologías de detección las cuales se mencionan de manera enunciativa mas no limitativa
   - Permitir la identificación del protocolo usado en la mayoría de las conexiones que se inspeccionen (Análisis de contenido)
   - Identificar de protocolos, aunque estos estén encapsulados (Protocol Tunneling Recognition)
   - Análisis heurístico
   - Detección de escaneo de puertos (Port Probes)
r) Protocolos y tipos de archivos soportados los cuales se mencionan de manera enunciativa mas no limitativa
   - SIP
   - IP
   - TCP
   - UDP
   - Java script
   - HTML
s) Detección de ataques desconocidos o variaciones de ataques conocidos a partir de firmas basadas en vulnerabilidades
t) Reensamblado de paquetes y sesiones fragmentadas
u) Detección de anomalías de tráfico a partir de análisis estadístico
v) Operar sobre firmas definidas por el usuario mediante el uso de regular expressions
w) Activar la captura de paquetes para protecciones específicas con el fin de tener análisis forenses
x) Bloquear propagación de gusanos, virus, backdoors, port sweep, port scanning, troyanos previniendo la infección de otros equipos y consumo de ancho de banda
y) Reconocer anomalías de tráfico como: umbrales de protocolos (paquetes, bytes, conexiones, etc.), análisis de patrones de tráfico, análisis de paquetes anormales
z) Protección contra ataques en capas aplicativas contra PHP (include, inyección, evasión etc.), Cross Site Scripting y filtros contra inyección de SQL
aa) Filtros contra ataques VoIP incluyendo los protocolos SIP, H323, Skinny, MGCP y servicios de Videoconferencia
bb) Técnicas de detección basadas en anomalías de protocolos
cc) Detectar y proteger contra anomalías estadísticas, protocolos y aplicaciones
dd) Ofrecer protección contra ataques de inundaciones de conexiones establecidas y conexiones por segundo
ee) Instalarse y proteger contra ataques en ambientes asimétricos
ff) Deberá de poder soportar tráfico IP de-fragmentado y tener la capacidad de reensamblar los paquetes antes de enviarlos a su destino
gg) Proteger servidores web contra ataques de XSS, PHP file, inyección de código, fallas de inyección, ejecución de archivos maliciosos, XSRF, referencias a objetos inseguros directos, autentificación rota, manejo de sesiones, almacenamiento criptográfico inseguro, comunicaciones inseguras, falla en la restricción de accesos URL

Modulo de Control de Aplicaciones

Ei
módulo deberá incluir y operar al menos con las siguientes características
a) Controlar y bloquear en tiempo real aplicaciones independientemente del puerto que utilicen
b) Identificar, autorizar, bloquear y limitar el uso de aplicaciones. Deberá contar con una base de datos mínimo 1000 aplicaciones
c) Controlar y bloquear al menos las siguientes aplicaciones, las cuales se mencionan de manera enunciativa mas no limitativa
   - BOTNET
   - ECONOMIA Y NEGOCIOS
   - MENSAJERIA INSTANTANEA
   - EMAIL
   - JUEGOS
   - MEDIA

- SOCIAL MEDIA
- NETWORK-SERVICE
- P2P
- PROXY
- ACCESO REMOTO
- VOIP
- WEB
- UPDATE

d) El control y bloqueo de protocolos deberá permitir la definición de políticas mínimo por usuario grupo y rango de direcciones IP
e) Controlar y bloquear las siguientes excepciones de los protocolos
   - Creación de protocolos personalizados
   - Soportar la apertura de otros puertos cuando sea requendo por innovación tecnológica
   - Soportar el protocolo HTTP sobre puertos no estándares (diferentes a 80 y 443) como funcionalidad adicional al soporte de los puertos estándares 80 y 443
f) Contener descifrado de SSL/HTTPS para revisión del contenido

Modulo de Control de Ancho de Banda

El módulo deberá incluir y operar con al menos las siguientes características

a) Asignar parámetros de 'traffic shapping' por usuario, grupo, dirección IP, rango de direcciones IP, categoría, aplicación
b) Políticas y/o configuraciones para asignar ancho de banda, de manera enunciativa más no limitativa por: usuario, grupo, dirección IP, rango de direcciones IP, categoría, aplicación
c) Priorizar el tráfico por categoría, contenido web, IP o grupos de IP's para las aplicaciones críticas definidas por la SHF, garantizando el ancho de banda
d) Asignar ancho de banda por aplicación controlando el tráfico por tipo de prioridad

Modulo de PrcvenciOn de Fuga de InformaciOn Pertmctra! (OLP)

a) Deberá ser capaz de bloquear fuga de información accidental o malintencionada en la red de datos en al menos los siguientes protocolos HTTP, HTTPS, SMTP y FTP sin la necesidad de instalar agentes sobre servidores proxy, servidores de correo o servidores de FTP
b) Deberá trabajar en "Modo Aprendizaje" o monitoreo, es decir, que la solución aprenderá la acción tomada con la primera interacción y la recordará para los siguientes eventos similares
c) Deberá integrarse la solución con directorio activo y base de datos de LDAP
d) Deberá proveer visibilidad de la situación actual de la red, mostrando eventos de seguridad importantes asociados a los sistemas críticos de la organización
e) Deberá contar con interfaz gráfica en tiempo real, aislando y resaltando eventos críticos para reconocerlos, evaluarlos y tomar acciones sobre ellos de manera que represente facilidad para evaluar eventos críticos, crear respuestas y remediar acciones
f) La solución deberá instalarse en el mismo equipo Firewall como una solución integrada
g) Deberá contar con políticas predefinidas que identifiquen al menos los siguientes tipos de datos para México
   - Datos de clave de elector IFE
   - Registro federal de contribuyentes – personas morales
   - Registro federal de contribuyentes – personas físicas
   - CURP
   - Información clasificada en español
h) Deberá soportar categorías de tipos de datos y grupos de tipos de datos
i) Deberá crear tipos de datos a la medida basados al menos en las siguientes características
   - Palabras clave (una o varias)
   - Plantilla de documentos
   - Atributos de archivos
   - Expresiones regulares
   - Combinación de tipos de datos
   - Diccionario de palabras
   - Fingerprint de archivos

j) Debera definir umbrales de coincidencias, es decir que rebasando cierto numero de incidencias el DLP tomara la acción definida en la política
k) Deberá soportar definición propia de datos
l) Deberá hacer inspección recursiva de contenido de archivos como .zip, RAR, tar, etc
m) Deberá definir un tamaño máximo de archivo que pueda ser procesado por detección de contenido
n) Deberá identificar tráfico HTTP/HTTPS sobre puertos no estándar
o) Deberá permitir manejo de cuotas por incidentes, para al menos los protocolos SMTP, HTTP, HTTPS y FTP
p) Deberá permitir cambiar o modificar las notificaciones hacia el usuario
q) Deberá poder definir acciones, para los protocolos HTTP, HTTPS, FTP y SMTP, que permitan la continuidad de la operación bajo condiciones extremas de carga
r) Deberá definir tipos de datos, basado en los atributos de un tipo de archivo, por ejemplo atributos específicos Office, vCalendar, Open Office, Quatro, Corel Draw, etc

O*ce

M6dulo de Antjwrus y Antispyware de Internet

El módulo deberá incluir y operar con al menos las siguientes características
a) Escaneo de virus y bloquear por lo menos con base a los protocolos POP3, FTP, SMTP, HTTP, HTTPS E IMAP, archivos de mensajería instantánea protocolos P2P, y todos los principales formatos de archivos comprimidos
b) Se deberá basar en patrones previniendo contra software espía y gusanos
c) Deberá permitir al administrador elegir la acción (block o pass) para al menos 50 diferentes tipos de archivos. La detección del tipo de archivo no debe ser basada en la extensión del mismo.
d) Descargas continuas, de manera que se comience a enviar el archivo escaneado antes de realizar el scan completo del archivo y de esta manera evitar timeouts cuando se realizan scans sobre archivos grandes
e) Escanear archivos de cualquier tamaño aun comprimidos con la opción de configurar un tamaño más pequeño de archivo. El administrador puede decidir el límite de tamaño de archivo antes de bloquearlo, o pasarlo sin ningun tipo de scan
f) Descompresión de archivos, con la opción de poder configurar el máximo nivel de anidación y de compresión para evitar ataques DoS
g) Deberá ofrecer al administrador la posibilidad de decidir que tipos de archivos pueden usar las descargas continuas, y cuáles deben ser escaneados, en su totalidad, antes de iniciar la transferencia al cliente
h) Escaneo por dirección, es decir que sea capaz de detectar y escanear archivos que se mueven en una dirección particular, por ejemplo de redes externas o cuando cruza una DMZ
i) Escaneo en tiempo real tanto de antivirus como de antimalware
j) Deberá tomar acciones cuando el escaneo de archivos falle o haya sobre carga en el motor de antivirus
k) Inspección sobre tráfico encriptado y descifrar los protocolos PPTP, L2TP, IPSec, SSL
l) Detección host infectados con bots, analizando el tráfico de la red utilizando una tecnología multicapa

Mödulo de identificacion

a) Proveer una forma de autentificación para los usuarios que no utilicen plataforma de Windows, además de dispositivos móviles.
b) Proveer configuración de acceso basado en tiempo para que los usuarios puedan entrar a los recursos de la red
c) Distinguir entre cuentas de servidores de aplicación y cuentas de usuario
d) Método de integración con el directorio activo sin usar las credenciales del administrador
e) Métodos de autentificación: nombre de usuario y contraseña, que podrá ser configurado en la base de datos interna de la herramienta, servidor de LDAP y servidor de RADIUS
f) Retener la identidad de los usuarios aun cuando estos cambien la dirección IP
g) Solicitar a los usuarios la autentificación después de un intervalo de tiempo
h) Verificar el estado de los controladores de dominio vía consola de comandos
i) Integración con el directorio activo sin la necesidad de instalar un agente en el servidor de dominio o en los equipos de los usuarios finales
j) Integración con otras soluciones como: control de aplicaciones y filtrado de URL

VPN S IPSEC Y SSL

a VPNs SSL sin cliente ova acceso remotQsoportando al menos 500 usuarios concurrentes

b) Soportar tuneles IPSEC de tipo sitio a sitio y cliente a sitio
c) Soportar tuneles L2TP sto
d) Soportar los sistemas operativos Windows en todas sus versiones a 32 bits y 64 bits IOS y Android
e) Soportar certificados PKI para la construcción de VPN'S cliente a sitio
f) Soportar algoritmos de cifrado AES DES y 3DES
g) Soportar distintos portales SSL que sirvan como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la plataforma
h) Capacidad de restringir las aplicaciones que pueden ser ejecutadas en el escritorio virtual

M6dulo de Administraciön. IntegraciOn y Reporteo

SQ a' memos s.gutentes Ce a
•,laves

c; monr:oreo Ce co; ,tcas oe farewa:u 'VPN•. de IPS de •so•, sea
y centra con 'oneonal•caoes de ce 'em
'"versos tara rode' N•'egar a traves r.c,r
manera
ae la consoa a jos camtu3s en ias quo
moo"'taeones
de
Genear Oitaccras que oe•ryutan on:ener segunaac como tecna
de ta red
Interface gra%za usuartc (GUI) mace'
Interface oasacta enea de cornanc'o
de 'a
rata „r.a
envetaca via SSI al cue
'a tarto equjrc mfe•renté 'a cons-c/a
Como en
Intexaun trensvaren:€: con que

Re dé er tea: Genera'
la de a

Se'a

a CLJ SS\' SSHv2 SSL SNMP V? tra%co a
de ant-' or •.oea la en tea: en

estan a Eaves equ.pc y al usuar•::

Genera' sc.ore e; estadé de de adomas voce' de
reoc.r•.es una so:a ventana er rex N' y estan
consumendo ancho Ce tanoa
Genera: act-Jones a€•rtas funcron de como on como
CPL' reacc16n sobre de usuar,os
accesc, no autoru•aeos el de ias sottwa'e .7,nes
•emota
Hace• actua•tzactooes de tvo One-Chu' ' en
Hace de cue de ia conso!a oe •sea men:s

como ecr SNMP

x) Diferenciar entre logs de usuarios regulares y los logs propios de la administración
y) Realizar un cambio automatico de logs basados en programaciones de tiempo o del tamaño del archivo
z) Asociar cada IP correspondiente a usuarios internos con su correspondiente nombre de usuario y nombre de máquina, tomando esa información del Active Directory, sin necesidad de instalar ninguna aplicación en el Domain Controller ni en las PCs de los usuarios
aa) Por cada coincidencia de una regla, se debe poder configurar alguna de las siguientes opciones Log, Alert, Send and SNMP trap, send and email
bb) Proveer al menos la siguiente información por cada equipo Sistema Operativo, Uso de Memoria, CPU
cc) Proveer el status de cada uno de los componentes del equipo (firewall, VPN, cluster, antivirus, etc.)
dd) Gráficas predefinidas de monitoreo vs la evolución del tiempo, del tráfico y los contadores del sistema, top de reglas de seguridad, top de usuarios P2P, túneles de VPN, tráfico de red, etc Debe proveer la opción de generar gráficas personalizadas
ee) Grabar las vistas de tráfico y contadores del sistema a un archivo, para posteriormente poder verlo en cualquier momento
ff) Programar backups en uno o más gateways
gg) Debe incluir un sistema de control de cambios integrado al servidor de administración
hh) Generar reportes de cambios realizados durante una sesión, para control del administrador y de los auditores

2 2 3 Continuidad del Servicjo de WAF (Firewall para Aplicac/onos Web)

