CONTRATO DE PRESTACIÓN DE SERVICIOS QUE CELEBRAN, POR UNA PARTE SOCIEDAD HIPOTECARIA FEDERAL, SOCIEDAD NACIONAL DE CRÉDITO, INSTITUCIÓN DE BANCA DE DESARROLLO, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "SHF", REPRESENTADA POR LA LICENCIADA MARÍA ELENA ZALDIVAR SÁNCHEZ, EN SU CARÁCTER DE DIRECTORA DE ADMINISTRACIÓN Y APODERADA LEGAL, ASISTIDA EN ESTE ACTO POR EL INGENIERO GREGORIO LINARES URENDA, DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y ÁREA REQUIRENTE; Y POR LA OTRA, OPERBES, S.A. DE C.V., CONJUNTAMENTE CON BESTPHONE, S.A. DE C.V., A QUIEN EN LO SUCESIVO SE LES DENOMINARÁ "LAS EMPRESAS", REPRESENTADAS POR LUIS ALBERTO DE LA GARZA AGUIRRE Y EL SEÑOR CÉSAR GERÓNIMO JIMÉNEZ CERVANTES, EN SU CARÁCTER DE APODERADOS LEGALES DE AMBAS EMPRESAS, DE CONFORMIDAD CON LAS DECLARACIONES Y CLAUSULAS QUE A CONTINUACIÓN SE EXPRESAN:

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

I.- "SHF" declara, por conducto de su representante, que:

a) Es una Sociedad Nacional de Crédito, Institución de Banca de Desarrollo que se rige por su Ley Orgánica publicada en el Diario Oficial de la Federación de fecha 11 de octubre de 2001 y sus respectivas reformas, y que tiene su domicilio en la ciudad de México;

b) Tiene interés en contratar la prestación del "Servicio administrado de telecomunicaciones", en los términos, plazos, cantidades, características y condiciones que se señalan en este instrumento y sus anexos;

c) Se encuentra debidamente representada para la celebración de este acto por la licenciada María Elena Zaldívar Sánchez, en su carácter de Directora de Administración, y de apoderada legal, quien acredita su personalidad mediante escritura pública número 31, 275 de fecha 01 de abril de 2016, otorgada ante la fe del licenciado Antonio Rosado Sánchez, titular de la notaría pública número 199 de la Ciudad de México (antes Distrito Federal), facultades que no le han sido limitadas, revocadas ni modificadas en forma alguna;

d) De conformidad con el oficio circular número 307-A.-4930, de fecha 13 de diciembre de 2017, emitido por la Secretaría de Hacienda y Crédito Público, cuenta con la autorización presupuestal para erogar recursos del ejercicio fiscal del año 2018; en el entendido de que, en su caso, los recursos a erogar por los ejercicios fiscales correspondientes al 2019, 2020 y 2021, estarán sujetos a la disponibilidad presupuestaria que autorice la Secretaría de Hacienda y Crédito Público, en términos de las disposiciones legales aplicables. En este sentido, este Contrato queda sujeto a la referida disponibilidad presupuestaria, por lo que sus efectos estarán condicionados a la existencia de los recursos presupuestarios respectivos para la "SHF", sin que la no realización de la referida condición suspensiva origine responsabilidad alguna para las partes, en términos del artículo 25 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y demás normatividad relativa y aplicable;

e) El ejercicio del presupuesto correspondiente a esta contratación fue autorizado de conformidad con el oficio de fecha 21 de diciembre de 2017, emitido por su Director General, en términos de la Disposición Novena de las Disposiciones generales para la celebración de contratos plurianuales de Sociedad Hipotecaria Federal, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo, conforme con los artículos 50 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria y el artículo 148 de su Reglamento, así como con las demás disposiciones normativas aplicables, a efecto de que la "SHF" pueda erogar recursos de ejercicios fiscales distintos, con motivo de esta contratación; en el entendido de que los compromisos excedentes no cubiertos quedarán sujetos, para los fines de su ejecución y pago, a la autorización y disponibilidad presupuestal de los ejercicios fiscales 2019, 2020 y 2021;

f) Este Contrato se adjudicó a OPERBES, S.A. DE C.V., conjuntamente con BESTPHONE, S.A. DE C.V., debido al procedimiento de Adjudicación Directa, con fundamento en los artículos 26 fracción III, 40, 41 fracción III y demás relativos y aplicables de la Ley de Adquisiciones,