"EL PROVEEDOR" continuará considerando una solución que ofrecerá protección a nivel capa 7 que garantice la seguridad de las aplicaciones web de SHF, mediante la automatización de la seguridad web, implementación flexible y transparente con una protección global y baja carga administrativa que asegure las bases de datos mediante el bloqueo de amenazas, inspeccionando peticiones desde Internet e impedir que el tráfico malicioso alcance la aplicación origen garantizando la disponibilidad, confiabilidad e integridad de los servicios sustantivos

Caracter'sticas Generaies

La tecnolog•a tncluira y operará al rneoos con las siguientes caracteristicas.

a) Medidas de seguridad a nivel de los flujos de transacciones HTTP y HTTPS de los servicios publicos en internet, sobre la capa de Aplicación
b) Descubrimiento, identificación y evaluación proactiva, con el fin de mitigar las amenazas de seguridad y las vulnerabilidades, evitando así el robo de datos y la manipulación de la información de SHF
c)

Throughput	Transacciones por segundo
300 a 500 Mbps	15,000 a 25,000

Caractori%ticao Tecnicas

La tecnologia •ncluira y operara at meno% con las Siguientes caracteristicas:

a) Las soluciones tipo I y II contaran con fuentes de poder redundantes
b) Con las siguientes Opciones de implementación:
   - Capa 2 de manera transparente para un mejor desempeño
   - Proxy inverso y proxy transparente
c) Fuera de Linea con la finalidad de mantener monitorización y análisis Auto-aprendizaje sobre el comportamiento de los usuarios, que permita hacer el descubrimiento de la estructura y patrones de uso de las aplicaciones Web a ser protegidas
d) Detectará, alertará y bloqueará ataques de capa 7, los siguientes son enunciativos mas no limitativos
   - SQL Injection
   - Cross Site Scripting
   - Directory Trasversal
   - Site Reconnaissance
   - Search Engine Hacking
   - Brute Force Login
   - Access Rate Control
   - Shema Poisoning

- Xml Parameter Tampering
- Xml Intrusion Prevention
- Wsdl Scanning
- Recursive Payload
- External Entity Attack
- Buffer Overflows
- Denial Of Service

e) Inspeccionará y auditará trafico SSL identificando errores de aplicación
f) Inspeccionará y auditará todo el tráfico HTTP identificando errores de aplicación
g) Mitigación de ataques automatizados como robots a gran escala con la capacidad de bloquear de manera rapida y precisa las conexiones sospechosas.
h) Listas Blancas/Negras de URL s e IP s para inspeccionar o bloquear peticiones a URL s é IP s específicas
i) Reputación de IPs y geolocalización
j) Normalización de datos codificados
k) Generará eventos y alertas pero que no realice ningún bloqueo real para facilitar la afinación y prueba de nuevas políticas
l) Creación de políticas de seguridad usando como criterio cualquier combinación de la menos los siguientes elementos
   - URL
   - HTTP
   - Header HTTP
   - Response
   - Pais de origen
   - Usuario Web
   - Cookies
   - Tiempo y tamaño de la respuesta HTTP
m) Soportar al menos los siguientes métodos de autentificación
   - De doble factor
   - LDAP Directorio Activo
   - Certificación de clientes SSL
n) Métodos de HEALTH CHECK tales como
   - PING
   - ICMP
   - HTTP
o) Interfaz de usuario web HTTP, HTTPS
p) Registro y monitorización SNMP
   - Syslog
   - Notificaciones vía correo electrónico
   - Capacidad de graficar
   - Consola de eventos en tiempo real
q) Al menos contara con la certificación ICSA LABS de WEB APPLICATION FIREWALL (WAF)

AdministraciOn. integraciOn y reporteo

a) Administración por SSH, CLI, HTTPS SNMP v3 proporcionando al menos tres cuentas de solo lectura para el personal responsable que SHF designe
b) Administración centralizada bajo las siguientes características
   - Cambiará la contraseña para tener acceso a la interface de administración, además de limitar el acceso a la misma, así como también el introducir la dirección de correo electrónico de los administradores que recibirán las alertas del sistema
   - Visualizará estadísticas numéricas y gráficas de sitos bloqueados por hora y por dia, contener información de los equipos atacados, (hostname- IP) Proporcionará el porcentaje de almacenamiento del firmware, carga del sistema y estado del mismo
   - Incluirá una pantalla de log´s donde se pueda visualizar la información de las conexiones, la fecha en que se realizó, IP origen, URL destino, contenido, acción realizada, con filtro para localización de registros por solicitudes permitidas, solicitudes bloqueadas, descarga de spyware, protocolo spyware, spyware website, descarga de virus identificados
   - Incluirá una pantalla desde donde se puedan visualizar reportes por tipo, con rangos de fechas y su visualización en línea
c) Proporcionará al menos los siguientes reportes

- Top por puerto, protocolo y/o servicio
- Top por IP origen y destino
- Top por tipo de transmisión multicast, pudiéndose proporcionar este reporte en un componente distinto del servicio WAF
- Top por severidad
- Top por acción tomada por el equipo

3.3.4 Continuidaa del Servicio dc IPS

Caractonst'cas töcn.cas

La tecnologia incluirá y operará al menos con las siguientes caracteristicas:

a) Basado en hardware de propósito especifico para hacer inspección a profundidad, no será unicamente una solución de software. El IPS inspeccionará los paquetes de capa 2 a capa 7 del modelo OSI sin afectar el desempeño de la red.
b) La siguiente tabla muestra las caracteristicas generales que "EL PROVEEDOR" considerará para la tecnologia de IPS.

Throughput Real '0	Sesiones Concurrentes	Interfaces
Gnos		

Caractor•stjcasTécnic

ea sotuoon •ncluira y operara al menos con tas siquientes caractensticas tecnicas_

a) Latencia bajo carga de red menor a 150 microsegundos.
b) Capacidad de manejar HA.
c) Opción de permitir el paso del tráfico en el segmento de red sin afectar el funcionamiento de la red (Bypass físico) en cada interface para garantizar alta disponibilidad y se activará en los siguientes casos:
   - Perdida de energia eléctrica.
   - Falla lógica en la interface de control.
   - Pérdida de conectividad con la tarjeta madre del dispositivo.
   - Colapso del sistema operativo.
d) Ruteo asimétrico.
e) VLANs, incluyendo frames 802.1q y Sensores Virtuales internamente en el equipo.
f) Politicas de seguridad específicas de acuerdo a la posición de la plataforma de IPS en la red y de que dispositivos estará protegiendo (Core, Perimetro, DMZ).
g) Interface de monitoreo en modo stealth, sin stack de TCP/IP en la interfaz.
h) No requerirá la modificación de los routers o switches para su implementación, funcionando como un puente en la red.
i) Interfaces de red necesarias para su operación protegiendo todas las zonas del Firewall (LAN, WAN, DMZ).
j) Translación de VLANs. Es decir la capacidad de inspeccionar y traducir el tráfico entre diferentes VLAN o interfaces VLAN.
k) Actualizaciones periódicas durante la vigencia del contrato de nuevas definiciones para protección contra spyware y virus. las actualizaciones se realizarán de forma automática, programada por fecha y hora.
l) La actualización de las nuevas definiciones de spyware, virus y variantes se aplicarán sin interferir en la operación del equipo y sin necesidad de reiniciarlo.
m) Contará con las siguientes certificaciones:
   - Certificación de NSSLabs
n) Está reconocido como lider dentro del cuadrante magico de Gartner para el rubro de Network Intrusion Prevention Systems 2012.
o) Basado en un marco que permitirá ampliar la protección con servicios de seguridad, integración con soluciones de terceros, diversos paquetes de filtros para la protección y otros personalizados de acuerdo a las necesidades de SHF.
p) Realizará un monitoreo transparente para los usuarios donde de forma automática bloquee ataques maliciosos y preservando la disponibilidad del ancho de banda de red.
q) Filtros/firmas en modo bloqueo sin necesidad de periodos de aprendizaje ni afinación por parte del operador.

r) Protección contra ataques de día cero y avalado por un programa reconocido para el manejo de este tipo de ataques a nivel mundial el cual debe de ser referenciable públicamente
s) Inspeccionara simultaneamente cargas útiles tanto en IPv4 como en IPv6
t) Inspeccionará IPv6 con VLANS
u) Inspección de tráfico IPv4 para Redes Móviles (2G/3G/4G). La inspección de tráfico se realizará sobre equipos con tecnologías 2G/3G/4/G conectados a la red inalámbrica de SHF
v) Basado en la tecnología conocida como "Stateful Inspection"
w) Funcionamiento activo semejante al de prevención en línea, pero sin bloquear tráfico. Sólo alerta que eventos serían bloqueados
x) Creación de reglas y filtros de acceso, por Adaptador, VLAN, Protocolo, Origen y Destino
y) Protección con base en servicios de reputación IP y de DNS para eliminar conexiones de origen maliciosas de Internet personalizadas por el usuario, ejército de bots, malware, atacantes conocidos y exploits
z) Protección para servidores Web contra ataques de inyección de SQL
aa) Tecnología de detección de Reputación de Archivos, IP, aplicaciones y protocolos
bb) Detección de ataques independiente del sistema operativo
cc) Se mostrará para cualquier evento el origen y el destino del ataque o incidente de seguridad
dd) Tecnologías de detección las cuales se mencionan de manera enunciativa mas no limitativa
   - Identificar el protocolo a partir del puerto utilizado (Port Assigment)
   - Identificar los protocolos que utilizan puertos aleatorios (Port Following)
   - Permitir la identificación del protocolo usado en la mayoría de las conexiones que se inspeccionen (Análisis de contenido)
   - Identificar de protocolos aunque estos estén encapsulados (Protocol Tunneling Recognition)
   - Análisis heurístico
   - Detección de escaneo de puertos (Port Probes)
ee) Protocolos y tipos de archivos los cuales de mencionan de manera enunciativa mas no limitativa
   - SIP
   - IP
   - TCP
   - UDP
   - [illegible]
   - HTML
   - MSRPC, HTTP
ff) Detección de ataques desconocidos o variaciones de ataques conocidos a partir de firmas basadas en vulnerabilidades
gg) Reensamblado de paquetes y sesiones fragmentadas
hh) Detección de anomalías de tráfico a partir de análisis estadístico
ii) Operará sobre firmas definidas por el usuario mediante el uso de expresiones regulares
jj) Resistencia al menos a las siguientes técnicas de evasión, las cuales se mencionan de manera enunciativa mas no limitativa
   - IP fragmentation
   - TCP Stream Fragmentation
   - RPC Fragmentation
   - URL Obfuscation
kk) Activará la captura de paquetes para protecciones específicas con el fin de tener análisis forenses
ll) Bloqueará propagación de gusanos, virus, backdoors, port sweep, port scanning, troyanos, previniendo la infección de otros equipos y consumo de ancho de banda
mm) Reconocerá anomalías de tráfico como: umbrales de protocolos (paquetes, bytes, conexiones, etc.), análisis de patrones de tráfico, análisis de paquetes anormales
nn) Protección para sistemas SCADA y tener la capacidad de proteger al menos los siguientes protocolos como DNP3, MODBUS, ICCP, MMS, siendo esta funcionalidad opcional
oo) Protección contra ataques en capas aplicativas contra PHP (include, inyección, evasión etc.), Cross Site Scripting y filtros contra inyección de SQL
pp) Filtros contra ataques VoIP incluyendo los protocolos SIP, H225, H323, Skinny, MGCP y servicios de Videoconferencia
qq) Técnicas de detección basadas en anomalías de protocolos
rr) Detección de ataques DOS/DDoS
ss) Detectará y protegerá contra anomalías estadísticas, protocolos y aplicaciones
tt) Protección contra ataques de inundaciones de conexiones establecidas y conexiones por segundo
uu) Capacidad de realizar los siguientes filtros
   - Plataforma Oracle

w)

Contra ataques mezclados (Blended)

- Contra troyanos
- Protección contra Fragroute y Whiske (Fragroute. Es una herramienta que utiliza técnicas de evasión realizando ataques que permiten forzar la fragmentación contra un sistema en concreto así como otros tipos de ataques de overlapping basados en TCP. Whiske. Permite realizar escaneos para identificar servidores de HTTP y sus vulnerabilidades de seguridad conocidas y ejecutar peligrosos escripts/programas maliciosos
- Exploit y código malicioso
- Puertas Traseras
- Políticas de Seguridad
- Ataques de reconocimiento
- Técnicas basadas en anomalías de protocolos
- Protección para análisis Forense
- Protección contra el spyware
- Protección contra el Phishing
- Protección contra gusanos como MS-Blaster, Slammer, Welchia, Sobig, BugBear, Nimda, Code Red y otros.
- Bloquear o identificar programas de mensajería instantánea (IM)
- Bloquear o identificar programas Peer to Peer (P2P)
- Bloquear o identificar programas Streaming

vv) Instalarse y proteger contra ataques en ambientes asimétricos.

ww) Podrá soportar tráfico IP de-fragmentado y tener la capacidad de reensamblar los paquetes antes de enviarlos a su destino.

xx) Técnicas de Normalización de Tráfico y Limpiado de la red de paquetes que consumen recursos en la red (IP/TCP/UDP/ICMP/ARP)

yy) Protegerá servidores web contra ataques de XSS, PHP file, inyección de código, fallas de inyección, ejecución de archivos maliciosos, XSRF, referencias a objetos inseguros directos, autentificación rota, manejo de sesiones, almacenamiento criptográfico inseguro, comunicaciones inseguras, falla en la restricción de accesos URL.

zz) Detección y bloqueo contra las siguientes aplicaciones P2P, IM, Streaming, Proxy y en general aplicaciones Web no productivas.

aaa) Detección y bloqueo sobre ataques desconocidos o variaciones de ataques conocidos en VoIP

bbb) Detectara anomalías o fragmentaciones ilegales en los protocolos y paquetes de Video

ccc) Criterios de cuarentena los cuales se mencionan de manera enunciativa mas no limitativa

- Dirección IP origen y destino
- Puerto o servicios
- Segmentos de red
- Dirección MAC
- Duración de la cuarentena

Admirustracion, integraciOn y Reporteo

a) Administración de forma centralizada y de manera independiente para SHF a través de una consola del mismo fabricante.

b) Integración de Syslog (número ilimitado de dispositivos).

c) Ajuste dinámico de severidad en los ataques, como resultado de la correlación de eventos.

d) Correlación de datos de vulnerabilidades.

e) Comunicación de datos en forma cifrada.

f) Generar reportes en formato texto y gráfico, con exportación a formatos HTML, PDF y CSV. SHF solicitará de acuerdo a sus necesidades las plantillas requeridas a "EL PROVEEDOR".

g) El envío de eventos relativos al performance y al funcionamiento del equipo será como mínimo a través de SNMP v3 y correo electrónico.

h) Medir el tráfico que pasa por las diferentes interfaces, los tipos y tamaño de trama, protocolos, y generar una representación gráfica de ellos mediante la consola de administración y reporteo.

i) Arquitectura modular, distribuida y multicapa.

j) Administración remota vía Web con interfaz gráfica, para el uso en modo de consulta de dispositivos y eventos de seguridad.

k) Realizará de manera remota y automática su actualización y configuración de políticas.

l) Soportará la creación de múltiples roles, en el cual se permita o niegue el acceso a los diferentes dispositivos, o se otorguen privilegios o no para la administración, visualización de eventos o generación de reportes.

m) Los datos que cursen por el dispositivo deben al menos ser almacenados en una base de datos relacional dentro de la misma consola de administración
n) Realizara automaticamente actualizaciones de software via remota o Web para asegurar una proteccion en tiempo real. Las actualizaciones aplicadas no deben requerir de la reinicialización del equipo
o) Proveerá información adicional sobre el evento recibido con una descripción del ataque y una liga de referencia
p) Mandara un TCP Reset asociado con un evento
q) Proporcionara reportes de los TOP más significativos de tráfico

3.3.5 Continuidad del Servicio de Protección Contra Malware

EcPRC3VEEOOR cont•nuarn nue y nacia Internet a {'aves inspeccion ae descartando las emena:a•, corneadas tasadas en "'mas ap•vc.ando rouns',lca ag'ewva en tosca se de manea y 'a de cerc y especi"cos euttanao en 'also•, 'a•sos e; sospechoso er un amtuen'e e/ de ta amena:a en OS "naies

Para se contempla'ô a' menos O

y c,oeava a menos can las

Se cor'%'dera tuna de a gror.orc,onar c:nva aescarqas 3e arcmvos y matware y sosoecnoso URL s dt,ersos de que evatue ts a'aaoes de tai manera cerm:ta rear .magenes de con los sistemas las e' tamt»en procesa: erma er, sanito. e,ecucsen y de cerc escataoen ae de a:aqu'.'

'loeva sera y SHE tesoetanoo 'os catos

s.gupente

erroteai.lzs

Puertos ut'izaoos e;

P'0õ-eso y te'

El caca: de emola: ccmrc.nom@rro s, ee.

a wen a'

La sera ne

Arcnwos

Arcnvvs Adore POP M•crvscft V,'ord Mecscft tuce! COM EXE

Arce.vcs corno son ZIP y

Contara con la caoactaaa y via era la se yavee„ Sorc- r:ara anâ'•s•!, sera cara: en'.recar todos los en ura como ewdencua y anahss lerenses

Contara CCJn ee la e' detectado

:omoamdos de arcntvc.s en rosca

cor ta arr:mvo como son a•crv entre o•.rcs

Con:ara con a un en (a sotre Cs penwt•endo cont.y con ana

a) Se contará con una consola que permita la administración y envió de actualizaciones a los equipos dedicados a la detección de malware distribuidos en la red
b) Se almacenarán todos los eventos generados en los equipos distribuidos en el entorno de red así como la capacidad de generar reportes basados en la información almacenada
c) Capacidad de integración con dispositivos de monitoreo y/o correlación de eventos mediante los estándares SNMP y RSYSLOG teniendo definidos parámetros de configuración para los más comunes
d) Capacidad para generar reportes estándar y ejecutivos donde refleje la operación de la solución

3 3.6 Continuidad del Servicio de COtre/aCiOn de Eventos

"EL PROVEEDOR" continuará ofreciendo a SHF una solución SIEM (Security Information Event Management, Información de Seguridad y Administración de Eventos) que permitirá la administración de eventos e información necesaria para el monitoreo, análisis, administración y reporteo identificando en tiempo real las amenazas, dotando de procesos, herramientas y flujos de trabajo para la contención oportuna de ataques, identificación de incidentes y riesgos potenciales para la infraestructura y los servicios tecnológicos de SHF. La solución será reconocida como líder dentro del cuadrante mágico de Gartner para el rubro SIEM, el más reciente divulgado a la fecha de la firma del contrato.

Dicha solución realizará la administración de toda la información de seguridad generada por todos los dispositivos de la infraestructura de red de distintos fabricantes y de "EL PROVEEDOR" mediante una aplicación inteligente que recopile, analice y correlacione los datos de todos los eventos de seguridad que se presenten dentro la red de SHF, utilizando bitácoras que generan los equipos. La solución consolidará automáticamente, administrará y escalará amenazas en tiempo real lo más próximo al ciclo de un posible ataque. Dicha información será manejada y almacenada en un histórico de hasta 3 meses en línea. Se incluirá el almacenamiento fuera de línea de toda la información colectada y generada por la solución de correlación, debido a que podrá ser solicitada y/o acceder en cualquier momento durante la vigencia del contrato.

La solución deberá permitir integrar las bitácoras de fuentes de información adicionales a las generadas por los dispositivos entregados por el proveedor, incluyendo activos internos de la SHF si es requerido. Las capacidades de la solución deberán ser al menos las siguientes:

Eventos por segundo sostenidos	Almacenamiento de Gestión
15,000	10 TB

La solución incluirá y operará al menos con las siguientes características:

a) Componentes dedicados a la recolección, normalización y categorización de eventos de seguridad, no utilizará agentes de ningún tipo para sus métodos de correlación y administración de log's.
b) Contará con sistemas de tolerancia a fallas tales como fuentes de poder duales y configuración de arreglo de discos.
c) Correlación en tiempo real y en memoria sin necesidad de consultar la base de datos para este propósito.
d) Correlación geográfica, es decir, utilizando las direcciones IP de Internet del evento o información de la ubicación del dispositivo para la configuración de reglas para alertas de eventos relacionados y que ocurran en distintas zonas.
e) Configuración ilimitada de reglas de correlación.
f) Integrar por lo menos los siguientes tipos de dispositivos y/o herramientas, las cuales se mencionan de manera enunciativa mas no limitativa:
   - Herramientas de análisis de vulnerabilidades públicas y comerciales, como: nessus y LanGuard.
   - Herramientas antivirus, como: Symantec, McAfee, Trendmicro, etc.
   - Dispositivos firewalls, como: Juniper, Cisco pix, Checkpoint, Netscreen, Fortinet, Palo Alto y McAfee.
   - Dispositivos IDS/IPS, como: Cisco, Netscreen, Source fire, Juniper, Tipping Point, McAfee, entre otros.
   - Routers & switches, como: Cisco y HP.
   - Syslog de plataformas Unix.
   - Windows eventlog.
   - Directorio Activo.
   - Filtrado de contenido web.

como Eochanpe v
oases t:ga'os

Ptva no "Stad0S o awe
"socsd•vos
'a Be eventos eventos
entre '05

E' e' de eventos ia ce gates
or.v"eg.andc ce log s tencrö ee awe
su en memento er
Eos

a a

ttavos c..taf•s mart-as de la cust0d•a desce ta even'o de raga
etaG* ee de atmacenam.ento y retencsOr de
Prueera eventos de con ia de eventc•s una proceso ae
JOS •n'er•az cvt›cas setan en y
de

Las
Reaqzarh en reai la de
tnformac.on En se analucen even•.os ics
de amena.•as Detector tos de segu',tac ,
amenazas aue vecoectan de

vulneraro.caoes .n'0'tnacon de :oras a/ a:acue y nose-vat-
•eat en es.'ts I"
v tasveara base de
la va sea de. n

Antes de -a :area de o score la
agreeata at

en iö ce :le• even:r.
V'es'0 G'se a
del ser a traves Ce

:fr• COO C

se de er sos

amena:as a' 'unal se comptometer la "e or a.--•.uc.
•toques 'eates
rata a-soc-acc cor cada ataxoe
J menos •as
ouncstcne foundscan

La de func•or.es
cuates seran env:adas a estDS oe za

Rea'zara dtmerswnes
de ae anafts•s y
'aus esa•uat de
estæa nasad,-.; en ft€mas de a de
calcu±cs
Lcr:'.ara con ur e". e'

tecn.cas de
evas:on as: a:aaues c.a

oe en tempo ae correlac•or es
colectores eventos ar.ah:at sos eventos ze
a amera:as o mas

Oe; n•ve• los •c.rsos eventos son e' ':'.e

asoaaaas

Antecedentes sc.nre e, destvmo o ambos

Se .nc:uven monitoree, e' uso

..•atts un de oirr:scer.amento para ja tasos un cara e: atmacenamien•.o de 'os conectores este repos".ono en so egemem:cs cada camços toc

La conso•a de basada en weo y su acceso a traves SSL a•3ema•, con aca tm•.ertaz una Oe comarac para su .J5uart3 er e' acceso para om:tar ao@r. O•..eoe c sts:ema que 'os agrupar de 'ermas

tase vocesr.as ub'cac;et' oe

E' C arn#ar la de

Sef•c-cueo ee .cr•, act,vos Seecc;on de jos en

Camena' ae las

nuevas oe

la fritas configurarse a aetas

al 515'.ema Oe

son iect'..ra •.av:•-- • ac-ceqo a 'a mediante Cuentas cor n:ema a a SHE La Paves de a SHF c:ei m•smt;

Se en la manoaies pa.•a y SHE a ins

oc.' una reco•ectanoc, se ae .rformac•on a' en 'ea; memooa estos e»ementos

ta ya atacan:e rato limnral ae forma sea e' D'-.atlvos

Para la AdministraciOn. Integracion Monitoreo y Reporteo:

"EL PROVEEDOR" llevará a cabo las siguientes actividades:

a) Configuración centralizada de log s operativos y de auditoria
b) Registro de acciones administrativas
c) Revisión local de cumplimiento con las políticas de seguridad
d) Identificación de activos
e) Amenazas identificando vulnerabilidades

Cara 3 u•.u3'OS en de rara analss sondo las cumes
y on de er oqenc:a contrato a ser se, eo cuaiaa.er
cara O fryense Paro toa' amacena•-.entt' necesano coe se 'ecueta para
remota y acc»ydo 10s

Seran ca;'aces de de 'es ct•versos segursau• er fecha doractn ongen de; EL se
PFOVEE
'Se 'as acoones se t'.aiar reocrzaeo oa'a 50 yC evitar que sur:ecav a cano
"e IOS em todos ya estatlec»dc oara 'a v actvldases ÇJL,eCan
en as' cata:oga'los Tamt:4" se
«cara Ia este

necesara para ia de: ataque de; %'c•: sera as'
su"cen'.e arf«rna' ta iP t.'
Ir.ciu•r necesanos a de red de SHF y detectar ameno:as
e!
ararcanoo ae segur•aac LAN servnores at"caclenes a
se tos 'asas trovocaaos o rrocesc,s

Ia de ln'otmac•t.n que le rec.or•.en os difererres se

•f%'dentes 10s 'esoonsat.•es a
c,orresponcente oe ta
'ed med'ar.:e
"e tes corvonen:es te de y
respues'as en "empo 'eal
'cs ce red ss•.emas segar.'ad y
retores camtvns v eventos aesarro;n de
o 'terlas euto
auartoea ae s

ae su

2cs; de even:os
Mane;ad"

Cc;eccitn ccyre'ac.on eventos y came•os

P dê reportes se '731caeores flave
reformance
en 'a anorrtyas en eventos 'e

un emace para .•ecc'eccton de eventos com ea fi" CQ r: e:

ar cerfrfc.acfo en 'a soluc;tn de y sera encargado de dar atencron en
sequmen',o ae
Servici0 de OperaciOn

Ooscnpcton del Sorvicio

'EL PROVEEDOR' tomará en consideración que se requiere cumplir con la atención, registro, resolución de incidentes, problemas y solicitudes de servicio, que permitan la continuidad operativa, en los niveles de servicio indicados, realizando monitoreo de la operación de la Red Privada Virtual y los elementos de Seguridad de SHF

3.4 Soporte Tecnico a 10s Servicios Contratados

"EL PROVEEDOR" debe considerar en su proposición los recursos técnicos y humanos necesarios para la prestación del soporte técnico en sitio y remoto 7x24 durante la vigencia del contrato para la atención de reportes a través de su Mesa de Ayuda para cumplir los niveles de servicio solicitados.

La decisión de realizar soporte en sitio o remoto mediante personal de "EL PROVEEDOR" obedecerá a la estrategia definida por éste para garantizar los niveles de servicio solicitados.

3'.1. Mantemmientos preventtvos. partes y refacciones

"EL PROVEEDOR" debe considerar en su proposición las tareas de mantenimiento preventivo y correctivo incluyendo la mano de obra, sustitución de partes y refacciones, viáticos que se generen, todo el equipamiento suministrado para la prestación de los servicios solicitados durante la vigencia del contrato, con el fin de mantener toda la infraestructura utilizada en la prestación de los servicios en las condiciones operativas óptimas para el cumplimiento de los niveles de servicio solicitados.