Arrendamientos y Servicios del Sector Público, y de su Reglamento, así como las demás disposiciones jurídicas aplicables;

g) El presente Contrato fue dictaminado procedente por su Comité de Adquisiciones, Arrendamientos y Servicios, conforme con el acuerdo II adoptado en la sesión extraordinaria 02/2018 de fecha 03 de abril de 2018, asegurándose las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes de acuerdo con la citada ley, y

h) Se formaliza el presente Contrato, bajo la modalidad de contrato abierto, con fundamento en lo dispuesto en el artículo 47 de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público, 85 de su Reglamento, y demás relativos y aplicables.

II.- "LAS EMPRESAS" declaran, por conducto de sus apoderados legales, que:

a) Es una sociedad legalmente constituida de conformidad con las leyes mexicanas bajo la denominación de OPERADORA BESTEL, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE, tal y como lo acredita con la escritura pública número 16,515 de fecha 22 de marzo de 2007, otorgada ante la fe del licenciado Felipe Ignacio Vázquez Aldana Sauza, Notario Público número 09 de la municipalidad de Tlaquepaque, Jalisco, e inscrita en la Dirección del Registro Público de la Propiedad y de Comercio del Estado de Jalisco, en el folio mercantil electrónico número 37737*1 de fecha 28 de agosto de 2007;

b) Cambia de denominación a OPERBES, S.A. DE C.V., tal y como lo acredita mediante escritura pública número 16970, tomo 85, Libro I, folios 168082 a 168085 de fecha 03 de julio de 2007, otorgada ante la fe del Notario Público No. 09 del Municipio de Tlaquepaque, Jalisco, licenciado Felipe Ignacio Vázquez Aldana Sauza, e inscrita en la Dirección del Registro Público de la Propiedad y de Comercio del Estado de Jalisco, en el folio mercantil electrónico número 37737*1;

c) En su objeto social se encuentra la prestación de los servicios como los que son del interés de la "SHF", y que cuenta con los siguientes registros: Registro Federal de Contribuyentes con clave número OPE-070326DNA;

d) Se encuentra debidamente representada para la celebración de este acto por el señor Luis Alberto de la Garza Aguirre y el señor César Gerónimo Jiménez Cervantes, quienes acreditan su personalidad mediante escritura Pública número 25, 706 de fecha 26 febrero de 2018, otorgada ante la fe del Lic. Manuel Enrique Oliveros Lara, Notario Público Número 100 de la Ciudad de México y que cuentan con facultades suficientes para obligarse, las cuales no les han sido limitadas, modificadas ni revocadas en forma alguna;

e) Es una sociedad legalmente constituida de conformidad con las leyes mexicanas bajo la denominación de BESTPHONE, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE, tal y como lo acredita con copia de la Póliza número 1906, de fecha 21 de septiembre de 1998, otorgada ante la fe del licenciado Ricardo Iñiguez Segura, Corredor Público número 39 del Distrito Federal (hoy Ciudad de México); e inscrita en el Registro Público de la Propiedad y de Comercio del Distrito Federal (hoy Ciudad de México), con el folio mercantil número 242,894;

f) En su objeto social se encuentra la prestación de los servicios como los que son del interés de la "SHF", y que cuenta con los siguientes registros: Registro Federal de Contribuyentes con clave número BES-9809218V6;

g) Se encuentra debidamente representada para la celebración de este acto por el señor Luis Alberto de la Garza Aguirre y el señor César Gerónimo Jiménez Cervantes, quienes acreditan su personalidad mediante escritura pública número Escritura Pública número 76,744 de fecha 26 febrero de 2018, otorgada ante la fe del Lic. Rafael Manuel Oliveros Lara, Notario Público Número 45 de la Ciudad de México y que cuentan con facultades suficientes para obligarse, las cuales no les han sido limitadas, modificadas ni revocadas en forma alguna;