EL "PROVEEDOR" debe elaborar un calendario y plan de mantenimientos preventivos por lo menos una vez al año le será validado y autorizado previo a su ejecución por SHF.

3 4.2 Contro de operac•On de la Red (NOCI

"EL PROVEEDOR" deberá realizar el monitoreo permanente de los elementos de los nodos y servicios solicitados durante la vigencia del contrato con el fin de verificar el estado de cada uno de los elementos que los soportan y tomar las acciones necesarias en caso de presentarse un evento que ponga en riesgo la operación del servicio, para ello el Proveedor debe contar con un Centro de Operaciones de Red (Network Operation Center, por sus siglas en inglés NOC).

El NOC será el encargado de ejecutar al menos las siguientes actividades:

a) Monitoreo proactivo y en tiempo real de todos los elementos de los nodos y servicios solicitados.

b) Prevenir problemas potenciales a través del monitoreo proactivo.

c) Solucionar y aislar los problemas presentados en los elementos de los nodos y la prestación de los servicios.

d) Llevar a cabo las tareas de operación, administración y mantenimiento de toda la infraestructura necesaria en los elementos de los nodos y la prestación de los servicios.

e) Notificar oportunamente las fallas de los elementos de los nodos y los servicios al personal designado por la SHF por alguno de los siguientes medios: correo electrónico, mensaje de texto, llamada telefónica.

f) Ante eventos de falla que afecten considerablemente a los elementos de los nodos y los servicios, deberá generar los reportes asociados a estos eventos indicando las causas, afectación, solución y manera de prevenirlo.

g) El NOC deberá contar con el soporte de tercer nivel por parte de los fabricantes de los equipos y soluciones indicados en su proposición.

.4.2.1 Herramienta de Monitoreo

"EL PROVEEDOR" debe de proporcionar una herramienta de monitoreo para los enlaces contratados sin costo adicional a la SHF.

La herramienta de "EL PROVEEDOR" empleada para realizar las actividades de monitoreo deberá contar al menos las siguientes características:

a "EL PROVEEDOR" es responsable de la administración del hardware y software, así como del licenciamiento para el correcto funcionamiento. La herramienta debe estar disponible para consulta de información en todo momento.

b) Consolidar sistemas de administración heterogéneos en una sola pantalla única de gestión general de la red.

c) Generar información sobre el rendimiento, alarmas, comportamientos y tendencias de la red, así como crear, planificar, ejecutar y personalizar informes sobre la salud y rendimiento de los recursos de la red.

ae

d) Monitoreo del rendimiento de red, identificando tendencias importantes y emitiendo alertas cuando el comportamiento de la red se desvía de los patrones establecidos.

e) Gestión proactiva que permita resolver problemas de rendimiento antes de que afecten a los servicios solicitados.

f) El sistema deberá contar con la funcionalidad de análisis del performance de la red a nivel telecomunicaciones.

g) Presentar la información referente a los servicios solicitados por la SHF.

h) Monitoreo proactivo y en tiempo real de los elementos que integran la solución de los servicios contratados por la SHF.

i) Indicar de manera visual el estaco ae tos nc•sos fanas alarmas en distintos cobres

j) Capacidad de visualización de la información histórica del monitoreo de los element

k) Generación de reportes del estado actual de los elementos, su desempeño y tende

l) Grafica de actualización en tiempo real del estado de la red para las diferentes variables.

m) Colectar las siguientes métricas en tiempo real: Utilización de ancho de banda, Pérdida de paquetes, errores y Latencia.

n) Generación de graficas con las estadísticas de red descritas en el punto anterior, para periodos de tiempo parametrizables (1 día, 1 semana, 1 mes, etc.).

o) Almacenar las estadísticas de red por un periodo de 3 meses para consultas históricas.

"EL PROVEEDOR" debe de proporcionar las cuentas de acceso a la herramienta para generación de reportes y consultas, explotando todas las variables y funcionalidades de la herramienta de monitoreo, con la opción de parametrizar dichos reportes.

El monitoreo en tiempo real para la detección de alarmas y eventos de fallas se realizara al menos cada minuto, este mismo intervalo de tiempo será utilizado para la medición de los niveles de servicio.

"EL PROVEEDOR" debe configurar al menos una comunidad SNMP Ver. 3 con derechos de lectura, independiente a la comunidad que el Proveedor utilice para el monitoreo de los diferentes equipos de comunicaciones que formen parte de su servicio y se encuentren en instalaciones de la SHF. Esta comunidad tendrá como objetivo, monitorear todos estos equipos desde un sitio diferente al NOC, con uno ó más servidores de la SHF (o un tercero definido por ésta) el numero de comunidades será al menos uno.

AdministraciOn de 10s oquipos de Conectividad a traves det protocolo de AutenticaciOn. Autorizacion. Contabittzaci0n.

Habilitar e implementar el protocolo AAA en los equipos Switch y Routers que forman parte de los enlaces de interne en las 3 localidades, y del enlace LAN to LAN, así como también en los equipos Firewall de las 3 localidades.

Monitoreo de Red para 10s sitios con criticidad Media y Estandar

Se requiere una solución para monitoreo de tráfico en la red LAN e Internet compatible con las funciones port-mirroring y vlan-mirroring, la cual deberá ser instalada en el sitio principal y deberá tener la función de capturar tráfico en tiempo real, y crear reportes personalizados.

Soportar protocofos de lujos, tanto individualmente como en Cualqcu•er de eaoso 'equit•endo de a' menos un Colector deinc;uso en tasas de muchos protocolos de concurrentemente usados

NetFIow (veston 5, 7 and 9)

SampledNetFl

NetStrea?i

r.flow3

SteelF;ow

Blue Coat / Packeteer FOR enhanced now NEAR enhanced Net%ow

La solucion debe.

- Amacena' e• 100% de todos los datos reco;ectaaos Sir surnanzcYlC.'"1 el perodo de por menos año
- Ester para reenviar de e: 1009c. c "tracos por agente e•çcrtaoor a otras herramentas ee flujos
- Estar para recibir ftups con multoes puertos ces:.nos TCP

Soportar nomeraoc ce c:ases cte OOS

- Scoortar ei agrupam.ento de IPs}subnets para proveer vistas independientesEjemp:o por area'logar por tonctcn. hO%ts de la rea -geoen estar C.svon101e a pertenecer a
- Soportar agruparmento de 'nterfaces de red para proveer Incepend.erre'. E! WAN o Erfltc•o Data Center 'nterfaces deben poder pertenecer a grupos

'(0 IPv4

7ener la de crear apacactones donce se {a capactdac crear mapas a oarttr de los metoeos Hovs youps puertos de una de Apbcacones auto reconoctdas en el trafico del oc,mtye de una apizacon

ee rear de apgcaclones a traves ce un proceso que permita el mapeo de una apltcacvon ea capas, Incluyendo: ae entrega apircac'On iADCs} como FE, ce

- Tener ga cav3üdad ae crear Otzarra servtcjos ce monitoreo oor.ge se monitoreen todos vos corneonentes involucrados er +1 seiwc.o de una ap\'cacun como son usuarios. servugores web. balanceadores de ap';cacgon_ servoores ae autenticaccn base ce datos y sus deoendenctas entre ei'05

de carga, servidores servidores DNS, bas

- Tener la capacidad ante un cambio de d pizarra visualizar la

de envtar una rottftcacion maneta proact,va de cesempefto 3e un evento en progreso y en ena ta salud «se una aphcacor ounto a ounto • Reconocer automatcamente enhanced NetF kaw de equipoestén 'nspecconado a mvel profundo oe paquetes ÍDPI sus sqas en ingles)

ident'ftcarto correctamente y agrupar;o con interfaces de WAN de 'os daspos'tW05

- Soportar de.duphcacyon de fluJ05 de datos entre e»poractores cornc tambten de Itu'0S de datos entre agentes y también sensores que 'nspecc.onan el m•smo mentras mantene una precisa wsta de Eremplo desde tantos agentes como sea postle sm oreocuowse vo:umen de trafico no reportado
- Combinar flujo de datos con datos recolectados va sensoresen un sob reg:stro
- Reportar relaciones ae dependencias iayer-,- entre serverc. llamado Descubrmento y mapeo de reactones de Soportar una muestra wsuat Junto con la posmovaae ue mediante un ststema taeu:ar La vanedad det grosor ee zas derera representar el volumen de bv:es er las conversaciones Soportar una caça superpuesta de tegtc r:.ae porwprotocos bandwtdth response time trns) E' en 'e;ac.ones cttent server y server server nabal'tar el discovery y eeucac:cn de todas las partes involucradas en ea movimven:c ee algunos componentes
- Hacer descubr•rnento y análts.s ee dependen: ras de catos ctsoombtes para ropu'ar una OB de geston de CMOB Soportar tanto una ba:aea too dé aros configuraciones os datos como tamben una API para vermcacton de dependencias er temor. rea:
- Conectar con servidores Mtcroscft Active Drectory y usuar.os asocaaos a las d'recctones vos recolectaaas cara ser usadoproposvtos de reponeo
- Soportar profundidad ízoom.ng m•nena do.•vn' en e; camtno ee los paquetes d:spontOles tamben atravese un sensor debe soportar mediante 00100 deech• un n:vei mas orofundo• down• respec:o de ta informac.on comprimida en os de los paquetes
- Provee' de manera detallada informac•on acerca de ambiewrtuafes de donde se pueda observar el traslape de tas redes vnua;es con ta rec fisca que estam host y tunees vidua;es ae d€sposrcvos estan generando
- Soportar conectMdad mediante gestton de scanners de vulnerabilidades
- Soportar automatvcamente escaneo de nuevo systema que aparezca una ta parte Ce la red de'ln,da e) usuarto Elemplo S/ un nuevo server aoarer.e en data escaneaflo automáticamente y notificar a' NOC

3.4 2.1 Reporteo de la Herramienta do Monitoreo

Con el objeto de contar con la información para controlar y monitorear los servicios proporcionados "EL PROVEEDOR" debe proporcionar los reportes correspondientes al desempeño de la Red, información que será entregada dentro de los primeros cinco días hábiles del mes siguiente, siendo requisito para el trámite de pago de la factura al mes de que se trate. Dependiendo de la importancia del reporte, de común acuerdo con la SHF se establecerán las fechas de los reportes identificados como críticos.

A continuación se describen los reportes básicos de la solución, planeación de la capacidad y administraron de los niveles de servicio los cuales la herramienta de monitoreo deberá tener la capacidad de generar, para lo cual "EL PROVEEDOR" debe considerar que la SHF estará en posibilidades de generarlos y obtenerlos cuando así lo requiera durante la vigencia de los servicios. Los reportes que será obligación de "EL PROVEEDROR" entregar como parte del servicio serán los solicitados en el inciso "4.4 Reportes de servicio".

riables de utilización de CPU, memoria, desempeño y errores por CPE

Reportes Básicos para servicio de acceso a trtemet

a) Reportes diarios, semanales, mensuales e históricos cor a' menc•s as siguientes vanares cvr.uu te acces
Internet

- Disponibilidad
- Utilización de ancho de banda de ent entraca y saoea
- Utilización por tipo de protocolos de e "e entrada desalida
- Bytes de entrada/salida
- Frames de entrada/salida
- Retardo/Latencia
- Tasa de transferencia (Troughput)
- Cantidad de errores

Reportes para la Administracion do 'os niveles oe servicio

a) Reportes de incumplimiento de acuerdos de niveles de servicio establecidos para cada uno de los nodos monitoreados.

b) Reportes de rendimiento por nodo, conforme a los niveles de servicio solicitados por la SHF.

c) Los reportes de niveles de servicio tendrán las siguientes características mínimas:

- ID de nodo.
- Nombre del ID.
- Nombre del mes que se evalúa.
- Valores esperados en el mes para cada Nivel de Servicio medido.
- Valores obtenidos en el mes para cada Nivel de Servicio medido.
- Diferencia entre el Valor esperado y el Valor obtenido.
- Monto en moneda nacional de la renta por nodo.
- Monto en moneda nacional de la penalización, en base al valor obtenido de la diferencia de valores esperados y obtenidos en base a las definiciones realizadas por la SHF en el punto de Niveles de Servicio.
- Total del monto a penalizar en el mes por Nodo.

3 4.3 Centro dc Opcrac•oncs de Seguridad (SOCI

"EL PROVEEDOR" continuara ofreciendo a SHF el servicio de un "Centro de Operaciones de la Seguridad" (SOC) que conforme a estándares y mejores prácticas (ISO27001 a nivel de prácticas de seguridad o similares) proporcionará la implantación, administración, operación, monitoreo y correlación de eventos de la seguridad, con altos niveles de servicio. "EL PROVEEDOR" incluye en la presente propuesta los certificados vigentes en ISO27001, en el Apartado SOC y NOC se incluye el certificado correspondiente. El "Centro de Operaciones de la Seguridad" (SOC) por ningún motivo será administrado y operado por un tercero diferente de "EL PROVEEDOR". "EL PROVEEDOR" aplicarán la proactividad (prevención) necesaria para evitar ataques e incidentes de seguridad y en su caso detectarlos y contenerlos de la red de SHF. A fin de garantizar los niveles de servicio requeridos, "EL PROVEEDOR" cumplirán como mínimo las siguientes especificaciones:

SOLO er que sean proc.edaade EL PROVEEDOR tor e'

roce' i

Be mrsmos

E' SOC ze EL PROVEEDOR' proocn:tonara a SHF 'a atercion sus :uam,•.:.

Oe y ae trcroen:es as: como au en un borano de anc

Para nt,ovas vorvcncs de s.stema coerat.vo oaa:hos o de

'ecomendada e' fatyr.ar:e rara 'a co'tecta ocoracitn 'a carto de L EL PROVEEOOR• no e.ce•Serâ horas e:

sotre o convenenc.ta de aolcarla y seta programaca en 'a

Se! eauco SI 'a es urgente se haré av»' orac-•n SHE para nesgas a operacron En amt»os casos evaluado e: vs':) t:c.enc SHÇ

C.:rrecc.tvn ge s:ffware de seguagaa ya sea en r.ast' de

Ea CenVo Ocerac•cnes de Segur'dc" ce accese se segu'±a.: e aestruct•ura

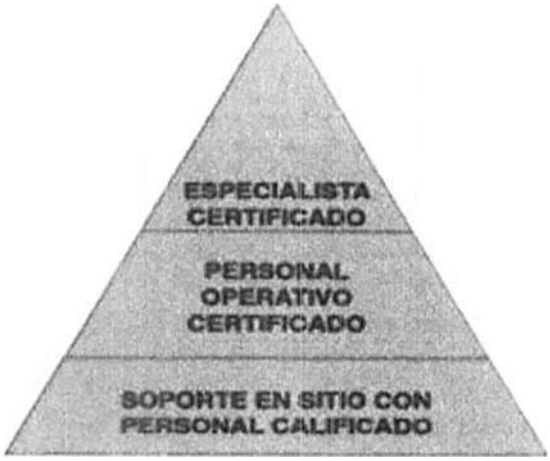
EL PROVEE DCJR COnta'ôn Con atenctr•, a Saoervvsara y y por menos ta mocet numero de sene tanto en V narc:ware de Cesernçe"o Oe ee segu'W.'a:.: cesoe a repones de cara

PROVEEOOR tievaran un tñmrr0S aue se a •a los 'esponsar:es de caca de tomo 3e ccmt'0i de se a' MRAGTIC-S' o en so aso el Que ic PROVFFDOR los •..pos de cambios

Tipo de Cambio	Definición	Tiempo de Solución
Urgente	Son todos los cambios a un componente de infraestructura de seguridad que se realiza para reparar lo antes posible una falla en algún servicio o que por su naturaleza pueden derivarse de un incidente o de un problema que afecte los niveles de servicio comprometidos y cuya única solución es a través de la aplicación de un cambio.	SLA del nodo
Alto	Son todos los cambios a un componente de infraestructura de seguridad, los cuales implican una interrupción sustantiva en el servicio.	Con autorización de la ventana por SHF
Estándar	Son todos los cambios a un componente de infraestructura de seguridad, que no representan ningún riesgo de afectación.	4 horas después de la solicitud de SHF

Modelode Operación SOC Y NOC

Cambio



a) "EL PROVEEDOR" compruebe que cuentan con experiencia en el ramo, tanto en el manejo de la infraestructura de seguridad como en el manejo de las prácticas y procesos basados en estándares internacionales. Su personal técnico cuenta con las certificaciones vigentes expedidas por algunas de las siguientes instituciones: ISC2, ISACA, SECURITY+, EC-COUNCIL, GIAC o ITIL relacionadas al nicho tecnológico que vayan a administrar; con un máximo de concentración de dos certificaciones por persona, las cuales deberán avalarse a través de la presentación de copia y original (para cotejo):

- Al menos un (1) certificado CISM (Certified Information Security Manager)
- Al menos un (1) certificado CISSP (Certified Information Systems Security Professional)
- Al menos un (1) certificado de ITIL-Fundamentals versión 3.
- Al menos un (1) certificado GIAC Incident Handler o CEH (Certified Ethical Hacker) del EC COUNCIL
- Al menos un (1) certificado de GCFA-GIAC (Certified Forensic Analyst)

En el Apartado SOC y NOC se presentan los certificados del personal de "EL PROVEEDOR"

b) Los Recursos Humanos indicados anteriormente serán responsables de garantizar que los servicios que presten "EL PROVEEDOR" a SHF se mantengan estables, en caso de incidentes de gravedad, ellos serán quiénes coordinen las actividades para resolver el incidente de que se trate y quiénes confirmen la solución definitiva, también informarán sobre las causas origen de la falla y en su caso las acciones correctivas para evitar que vuelva a presentarse el incidente. "EL PROVEEDOR" tomaron en consideración que además de la documentación que se consignara en cada uno de los tickets, en el caso de incidentes considerados como de gravedad y/o a solicitud del personal responsable asignado por SHF, se requerirá un correo electrónico con la información del incidente, sus causas origen y las acciones correctivas para evitar que se vuelva a presentar el incidente, adjuntando un documento firmado por el personal certificado que sustente la revisión del incidente en comento.

c) "EL PROVEEDOR" asegure al menos 1 ingeniero certificado por el fabricante para cada una de las Tecnologías ofertadas para el NOC y SOC, los cuales darán soporte y mantenimiento preventivo a la solución de seguridad de SHF, así como al hardware asociado, los sistemas operativos y programas que coadyuven a la operación de las herramientas durante el periodo de vigencia del contrato, con la finalidad de:

- Asegurar el correcto funcionamiento de las soluciones del software de la seguridad perimetral y de infraestructura de Internet.
- Asegurar el correcto funcionamiento del sistema operativo correspondiente para las soluciones del software de seguridad perimetral y de infraestructura de Internet.
- Brindar asesoría a cada área solicitante para el monitoreo de cualquier módulo y del manejo de las soluciones de seguridad perimetral y de infraestructura de Internet.
- Informar al personal designado por SHF sobre la última actualización disponible para las soluciones de seguridad, con el fin de valorar la necesidad de aplicarlas para que en su caso "EL PROVEEDOR" lleven a cabo dichas actualizaciones.
- Analizar las políticas y reglas de la solución de seguridad de SHF, con el fin de llevar a cabo los ajustes y las correcciones en caso de ser necesario. Dichas correcciones serán realizadas por "EL PROVEEDOR" bajo la supervisión del área técnica de cada área solicitante.

En el Apartado SOC y NOC se presentan las certificaciones del personal considerado por "EL PROVEEDOR" para la prestación del servicio

d) Los recursos Humanos que "EL PROVEEDOR" presente en la propuesta técnica con las certificaciones solicitadas no tendrán cambio durante la vigencia del contrato en caso de realizarlo dará aviso con 15 días naturales de anticipación a SHF e indicando el recurso sustituto el nuevo recurso tendrá la certificación igual o superior al de la persona que deja de laborar para "EL PROVEEDOR" el personal presentado en la proposición técnica será el que brindará la operación a los servicios requeridos por SHF La falta de alguno de los recursos dará lugar a la aplicación de la deducción correspondiente
e) Los Recursos Humanos indicados anteriormente ejecutarán la operación de los servicios que "EL PROVEEDOR" preste a SHF
f) Como parte del servicio y dependiendo de las necesidades de SHF segun las tecnologías del "Anexo A-1 Matriz de Inmuebles y Configuración", se incluye en sitio al menos 1 Ingeniero independiente del personal que "EL PROVEEDOR" requiera para su operación en Seguridad o Redes y contará con experiencia comprobable en los servicios de seguridad perimetral o redes que solicita SHF y en caso de requerirlo se proveerá el espacio donde operará el Ingeniero solicitado

En el monitoreo de los equipos de seguridad propuesto por "El PROVEEDOR" debe cumplir con:

a) Centro de monitoreo con las siguientes características, como mínimo
   - Acceso mediante controles de acceso biométricos o automatizados
   - Consolas de Monitoreo para visualizar los eventos
   - Laboratorio de pruebas y homologaciones
b) Realizar la detección proactiva de fallas mediante la generación de alarmas
c) Notificar automáticamente las alarmas de cada dispositivo de seguridad para la escalación de la falla hacia el sistema de la Mesa de Ayuda
d) Notificar automáticamente vía correo electrónico y/o vía telefónica a los responsables asignados por SHF al detectarse un incidente de seguridad
e) Herramienta de monitoreo con acceso vía HTTPS para al menos 3 usuarios simultáneos de SHF
f) Monitoreo del desempeño de los equipos de seguridad incluyendo utilización de CPU memoria errores
g) Capacidad de graficar por día semana de manera mensual y anual o incluso de manera personalizada a las necesidades de SHF El monitoreo de los elementos de la solución de seguridad será en Tiempo Real en forma 7x24x365
h) En el apartado SOC y NOC se especifica el centro de atención técnico para el seguimiento de reportes de incidentes, en sus cuatro niveles con un procedimiento de escalamiento que asignen "EL PROVEEDOR", indicando nombre, cargo, correo electrónico y teléfono celular
i) SHF tendrá derecho a solicitar en cualquier momento a "EL PROVEEDOR", el reporte de un incidente de seguridad, así como la información recopilada en periodos específicos incluyendo el diagnóstico lo anterior se entregará en un máximo de 24 horas a partir de que SHF lo solicite por medio electrónico Los alcances de este reporte de incidentes de seguridad serán definidos con "EL PROVEEDOR" como parte de las reglas de operación

3 4 Herramientaş de Monitoru

a) "EL PROVEEDOR" incluirá todas las licencias, mantenimientos y actualizaciones necesarias tanto en software y hardware, para mantener su operación continua, con una disponibilidad del 99 9 % mensual de las mismas en el Centro de Operaciones de Seguridad
b) Monitoreo en línea de las alarmas de seguridad generadas en los equipos de seguridad
c) Levantamiento automático de un reporte en la herramienta del Centro de Operaciones de Seguridad al detectarse un incidente de seguridad por medio del sistema de monitoreo Después de esto se notificará inmediatamente al personal asignado por SHF sobre el incidente, mediante llamada telefónica correo electrónico Para atención de reportes de seguridad "EL PROVEEDOR" proporcionarán un número único 01800 y una vez establecida la naturaleza se deberá canalizar con alguno de los ingenieros especialistas para su atención En el caso de que falle el 01800, "EL PROVEEDOR" proporcionarán un número local alternativo
d) Una vez que es detectado algún incidente de seguridad se llama proactivamente a SHF para iniciar el proceso de soporte, el personal del Centro de Operaciones de Seguridad contará con una hora a partir de que se levantó el reporte, para que en forma remota contenga la incidencia a nivel perimetral mediante los cambios pertinentes en la configuración de los equipos de seguridad proporcionados, en tanto se determina la corrección que el propio fabricante publique (concepto: día cero)

El PROVEEDOR de rotea'» Medio:
es at ce

u Estandar:

r Critico:

c cv=aa tc,T.a:

cn:c c,ara

a

en se '.nea

Ceva a

PROVEET)OR

cc:

...n;' la se

se ae r.:ataiorrra ios sou»entes

de SHF "feztaccr. to•.a. a: servic.r• ve.'d'da

E SHF

d e S H f a u n i n : . z e r t e s e

una a e ias

Cs atsvastt:vos asl

en server.'0 a 'a

trae corsecaenoas de ovactc a e

E' se oa 'alias

ana a oe vara en 'a ae

los e; far•ocante

Son v m, tr.murvcarse

con c%ente ante

EL PROVEEOOR se

CC.mo con atencuon Int"ed'ata

'Nso post%vc mecarus.•mos ya

a SHFj

Es t.emp: 'E'

como

se SHF a

•

caso no:as Es e' e:

corro

E

v u t r e ' a

(en caso de

Y.dc PROVEEL)C'R se a

es:e se se en Can SHF €_' d€•ra7S prevent•va Ce

a a ai

SHE

«a Tesauesta a

PFC)VECOOR a

EL PROVEEOOR

a Fas

EL F'ROVEEDOR t'-•vortes sus a ger,ë'ar de

ce la

Son a SHF SHF para

3 4 4, Mesa do Ayuda

'EL PROVEEDOR" debe contar con un centro de atención con la capacidad suficiente para tender las consultas, solicitudes y problemas relacionados a los servicios solicitados conforme a los tiempos establecidos en el apartado Niveles de Servicio

Los sistemas de Monitoreo, el NOC, el SOC y la Mesa de Ayuda deberán entrar en operación a partir de la puesta en servicio del primer nodo o servicio que proporcione el Proveedor a SHF

La Mesa de Ayuda debera operar 7X24 durante la vigencia del contrato para brindar la atención a la SHF

Las tareas minimas que el Proveedor realizará con la Mesa de Ayuda son: recibir, registrar, analizar y canalizar los reportes de incidentes o fallas a las áreas de atención correspondientes, dar seguimiento y solucion a las solicitudes informando a la SHF oportunamente

La Mesa de Ayuda recibirá en forma centralizada las llamadas a través de un numero telefónico unico con servicio 01-800, sin costo adicional para SHF

'EL PROVEEDOR" conjuntamente con la SHF, definirán, actualizarán y difundirán el catálogo de servicios que proporcionará a Mesa de Ayuda

La Mesa de Ayuda contará con un sistema de consulta en linea, donde podrá darse el seguimiento a los reportes levantados de manera proactiva via telefónica o correo electrónico

'EL PROVEEDOR" debera proporcionar, previo a la puesta en operación de los servicios, una matriz de escalamiento la cual contendrá al menos la información de los contactos (Nombre, Puesto, Teléfono Oficina, Telefono Móvil, etc.) para su localización en todo momento, así como los tiempos establecidos para pasar al siguiente nivel. Por su parte, la SHF proporcionará una matriz de escalamiento de contactos y responsables de la solución a fin de coordinar la restauracion de los servicios

3 4 5_ Administración de Altas Bajas y Cambios cn los Nodos

3er•erâ 'as aras Ce des

El. PROVEEOC)R oe mtyac.ene•s en r. software ha:er

reponaõos Gue sea por ia SEE menos ze

a e: el coa, se

acuerdo con e. Proveedor 'Se a las c.c"ltcas 1.3

Cuesta en oer

e: ia SHF a a de de ei se ea y PROVEEDOR

ea e' Se ara taa O tos se: Centro ae 'a Rec tNOC/c}e

PROVEEDOR a Se; area y

'EL PROVEEC>OR 'o Vdent'ficarâ V a

EL anal:sls y la fe

en arnoos casos dara aviso a la SHF con ea 'oma de

PROVEE 008' actvv:aces a y eiat.ora:a e;

EL PROVEEDOR' 'a SHE el cvoyama de tratwa;o para sa nay rea'.•arar en

con ee proseed0' servcctos acoe•'ao a' do EU PROVEEOOR' las

configuraciones

EL PROVEEDOR csfoceder:, a el aita c ae los servc.os

awso v ia SHF ren ta suoerws•on ce esta

Pruebas y ceo ateas SHE

PROVEEOOR

Ce alta e; nuevo serwc.'0 en s:srema oe V

pRC'VE E serviC•oS Peson,y de SHE

PROVEEDOR resguardos de

rases Oe Datos y

- 'EL PROVEEDOR' mantendrá respaldos actualizados de las configuraciones de todos los elementos del nodo (para todos los nodos de la SHF).