Bestel
Jurídico

h) Han ofrecido a la "SHF" proporcionarle los servicios a que se refiere el inciso b) de la Declaración I anterior, conforme con lo pactado en este Contrato y en sus anexos, así como con la normatividad, legislación y reglamentación de la materia aplicable; cumpliendo al efecto con las especificaciones fijadas en las Normas Oficiales Mexicanas, en las Normas Mexicanas o, en su caso, las normas de referencia, de conformidad con lo dispuesto por los artículos 55 y 67 de la Ley Federal sobre Metrología y Normalización;

i) Cuentan con la capacidad jurídica y económica, así como con la organización y los elementos técnicos y humanos, especializados y necesarios, por lo que es patrón que reúne los requisitos a que se refiere el artículo 13 de la Ley Federal del Trabajo;

j) No se encuentran en alguno de los supuestos a que se refiere la Ley General de Responsabilidades Administrativas, por lo que hace a los supuestos relacionados con las contrataciones públicas; así como que tampoco se ubica en alguno de los supuestos a que hace referencia los artículos 50 y 60 antepenúltimo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público;

k) Conocen plenamente el contenido y los requisitos que establecen la normatividad y disposiciones jurídicas nacionales y extranjeras aplicables en la materia de contratación, a la fecha de celebración de este instrumento, así como el contenido de sus anexos;

l) Cumplen con lo establecido en el artículo 32-D del Código Fiscal de la Federación y de conformidad con la regla de la Resolución Miscelánea Fiscal que le resulte aplicable para el ejercicio fiscal del 2018, según lo establecido en el documento que se adjunta a este Contrato como anexo "B";

m) Cuentan con el documento de opinión de Obligaciones Fiscales en Materia de Seguridad Social, de conformidad con el numeral 4.2.6.1. Elementos del Subproceso del Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como por el Acuerdo ACDO.SA1.HCT.101214/281.P.DIR y su Anexo Único, dictado por el H. Consejo Técnico, relativo a las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social, que se adjunta a este Contrato como anexo "C", y

n) Se encuentran al corriente de sus Obligaciones Fiscales 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 en materia de aportaciones patronales y entero de descuentos, según lo establecido en el documento que se adjunta a este Contrato como anexo "D"."

Expuesto lo anterior, las partes otorgan las siguientes:

C L A U S U L A S

PRIMERA.- Bajo los términos y condiciones del presente Contrato y sus anexos dentro de un presupuesto mínimo de $3,402,000.00 M.N. (TRES MILLONES CUATROCIENTOS DOS MIL PESOS 00/100 MONEDA NACIONAL) más el correspondiente Impuesto al Valor Agregado, y un presupuesto máximo de $8,505,000.00 M.N. (OCHO MILLONES QUINIENTOS CINCO MIL PESOS 00/100 MONEDA NACIONAL), más el correspondiente Impuesto al Valor Agregado, para el ejercicio fiscal 2018, y dentro de un presupuesto mínimo de $4,872,000.00 M.N. (CUATRO MILLONES OCHOCIENTOS SETENTA Y DOS MIL PESOS 00/100 MONEDA NACIONAL) más el correspondiente Impuesto al Valor Agregado, y un presupuesto máximo de $12,180,000.00 M.N. (DOCE MILLONES CIENTO OCHENTA MIL PESOS 00/100 MONEDA NACIONAL), más el correspondiente Impuesto al Valor Agregado, para el ejercicio fiscal 2019, y dentro de un presupuesto mínimo de $4,872,000.00 M.N. (CUATRO MILLONES OCHOCIENTOS SETENTA Y DOS MIL PESOS 00/100 MONEDA NACIONAL) más el correspondiente Impuesto al Valor Agregado, y un presupuesto máximo de $12,180,000.00 M.N. (DOCE MILLONES CIENTO OCHENTA MIL PESOS 00/100 MONEDA NACIONAL), más el correspondiente Impuesto al Valor Agregado, para el ejercicio fiscal 2020, y dentro de un presupuesto

Bestel Jurídico

mínimo de $1,218,000.00 M.N. (UN MILLÓN DOSCIENTOS DIECIOCHO MIL PESOS 00/100 MONEDA NACIONAL) más el correspondiente Impuesto al Valor Agregado, y un presupuesto máximo de $3,045,000.00 (TRES MILLONES CUARENTA Y CINCO MIL PESOS 00/100 MONEDA NACIONAL), más el correspondiente Impuesto al Valor Agregado, para el ejercicio fiscal 2021, "LAS EMPRESAS" se obligan a prestar los servicios descritos en el inciso b) de la Declaración I de este Contrato, de conformidad con los términos, plazos, condiciones, características, especificaciones, y cantidades mínimas y máximas que se señalan en el anexo "A" de este instrumento, los cuales se denominarán, para fines de brevedad como "LOS SERVICIOS", en el entendido de que, en su caso, los recursos a erogar por los ejercicios fiscales correspondientes a los años 2019, 2020 y 2021, estarán sujetos a disponibilidad presupuestaria que autorice la Secretaría de Hacienda y Crédito Público, en términos de las disposiciones normativas aplicables.