La SHF y 'EL PROVEEDOR' acordarán el procedimiento de control de cambios y los formatos correspondientes para la operación y seguimiento de los casos que se rijan por este proceso, mismo que será acordado y entregado previo a la puesta en operación del servicio.

Cuando los cambios afecten a más de uno nodo de la SHF, el procedimiento a seguir será definido con al menos 5 días hábiles de anticipación a la fecha estimada de ejecución.

'EL PROVEEDOR' generará y mantendrá actualizada una memoria técnica de los servicios integrando los correspondientes controles de cambios.

'EL PROVEEDOR' tomará las medidas correspondientes, para que sólo personal autorizado acceda a los equipos de comunicaciones, para efectuar cualquier cambio y/o monitoreo.

Para el acceso físico a los elementos, el Proveedor solicitará con 48 horas de anticipación las autorizaciones correspondientes.

Para casos no previstos en este documento o emergencias, se podrá autorizar vía correo electrónico y llamada telefónica, por el personal designado por la SHF. Una vez concluida la emergencia, se llevará a cabo el levantamiento y registro del control de cambio correspondiente.

Cuando así le convenga, la SHF podrá solicitar baja definitiva de uno o la totalidad de los elementos de un nodo (cualquiera que sea éste) sin penalización alguno para la SHF. Para el caso de los elementos en donde el presente documento indique un tiempo mínimo de contratación, la SHF no podrá dar de baja anticipada del elemento en cuestión, siempre que no se haya cumplido el tiempo mínimo de contratación, pudiendo únicamente solicitar la reubicación del elemento en cuestión en otro de sus nodos.

3.4.60 Adic•onos do nodos, reubicaciones y cambios on ancho de banda

'EL PROVEEDOR' se basará en la *Tabla 2* 'Anchos de Banda soportado por Tipo de Medio' donde se indica para cada tipo de medio de transmisión los anchos de banda soportados sin cambio físico del mismo, asimismo 'EL PROVEEDOR' deberá indicar en su proposición el tipo de medio de transmisión a instalar en cada nodo para la SHF. **El**

Tabla 2 'Anchos de Banda soportado por Tipo de Medio'

Tipo de Medio	Ancho de Banda Soportado
Cobre 128	128 Kbps
Cobre 1024	1024 Kbps
Cobre 2048	2048 Kbps
Fibra Óptica E3	32768 Kbps
Fibra Óptica	500000 Kbps
Microonda E3	32768 Kbps
Microonda	155000 Kbps

Con base a la *Tabla 2* 'Anchos de Banda soportado por Tipo de Medio' y la información del medio instalado en cada nodo, la SHF podrá solicitar incrementos de ancho de banda, en donde el medio lo permita, 'EL PROVEEDOR' deberá ofrecer un tiempo de respuesta máximo de 72 horas a partir de la petición formal del incremento de ancho de banda del nodo. Caso contrario, se tomará el nivel de servicio como si fuese una reubicación de nodo.

En caso de reubicaciones dentro del mismo domicilio, estas serán sin costo adicional para la SHF. 'EL PROVEEDOR' realizará el plan de trabajo en coordinación con la SHF, mismo que será evaluado y autorizado previo a la realización del traslado.

Cuando se requieran ampliaciones o incrementos en los servicios solicitados de la presente proposición, serán coordinados y autorizados por la SHF de acuerdo a la disponibilidad del presupuesto.

Para el caso de baja de servicios, la SHF podrá por motivos funcionales o de operación, dar de baja nodos de la Red o servicios sin penalización alguna, para lo cual notificarán por escrito, la fecha de cancelación de los mismos a "EL PROVEEDOR" con un mínimo de 30 días naturales de anticipación; dicha fecha no necesariamente corresponderá a las fechas de corte para la facturación, por lo cual no se reflejará el cobro proporcional del periodo posterior a la baja del servicio.

En caso de que la SHF agregue nodos o servicios "EL PROVEEDOR" deberá:

- Mantener el esquema de costos ofertado.
- Integrará los nuevos servicios de acuerdo a las características técnicas establecidas en el contrato con el proveedor ganador.
- La adición de nodos a la red estará sujeta a la disponibilidad del presupuesto.

Se considerará como adición (nuevo nodo) a los nuevos nodos o localidades que se integren a la red, así como nodos existentes que requieran cambios en su configuración original, debido a una modificación en características (ancho de banda o componentes funcionales adicionales al CPE), que representen cambios en infraestructura de acceso o modificación de CPE.

3.4 7 Entrega y soporte det servicio.

"EL PROVEEDOR", alineará todos sus procesos relacionados con la administración del servicio provisto a la SHF a la biblioteca de Mejores Prácticas de ITIL v3 (IT Infrastructure Library), lo anterior considera a la Mesa de Ayuda y a todos los procesos de entrega y soporte del servicio, a saber:

- Administración de configuraciones
- Administración de cambios
- Administración de incidencias
- Administración de problemas
- Administración de liberaciones
- Administración de la capacidad
- Administración de los niveles de servicio
- Administración de la disponibilidad

3 4 8 Asistencia Técnica en Sitio y Remota

"EL PROVEEDOR" considerará en su proposición los recursos técnicos y humanos necesarios con experiencia de al menos 3 años en administracion de redes, el personal presentado en la proposición técnica será el que brindará la operación a los servicios requeridos por SHF para la prestación de asistencia en sitio de acuerdo a los niveles de servicio solicitados durante la vigencia del contrato.

SHF definirá y seleccionará las características del personal en sitio, como: horario, días de la semana, perfil entre otros. "EL PROVEEDOR" deberá:

a) Integrar como parte de su solución las herramientas de monitoreo, infraestructura de hardware, software y seguridad que considere convenientes, así como el personal necesario para atención de fallas y soporte en sitio; dicha infraestructura y servicio se deberá mantener en el nodo central de SHF y será utilizada para atender la operación crítica, en horario de 7:00 a 20:00 hrs., de lunes a viernes.
b) El personal asignado por "EL PROVEEDOR" para la administración, monitoreo y soporte en sitio de la seguridad e Internet atenderá sus actividades en las instalaciones de SHF de lunes a viernes en un horario de 7:00 a 20 horas. Para los horarios restantes (lunes a viernes de 20:01 a 6:59 horas, sábados y domingos), se deberá atender desde su(s) centro(s) de servicio(s) regionales).
c) "EL PROVEEDOR" supervisará y en su caso corregirán en forma proactiva, el estado lógico y físico de los equipos y enlaces de comunicaciones ofertados, utilizando para ello la infraestructura instalada en el punto "Servicio de Operación".
d) "EL PROVEEDOR" será responsable en todo momento de mantener la comunicación entre las distintas instancias de asistencia y contará con la información pertinente para el escalamiento de fallas.

e) 'EL PROVEEDOR', a través de personal en sitio, garantizará a SHF la ejecución de los siguientes procesos

- Administración y monitoreo continuo de la operación de la red para la prevención de fallas
- Detección oportuna de fallas inclusive, previo a que sean reportadas por SHF
- Recuperación del servicio conforme a la disponibilidad y niveles de servicio solicitados
- Diagnóstico y corrección de raíz en las fallas presentadas
- Control y gestión oportuna de los reportes de falla que le asigne el área técnica o la Mesa de Ayuda de SHF hasta su cierre y Vo Bo de las áreas internas designadas por la misma
- Notificación en tiempo real a través de una llamada telefónica a la Mesa de Ayuda de SHF en el cual se indiquen los problemas y las interrupciones así mismo se notificarán los restablecimientos correspondientes a cada uno de los enlaces, equipos, interfaces o cualquier componente de la red, Internet y solución de seguridad que impacte el nivel de servicio solicitado. Se proporcionarán reportes para el cierre de fallas reportadas, documentando causa, diagnóstico y solución

f) Emisión de la información para la planeación de capacidad de la infraestructura de conectividad y servicios en la red, en base al monitoreo continuo y reportes estadísticos obtenidos

g) Emisión de la información para la planeación de capacidad de la infraestructura, anchos de banda de los canales y servicios en la red, en base al monitoreo continuo y reportes estadísticos obtenidos

h) 'EL PROVEEDOR' contarán cuando menos con un centro nacional de soporte y atención a fallas las 24 horas, los 365 días del año, el cual trabajará en forma complementaria con el esquema de monitoreo y administración descrito en esta sección

i) SHF proporcionará facilidades de espacio, iluminación, conexión a los servicios de voz y datos para la instalación de la infraestructura de administración, monitoreo y recuperación del servicio para el personal técnico que opere dicha infraestructura. Los alcances de estas facilidades por persona a brindar asistencia técnica son enunciativas más no limitativas y se listan a continuación

- Espacio físico
- 1 línea telefónica digital con aparato para realizar sólo llamadas locales
- 1 puerto Ethernet para conexión a la red de SHF
- 2 contactos eléctricos soportados a energía no regulada

j) La asistencia técnica y soporte remoto deberá cubrir los requerimientos especificados en la sección del NOC

4. Niveles de Servicio

Los niveles de servicio estarán relacionados en términos de disponibilidad, desempeño del servicio, entrega de los servicios, tiempo de solución a fallas (TTR por sus siglas en inglés), reportes y penalizaciones. En todos los cálculos para la determinación de niveles de servicio serán valores truncados a dos decimales.

4 Disponibilidad

La Disponibilidad se define como la medida del porcentaje de tiempo, en que un sistema (o un componente del sistema) realiza la función que le es propia. Es decir, disponibilidad es la proporción de tiempo en que el sistema cumple con la función para la cual está dispuesto, en relación con el tiempo en que debería haber estado disponible.

4 Calcuto de la disponibilidad por Nodo

La disponibilidad por Nodo se calcula en base a las siguientes formulas

Fórmula 1. Cálculo de Disponibilidad por nodo

$$\%Dispnodo = Tdispl \times 100 / Totalmes$$

Donde

Variable	Descripción
%Dispnodo	Disponibilidad medida en porcentaje de cumplimiento del nivel de servicio por nodo
Tdispl	Tiempo en minutos de disponibilidad del nodo.
Totalmes	Número de minutos totales que debió estar disponible el nodo durante el mes.

Para determinar la disponibilidad mensual del nodo, se realizará un comparativo de la disponibilidad mensual de cada uno de los elementos del nodo que se trate, y la disponibilidad mensual que resulte la más baja de entre éstas, será igual a la disponibilidad mensual del nodo.

nula 2. Cálculo de los minutos de servicio mensual

$60 \times 24 \times Días\ del$

43 2 Disponibilidad det servicio

Er a siguiente •.at:a se cresen:an las tisponibilidades de servicioocr ae nodo, solicitada por.a SHF

NIVELES OE SERVICIO		
	NODO CRITICIDAD ALTA	NODO CRITICIDAD ESTANDAR
Disponibilidad Del Servicio 7x24x365	>= 99.98%	< 99.80%

'EL PROVEEDOR' deberá proporcionar en el diseño de su solución, todos los elementos del nodo que requieran redundancia y/o esquemas de alta disponibilidad, para poder cumplir con los niveles de servicio especificados en el Anexo 1-A "Inmuebles y Requerimientos de Servicio e Infraestructura para SHF" de acuerdo al tipo de nodo, ubicación geográfica, condiciones físicas, y demás consideraciones que estime pertinentes.

'EL PROVEEDOR' debera entregar en su proposición, el diseño de la solución ofertada para cada nodo, indicando en éste las redundancias y/o esquemas de alta disponibilidad considerados.

Si durante la vigencia del servicio el Proveedor debe realizar cambios en la solución para poder dar cumplimiento a la disponibilidad solicitada por la SHF, estos cambios deberán ser programados y observar los acuerdos establecidos en el proceso de control de cambios, asimismo estos cambios no causarán costos adicionales para la SHF, siempre y cuando dichos cambios no sean debido a una solicitud expresa de la SHF para cambiar el nivel de servicio del nodo que se trate, en cuyo caso solo se incrementará el costo mensual en base a la suma de los costos ofertados por 'EL PROVEEDOR' para cada elemento del nodo en el nivel de disponibilidad solicitado.

4 3 Modic•on de la disponibilidad dol servicio

La medición de la disponibilidad de los servicios se realizará en forma diaria recolectando la información generada a través de la herramienta de monitoreo, acumulando esta información hasta el cierre del mes, en donde se realizarán los cálculos finales del comportamiento de la disponibilidad de los servicios durante ese periodo.

La información recolectada en forma diaria no será compactada ni se realizarán promedios de los promedios al final del mes, la base de cálculo será la información que se obtenga en forma diaria.

La herramienta de monitoreo propuesta por 'EL PROVEEDOR' deberá proporcionar información al menos cada minuto, la cual se almacenara en una base de datos de la misma herramienta y estará disponible en cualquier momento (dentro del plazo de 3 meses) para la SHF por medio de las consolas de Monitoreo.

El calculo propuesto para la disponibilidad de cada elemento del nodo consiste en tomar una muestra a cada elemento del nodo cada minuto para hacer un total de 1440 muestras por día por elemento, para conocer la disponibilidad mensual de cada elemento del nodo, se realizará la suma de muestras disponibles entre el total de muestras disponibles posibles para cada periodo mensual para cada elemento. Para la definición del tamaño del paquete que será utilizado para la medición de las muestras, 'EL PROVEEDOR' propondrá el valor más adecuado de acuerdo a su solución para la medición de los niveles de servicio, en donde aplique.

Para determinar la disponibilidad mensual del nodo, se realizará un comparativo de la disponibilidad mensual de cada uno de los elementos del nodo que se trate, y la disponibilidad mensual que resulte la más baja de entre éstas, será igual a la disponibilidad mensual del nodo.

En la mesa de trabajo se acordarán los eventos que acumulan indisponibilidad del servicio y aquellos eventos no imputables a "EL PROVEEDOR" que no serán considerados como indisponibilidad del servicio. lo anterior será implementado a través de la mesa de ayuda y su proceso de administración de incidencias.

En casos en los que sea necesario acceder al sitio y no haya personal de la SHF que pueda proporcionar el acceso se detendrá el conteo del tiempo de indisponibilidad justo cuando personal de "EL PROVEEDOR" informe esta eventualidad a la SHF y ésta última corrobore la situación. En este caso, el tiempo volverá a contarse a partir de la hora en que esté disponible el acceso al sitio, especificado por la SHF. Los procedimientos de acceso y los acuerdos operativos para el reinicio del conteo de la indisponibilidad serán acordados con "EL PROVEEDOR". Esto será aplicable en general, para todos los niveles de servicio siempre y cuando el diagnóstico del problema, acordado con la SHF, identifique que la solución del mismo depende del acceso al sitio en cuestión.

4_1.4 Tiempo de reparación de fallas.

Cuando "EL PROVEEDOR" haya ofertado esquemas de redundancia y/o alta disponibilidad en el nodo y se presente cualquier tipo de falla ya sea lógica o física que no afecte la disponibilidad del mismo, asegurará, a través de los diferentes mecanismos previstos dentro de su estrategia, un adecuado proceso de administración de incidentes, que dé como resultado el cumplimiento del tiempo de reparación de fallas (TTR por sus siglas en inglés) para la atención y solución de incidentes, sobre los distintos componentes del servicio y sobre los elementos que forman parte solución. El tiempo de reparación de la falla es de 24 horas a partir del inicio del incidente, tanto para nodos de criticidad alta y estándar.

Las penas convencionales que se llegaren a aplicar por este concepto son independientes de las deductivas que pudieren aplicarse por indisponibilidad del nodo.

.t 1 Latencia

En términos generales, el término latencia se aplica en una red de datos a la cantidad de tiempo que le toma a un paquete viajar desde un punto origen a un punto destino.

Por razones prácticas, la medición de la latencia se realiza considerando una trayectoria de ida y vuelta entre el punto origen y destino (round trip). Para la definición del tamaño del paquete que será utilizado para la medición de las muestras, "EL PROVEEDOR" propondrá el valor más adecuado de acuerdo a su solución para la medición de los niveles de servicio en donde aplique.

La latencia máxima requerida será medida de cualquier CPE a cualquier otro CPE que forme parte de la red SHF. La latencia será medida del puerto Ethernet al puerto Ethernet de cada CPE, entendiendo como puerto Ethernet del CPE, el puerto LAN donde "EL PROVEEDOR" proporcionará la conectividad hacia el inmueble de la SHF.

Para el cálculo de la latencia se utilizará el mismo mecanismo de medición de muestras obtenidas para el cálculo de la disponibilidad (latencia entre el nodo de origen y nodo destino), en donde el Licitador ganador registrará estos tiempos de manera individual para cada una de las clases de servicio definidas.

El Proveedor suministrará un plan de trabajo para la implantación de mediciones de latencia por clase de servicio, mientras este plan no esté concluido la SHF definirá cuál de los 2 valores de latencia (Calidades de Servicio), será usado para efectos de medición por cada nodo. Al finalizar el mes, se promediará el tiempo medido en cada muestra.

La red de "EL PROVEEDOR" debe permitir que se realicen mediciones de latencia desde cualquier CPE hacia cualquier otro CPE por parte de la SHF o quien ésta designe para tal fin. Esta información, podrá ser utilizada para determinar si existen diferencias respecto a lo reportado por el NOC.

La latencia será medida en todos los CPE de la red, desde un nodo propuesto por "EL PROVEEDOR" y autorizado por la SHF e incluso pudiendo ser el nodo de monitoreo del Proveedor.

4, DegradaciOn por perdida de paquetes

Para la medición de la perdida de paquetes, se realizará la sumatoria mensual de paquetes perdidos, transmitidos y recibidos y será comparada contra la sumatoria de información transmitida y recibida. Se utilizará un mecanismo de medición similar de recolección de muestras al usado para la medición de la disponibilidad, en donde "EL PROVEEDOR" registrará estas muestras para cada uno de los nodos de la SHF.

El porcentaje de perdida sin interrupción total del servicio del enlace no deberá ser superior al 1% mensual.

No aplicará para el conteo de pérdida de paquetes, si existe en el mismo periodo de falla condiciones de indisponibilidad física o lógica, o degradación por latencia, en cuyo caso dichas condiciones serán deducidas de acuerdo a los niveles de servicio establecidos para esos efectos.

4.1.5.3. Nivel de servicio

En la siguiente tabla se presentan los niveles de servicio requeridos, para las diferentes clases de servicio:

Clase de Servicio	Nivel de servicio solicitado	
CoS	Tiempo máximo de ida y vuelta en milisegundos	Pérdida paquetes
Conversacionales (voz)	120	<1%
Interactivos (datos)	150	<1%

Para los nodos ubicados en el Área Metropolitana de la Ciudad de México y Metepec.

La garantía de pérdida de paquetes, menor al 1%, será válida siempre y cuando no se exceda el ancho de banda disponible por clase de servicio asignado por la SHF, y será responsabilidad de "EL PROVEEDOR" documentar y notificar a la SHF este tipo de eventos.

Perdida de Paquetes

Para la medición de la pérdida de paquetes, se realizará la sur la iual de paquetes perdidos tidos y recibidos y será comparada contra la sumatoria de información y recibida. Se utilizará un de medición similar al usado para el cálculo de la disponibilidad. suma•.ona

Fórmula 3. Cálculo del porcentaje por Pérdida de Paquetes al mensuat de varsm

"ansm•t'3a mer_ansm:,

$$\%Perdida\_Paq = 1 - (\sum PaqPerd\_Trans - \sum PaqPerd\_Recibi - (\sum Paq\_Trans - \sum Paq\_Recibi) * 100$$

No aplicará para el conteo de pérdida de paquetes, si existe en el mismo periodo de falla condiciones de indisponibilidad física o lógica, o degradación por latencia.

4 2D Disponibilidad det Servicio de Acceso a Internet

"EL PROVEEDOR" mantendrá una disponibilidad del Servicio de Acceso a Internet de acuerdo a lo solicitado en el Anexo I-A "*Inmuebles y Requerimientos de Servicio e Infraestructura para SHF*". En el caso de no poder cumplirlos el Proveedor realizará las adecuaciones necesarias en los equipos para cumplir con los niveles de servicio solicitados, estas adecuaciones se programarán para evitar una afectación al Negocio de la SHF.

La latencia no será mayor a 85 milisegundos de ida y vuelta al punto de acceso a la red pública más cercano en términos del número de saltos necesarios para alcanzarlo.

Disponibilidad de' servicio de Internet

det noac "e Interne: se a oe formula

Fórmula 4. Cálculo de Disponibilidad del Servicio de Internet

$$\%Disp\_Internet = (Disp2/\ Totalmes) * 100$$

Donde

Variable	Descripción
%Disp_Internet	Disponibilidad medida en porcentaje de cumplimiento del nivel de servicio
Tdisp2	Tiempo en minutos de disponibilidad del servicio de Internet
Totalmes	Numero de minutos totales que debió estar disponible el nodo durante el mes. *(Formula 2. Calculo de los minutos de servicio mensual)*

4 3. Entreça ac Scrvsoos

Los tiempos máximos de entrega de los servicios que cumplirá "EL PROVEEDOR" son los siguientes

Para cambios de domicilio de nodos existentes, la SHF y "EL PROVEEDOR" determinarán de común acuerdo las fechas de baja y activación del nuevo domicilio, las cuales no se excederán de 4 semanas contadas a partir de la notificación formal

Baja de nodos dentro de los 5 días siguientes a la solicitud formal. Transcurrido dicho plazo, la prestación del servicio posterior será bajo responsabilidad de "EL PROVEEDOR", sin costo para la SHF

Modificaciones a anchos de banda, siempre y cuando no impliquen un cambio físico en el o los enlaces de transmisión (incrementos por configuración): 3 días naturales. Si implican cambio físico aplican los tiempos de cambios de domicilio. Para ello "EL PROVEEDOR" deberá indicar en su proposición, una tabla en la que indique los anchos de banda compatibles y que cuya modificación no implica un cambio físico de la infraestructura

Reconfiguraciones lógicas en caso de contingencia en un tiempo de 4 horas

Estos tiempos comenzarán a contar a partir de que se emita la solicitud de servicios correspondientes por parte de la SHF.

Las notificaciones y/o respuestas serán válidas formalmente por oficio con excepción de las reconfiguraciones

4

4 Reportes de' servicio„

Aplica para todos los reportes y será condicionante para el pago de la facturade "EL PROVEEDOR"

Con el objeto de medir el desempeño de los servicios proporcionados por "EL PROVEEDOR", será necesario generar los reportes de comportamiento, desempeño y disponibilidad con la cual se proporcionen los servicios solicitados, de acuerdo con los niveles de servicio definidos

Los reportes serán entregados por "EL PROVEEDOR" a la SHF de la siguiente manera:

NUMERO OE REPORTE	NOMBRE DESCRIPCION	FRECUENC'A OEt REPORTE
	El. ROVFEDOR entregará reportes de administ de iguraciones y cambios en la infraestructura, as de contalización de una memoria técnica integral la actuis servicic de b•.	Cada tres meses durante los primeros 5 días hábiles del mes siguiente al periodo comprendido

	Utilización de ancho de banda por enlace, utilización ancho de banda por QoS (Calidad de servici Disponibilidad, Latencia y Pérdida de Paquetes por sitio y p elemento funcional que forme parte de la solución	Se entregarán dentro de los primeros 5 dias hábiles de cada mes
	Reporte de Atención y solución de fallas, indicando los tip de fallas, su tiempo de reparación (TTR), si afectan o no disponibilidad	Se entregarán dentro de los primeros 5 dias hábiles de cada mes
	ibilidad, Latencia y Degradación por Pérdida es del acceso a Internet, por sitio	Se entregarán dentro de los primeros 5 dias hábiles de cada mes
	stico, planeación de capacidades y proposicion s. Este reporte sera presentado para la SHF	Se entregará de manera semestral, durante los primeros 5 dias hábiles del mes siguiente al periodo comprendido
	e ejecutivo, contendrá estadísticas principales de u npeño, sumarizado para la SHF	Se entregará de manera semestral, durante los primeros 5 dias hábiles del mes siguiente al periodo comprendido
	informes Ejecutivos por ir te. Este informe ejecuti contendrá la descripción si de la falla, sus causas y acciones que se tomaron esolverlas, el formato y forma de entrega se defin s el Proveedor como pa de las reglas de operació emo.ugo, el formato sa la'. electrónico	El Proveedor entregará a solicitud de la SHF, un reporte ejecutivo de los incidentes que considere criticos durante los 3 dias siguientes al evento

Los reportes señalados son los unicos reportes que serán entregados por "EL PROVEEDOR" a la SHF.

La lista de reportes anterior sera extendida en contenido, tipo de reporte y frecuencia de entrega de común acuerdo entre la SHF y "EL PROVEEDOR"

El Proveedor entregara los Reportes acordados en medio electrónico en formato PDF, Excel, Word o ASCII, a solicitud de la SHF.

Niveles de Sorvicio Aptgcables a 105 Elementos de Seguridad

"EL PROVEEDOR" garantizará la segundad mediante el monitoreo en tiempo real al estado de la seguridad relativo a los servicios ofrecidos en su proposición, así como sistemas de detección de intrusiones que pudieran ocurrir, brindando visibilidad, tanto en el flujo de datos y la postura de seguridad. En la siguiente tabla, se presentan los niveles de servicio esperados para las tareas de administración y monitoreo de la infraestructura de seguridad.