Las cantidades referidas en la presente cláusula se determinarán conforme al número de "LOS SERVICIOS", que requiera "SHF", en el entendido de que el costo unitario de cada uno corresponde al que se indica en el anexo "A" de este instrumento, en el entendido de que son precios fijos.

SEGUNDA.- En relación con lo expresado en la cláusula precedente, "LAS EMPRESAS" se obligan además a lo siguiente:

a) Llevar a cabo la prestación de "LOS SERVICIOS" a partir del cuatro de abril de dos mil dieciocho, y hasta el tres de abril de dos mil veintiuno, conforme con los términos, plazos, condiciones, características, especificaciones, establecidas en este Contrato y sus anexos;

b) Aportar por su cuenta todo el personal, así como todos los recursos, elementos, materiales, accesorios y equipos que se requieran para la correcta prestación de "LOS SERVICIOS";

c) Prestar "LOS SERVICIOS" conforme con los procedimientos más adecuados que la técnica aconseje;

d) Tramitar por su cuenta o contar con las licencias o permisos que se requieran para la realización de "LOS SERVICIOS";

e) Garantizar la buena calidad de "LOS SERVICIOS" materia de contratación durante 30 (treinta) días, a partir de la respectiva fecha de aceptación por parte de la "SHF". Esta garantía es sin perjuicio de la expresada en la cláusula Tercera;

f) Prestar "LOS SERVICIOS" auxiliándose, en su caso, del personal técnico que esté debidamente capacitado y autorizado en términos de la legislación aplicable y de los anexos de este Contrato;

g) Cumplir y vigilar que se cumpla estrictamente con las disposiciones legales y reglamentarias que resulten aplicables a la prestación de "LOS SERVICIOS", y en el evento de que, por incumplimiento de dichas disposiciones, se impusiere a la "SHF" alguna multa o sanción, "LAS EMPRESAS" se obliga a cubrir, por su cuenta, el importe de éstas y a realizar de inmediato los trámites correspondientes, a fin de regularizar la situación creada;

h) Ajustarse en la prestación de "LOS SERVICIOS", a las medidas de seguridad, horarios, días y otras especificaciones que la "SHF" determine, en caso de requerir el acceso a sus oficinas;

i) Destinar el número suficiente de sus trabajadores y colaboradores, a efecto de que "LOS SERVICIOS" sean prestados con la debida oportunidad, eficiencia y seguridad, de manera que los intereses de la "SHF" queden debidamente protegidos. Asimismo, "LAS EMPRESAS" se obligan a proporcionar a su personal, el equipo necesario para el debido cumplimiento de las obligaciones que para él derivan de este Contrato;

j) Atender puntualmente a las indicaciones que para el eficaz desempeño de "LOS SERVICIOS" reciba de la "SHF" a través de la persona o personas autorizadas al efecto. Asimismo, presentar a la "SHF", cada vez que lo solicite, un reporte por escrito que contenga el estado que guardan "LOS SERVICIOS" de que se trata, así como sus comentarios respecto a éstos;

Bestel
Jurídico

k) Poner en conocimiento de la "SHF", inmediatamente y en forma escrita, cualquier hecho o circunstancia que pudiera traducirse en beneficio, daño o perjuicio de los intereses de la propia "SHF", a menos que la urgencia del caso requiera hacerlo por cualquier otro medio;

l) Conservar en el lugar o lugares que la "SHF" le indique, los instrumentos o materiales necesarios para la adecuada prestación de "LOS SERVICIOS", en el entendido de que dichos instrumentos serán guardados bajo la exclusiva responsabilidad de "LAS EMPRESAS";

m) Guardar estricta confidencialidad y/o reserva sobre la prestación de "LOS SERVICIOS", asumiendo la responsabilidad que por daños y perjuicios se pudiera causar a la propia "SHF" o a terceros;