SERvtctO	NIVEL COMPROMEt1DO
Atención a requerimientos de configuraciones de segundad	30 minutos después de acoraado e: camăn or'te el Licitante y SHF
Tiempo de solución de incidentes de seguridad	Por prioridad **Crítico** – Identificación y contención inmediata **Medio**- 60 minutos **Estándar**- 24 hrs Programado
Licenciamiento y entrega de actualizaciones	Licenciamiento y actualización del software "EL PROVEEDOR" durante todo el contrato. Entrega de la mec hábiles después de liberada la version "r:worcvonado ocr EC de la mec.a mâ.smč 3 a.as

Administración y control de accesos remotos y túneles VPN	Tiempo máximo de sotuc.ôt: 2 horas después r.:e [a de SHF
CC '_'amťos	Por tipo Urgente – Inmediato, una vez autorizado o solicitado por SHF Impacto Alto -24 hrs Programado Impacto Medio -48 hrs Programado Impacto Estándar -24 hrs una ve: autorizado o solicitado or.' SHF
Dictamen de actividades sospechosas	„•,ua'.cs LAN c Tiempo máximo entrega de dictamen: 4 horas
Notificación y atención de actividades sospechosas	Crítico De acuerdo a la disponibilidad del nodo y aplicaciones y/o servicio Medio 60 minutos Estándar 24 hrs Programado
Atención a incidentes de día cero	Tiempo máximo de una hora a partir de la detección para contener la incidencia a nivel perimetral mediante los cambios pertinentes en la configuración de los equipos de seguridad
Recursos Humanos Certificados para soportar los servicios	Disponibilidad de •.odi.3 versonal solicitado durante la vigencia del contr

Control de accesos a pâgłnas web o URĽS no autorizadas

En el caso de existir algún sitio web, al cual se tuvo acceso por primera vez por algún usuario de SHF que no se encuentre categorizado en la base de datos del Fabricante, "EL PROVEEDOR" considera por lo menos 24 horas naturales para reclasificar el sitio en la categoría correspondiente; así mismo SHF podrá solicitar la reclasificación de URL's las cuales serán ejecutadas en un máximo de 24 horas naturales

5. Documentación Técnica Adicional

El Proveedor deberá entregar la siguiente información técnica adicional

1 Procedim•entos del NOC V del SOC

- Procedimiento de escalamiento de niveles de atención (tiempo estimado entre cada escalamiento de nivel, así como los teléfonos de oficina, y celulares de los responsables de cada nivel)

- Procedimiento para la atención de fallas e incidentes

5 2. Documentación de la herramienta de monitoreo

- Documento referente al uso y consulta de la herramienta de monitoreo

6. Temas Administrativos y legales.

5. "EL PROVEEDOR" deberá de coordinar la transferencia de servicios con el futuro proveedor de servicios en el caso de un cambio, elaborando conjuntamente la logística de transición, misma que será avalada y autorizada por la SHF

Eñ ñ, Ñan'e,nas las necesidades rancu!ares en Temas Administrativos y [epates ue le apliquen a la SHF

6.1 Condiciones tecmcas para ta transicion a un nuevo proveedor posterior al termino del contrato

obligación de "EL PROVEEDOR" que preste
ea ..:e'ma realizar bajo las siguientes condiciones el servoo durante el período de transición a un nuevo proveedor
se

a) "EL PROVEEDOR deber* garantizar los niveles de servicios durante la transición hacia un nuevo "proyecto".

EL PROVEEOOR a' ermino deeste rroyecto garantizará 'os niveles de durante ei getra

de servicios al nuevo proveedor

Dicho periodo de transición para la
caso se celebren. De ser necesario el

Durante dicho periodo "EL PROVE
SHF para garantizar la continuidad

a incluido en la vigencia del contrato o de los convenios que en su
servicios será pagado mediante una ampliación al contrato

te estos

proporcionar la orientación tecnológica adecuada al personal de la
contratados

la m•grat'O" estar* incru'dc en ia

EL PROVE-€:OOR debera de
05 seno:.os

PROVEEDOR' Oe mantener Jos n.veles de 'a
ot..,eti.cs Clanes en corto

s de servicio de la SHF, integrará un grupo de trabajo para que
plazo

fens

c) En su caso. PROVEEDOR ᵘ integrara la infraestructura necesaria para conectarse al nuevo proveedor

El proveedor durante el periodo de transición mantendrá la infraestructura que proporcione el servicio de Internet y LAN to LAN con objeto de que el nuevo proveedor integre su infraestructura total de solución y no afecte los procesos de operación de la SHF.

Adicionalmente, es importante mencionar que "EL PROVEEDOR", dará todas las facilidades que la SHF considere pertinentes, para garantizar la transparencia en el proceso de transición al nuevo proveedor de servicios.

Durante la etapa de migración de los servicios, "EL PROVEEDOR" retirará todos los equipos que hubieran sido parte de la solución y que sean única y exclusivamente de su propiedad en un plazo no mayor a 30 días naturales posteriores a la migración de nodo que se trate, dichos retiros formarán parte del acta de liberación del servicio y será requisito para la liberación de la Garantía de Cumplimiento del Contrato.

c) En su caso. -Ee PROVEEDOR" se coordinará con et nuevo proveedor para realizar la migración progresiva del proyecto.

En su caso, "EL PROVEEDOR" durante el periodo de transición hacia el nuevo proveedor de servicios que hubiere resultado ganador en la SHF, integrará un grupo de trabajo para la coordinación en la etapa de migración progresiva del proyecto, estableciendo un plan de trabajo donde se reflejen los límites y participación de (EL PROVEEDOR - LA SHF - PROVEEDOR NUEVO) los servicios licitados con objeto de no afectar la operación de la Red de la SHF.

Es importante señalar que "EL PROVEEDOR", en conjunto con la SHF, apoyará a la integración continua y transparente de los servicios bajo las prioridades y normas que la SHF determine.

6 ú Actualizacion Tocnotomca

Durante la vigencia del contrato, en caso de obsolescencia que impida brindar los servicios con los niveles de servicio solicitados por la SHF, los equipos o soluciones utilizados por el Proveedor, y en general todo el equipamiento y software que incluya "EL PROVEEDOR" en su proposición, deberá ser sustituido por uno de nueva tecnología, sin costo adicional para la SHF.

"EL PROVEEDOR" deberá garantizar el acceso a información técnica relacionada con las tecnologías, que forman parte de su solución y que está a disposición por parte de los fabricantes de equipo que sean integrados dentro de su solución. Este acceso se refiere a cuentas de acceso a los sitios de soporte en Internet de cada fabricante, al menos 2 para la SHF para todos los fabricantes que cuente con el servicio y que así le sea solicitado, acceso a boletines de información, publicaciones periódicas y/o seminarios que estén integrados como parte de la oferta comercial de los fabricantes a sus clientes, siendo la SHF un cliente indirecto por la contratación de los servicios del Proveedor de la solución. Algunos ejemplos de situaciones que serán consideradas como obsolescencia son, de manera enunciativa más no limitativa, que el Sistema Operativo no sea capaz de soportar nueva funcionalidad, o actualización de seguridad, cuando el fabricante retira el soporte de la familia o modelo del equipo, etc.

a

7 L Penas convencionales y deductivas,

Se aplicará una pena convencional a "EL PROVEEDOR", por el atraso en la prestación del servicio de acuerdo siguiente tabla:

CONCEPTO	PLAZOS ESTABLECIDOS	REQUERIMIENTO	PENALIZACIÓN
Incrementos o decrementos de ancho de banda	30 días a partir de la solicitud formal	Incrementos o decrementos de ancho de banda en nodos con cambio en medio de transmisión de acuerdo con la Tabla 2 "Anchos de banda soportados por tipo de medio"	2 al millar por cada día de atraso del monto total de la facturación mensual de los servicios correspondientes al nodo(s) afectado(s)
Entrega de servicios Cambios de domicilio	4 semanas a partir de la solicitud formal	Cambio de domicilio de un nodo ya instalada	2 al millar por cada día de atraso del monto total de la facturación mensual de los servicios correspondientes al nodo(s) afectado(s)
Entrega de Reportes	Cada tres meses durante los primeros 5 días hábiles del mes siguiente al periodo comprendido	De administración de configuraciones y cambios en la infraestructura, así como la actualización de una memoria técnica integral de servicios	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios
Entrega de Reportes	Se entregarán dentro de los primeros 5 días hábiles de cada mes	Utilización de ancho de banda por enlace. Utilización de ancho de banda por QoS (Calidad de Servicio). Disponibilidad, latencia y pérdida de paquetes por sitio y por elemento funcional que forme parte de la solución	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios
Entrega de Reportes	Se entregarán dentro de los primeros 5 días hábiles de cada mes	Reporte de atención y solución de fallas, indicando los tipos de fallas, su tiempo de reparación (TTR), si afectan o no la disponibilidad	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios
Entrega de Reportes	Se entregaran dentro de los primeros 5 días hábiles de cada mes	Disponibilidad, latencia y degradación por pérdida de paquetes del acceso a Internet, por sitio Estadísticas por tráfico anómalo en Internet	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios
Entrega de Reportes	Se entregará de manera semestral, durante los primeros 5 días hábiles del siguiente al periodo comprendido	Diagnóstico, planeación de capacidades y propuesta de mejoras	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios

i,

(a

Se aplicara una deductiva a "EL PROVEEDOR" en caso de que se presenten fallas en la prestación del servicio derivadas del incumplimiento parcial o prestación deficiente de los servicios, en los términos que a continuación se indican:

DISPONIBILIDAD NODOS DE CRITICIDAD ALTA	DEDUCCIÓN
Cuando no se cumplan con los objetivos de las disponibilidades del servicio por nodo, para los diferentes niveles de disponibilidad, conforme al esquema de medición propuesto. Incluye todos los elementos que conforman cada nodo	5 al millar, por cada minuto de indisponibilidad sobre el nivel de servicio establecido y en base al importe de la factura del mes de incidencia mensual por nodo, para él o los nodos afectados Con un máximo de 2 eventos al mes por nodo
DISPONIBILIDAD NODOS DE CRITICIDAD ESTANDAR	**DEDUCCIÓN**
Cuando no se cumplan con los objetivos de las disponibilidades del servicio por nodo, para los diferentes niveles de disponibilidad, conforme al esquema de medición propuesto. Incluye todos los elementos que conforman cada nodo	4 al millar, por cada minuto de indisponibilidad sobre el nivel de servicio establecido y en base al importe de la factura del mes de incidencia mensual por nodo, para él o los nodos afectados Con un máximo de 3 eventos al mes por nodo
LATENCIA	**DEDUCCIÓN**
Latencia	2 al millar por cada milisegundo que el promedio exceda el límite establecido por cada clase de servicio, sobre el importe de la factura mensual por nodo, para él o los nodos afectados por incumplimiento del nivel de servicio acordado En caso de reincidencia durante dos meses consecutivos, la deducción será de 5 al millar por cada milisegundo hasta el mes en que no presente incumplimiento Con un máximo de 3 meses consecutivos
TIEMPO DE REPARACIÓN DE FALLA	**DEDUCCIÓN**
Tiempo de reparación (TTR) para falla o incidente o reconfiguración lógica, mayor a lo acordado	5 al millar por cada hora o fracción sobre el nivel de servicio establecido y en base al importe mensual por nodo para él o los nodos afectados Con máximo de 10 eventos al mes
INTERNET	**DEDUCCIÓN**
Cuando no se cumplan con los niveles mínimos de disponibilidad del servicio	5 al millar por cada minuto de indisponibilidad sobre el nivel de servicio establecido y en base al importe de la facturación mensual del servicio de Internet Con máximo 4 eventos al mes
DEGRADACIÓN POR PERDIDA DE PAQUETES	**DEDUCCIÓN**
Cuando no se cumplan con los niveles mínimos solicitados requeridos	2 al millar por décima porcentual sobre el parámetro requerido de pérdida de paquetes sin interrupción total del servicio del enlace sobre el importe de la factura por nodo para él o los nodos afectados En caso de reincidencia durante dos meses consecutivos, la deducción será del 5 al millar por décima porcentual hasta el mes en que no presente incumplimiento Con un máximo de 3 meses consecutivos

8 Anexo

8.1 Anexo t.A 'Inmuebles y Requenrn•entos de Servicio e Infraestructura para SHF.

Localidad	Domicilio	Servicios						Precio Mensual
		Red				Cantidad de Tráfico		
		Tipo de Enlace	Ancho de Banda Piso	Ancho de Banda Techo	Nivel de Criticidad	Conversacionales	Interactivos	
		Internet en Demanda	50 Mbps	100 Mbps	Alta	0%	100%	
		Internet Fijo	50 Mbps	100 Mbps				
		LAN to LAN Fijo (Mensual)	100Mbps		Estándar	0%	100%	
		Internet en Demanda Fijo 1/2	20 Mbps	50 Mbps	Alta			
		Administrados						
		Análisis de Tráfico Internet						
		Análisis de Tráfico LAN						
		Seguridad						
		FW						
		IPS						
		VAF						
		Contención de Ataques Perimetral						
		MF						
		Correlacionador						
		POMV						
		Red				Cantidad de Tráfico		
		Tipo de Enlace	Ancho de Banda Piso	Ancho de Banda Techo	Nivel de Criticidad	Conversacionales	Interactivos	
		Internet en Demanda	50 Mbps		Estándar	0%	100%	
		Seguridad						
		MF						
		Red				Cantidad de Tráfico		
		Tipo de Enlace	Ancho de Banda Piso	Ancho de Banda Techo	Nivel de Criticidad	Conversacionales	Interactivos	
		Internet en Demanda	50 Mbps		Estándar	0%	100%	
Precio de hasta 8 Certificados SSL para un dominio de internet								

TOTAL MENSUAL

TENENCIA

Servicio	Ancho de Banda	Precio mensual
nento del Servicio de Internet	50M	$
nento del Servicio de Internet	100M	$
nento del Servicio de Internet	200M	$
nento del Servicio de L2L	50M	$
nento del Servicio de L2L	100M	$
nento del Servicio de L2L	200M	$

Atentamente

Eduardo Motates Barrios

c ion de Infraestructura Tecnofogca

Ruben Quintero Ubando

Subdireccvor de Seguridad Irforma:r.a

Julio Cesar Arciniega Santos

Subdirector de Ingemena de Sistemas