b) En caso de que "LAS EMPRESAS" incumplan en la prestación de "LOS SERVICIOS" en el plazo previsto en el inciso a) de esta cláusula, así como en los plazos específicos que se puedan señalar en el anexo "A" de este instrumento, cubrirá a la "SHF", por cada día natural de retraso, una pena convencional de 1 al millar, sobre el monto total de "LOS SERVICIOS" no prestados oportunamente, durante los primeros cinco días naturales de retraso; de 1.5 al millar, sobre el monto total de "LOS SERVICIOS" no prestados oportunamente, por los cinco días naturales siguientes y de 2 al millar, sobre el monto total de "LOS SERVICIOS" no prestados oportunamente, por los días naturales subsecuentes; así como por la inadecuada ejecución de "LOS SERVICIOS" que dé lugar a reclamaciones o rechazo de éstos en términos del anexo "A"; en el entendido de que estas penalizaciones no excederán el importe de la garantía de cumplimiento de Contrato. No obstante, la "SHF" podrá considerar la aplicación de la referida pena convencional hasta por un plazo máximo de 20 (veinte) días naturales, siendo éste el límite a que hace referencia el artículo 53 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. La pena convencional mencionada no será aplicable si la causa del retraso es imputable a la "SHF", o a su personal.

En este acto, "LAS EMPRESAS" autoriza a la "SHF" a deducir de los pagos que, de conformidad con la cláusula Tercera de este Contrato, la segunda deba hacer a la primera, el importe de la pena referida en el párrafo que precede, en el entendido de que cualquier pago de "LOS SERVICIOS" que tenga que realizar la "SHF" a favor de "LAS EMPRESAS", quedará condicionado al pago que éstas deban efectuar por concepto de penas convencionales. Lo anterior, sin perjuicio de hacer, en su caso, efectiva la garantía que se establece en la cláusula Tercera de este instrumento.

La suma de las penas convencionales pactadas en este Contrato, no podrá en ningún caso exceder el importe de la garantía de cumplimiento de Contrato que se expresa en la cláusula Tercera. Si el monto de las penas llega al límite antes expresado, la "SHF" podrá iniciar el día hábil siguiente, el procedimiento de rescisión administrativa, salvo que resuelva, conforme con las disposiciones aplicables, iniciarlo dentro del plazo que éstas mismas prevén.

n) Entregar a la "SHF" la póliza de fianza de cumplimiento a que se refiere la cláusula Tercera de este Contrato, en un plazo no mayor de 10 (diez) días naturales, contado a partir de la fecha de firma de este instrumento;

o) Reponer "LOS SERVICIOS" que sean rechazados o devueltos por la "SHF", en razón de que se identifiquen defectos y/o discrepancias, o incumplimiento respecto de las características y condiciones establecidas en el anexo "A" de este instrumento, en un lapso no mayor de 10 (diez) días hábiles bancarios contado a partir de la fecha de rechazo o devolución;

p) Facturar sus servicios enviando el Comprobante Fiscal Digital por Internet (CFDI), conforme a la normatividad fiscal que resulte aplicable. El CFDI, en archivos PDF y XML, deberá depositarse en el siguiente Buzón: cfdshf@shf.gob.mx, marcándole copia a las siguientes direcciones de correo electrónico molvera@shf.gob.mx, y eogarcia@shf.gob.mx;

q) Sujetarse a lo dispuesto en el anexo "E", en cuestiones de facturación, devolución, rechazo y/o condiciones específicas de "LOS SERVICIOS";

Bestel
Jurídico

r) Otorgar el soporte técnico especializado de "LOS SERVICIOS", en los términos contenidos en el anexo "A", durante 90 (noventa) días contado a partir de la firma del Contrato;

s) En su caso, brindar la información y documentación relacionada con el presente Contrato que le sea requerida por las autoridades fiscalizadoras, en términos de lo señalado por el artículo 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, artículo 107 de su Reglamento, y demás normatividad relativa y aplicable;

t) En caso de así considerarlo conveniente, presentar ante la Secretaría de la Función Pública, su solicitud de conciliación por desavenencias derivadas del cumplimiento y/o ejecución del Contrato, debiendo cumplir con los requisitos contenidos en los artículos 77 y 78 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y artículos 127 y 128 de su Reglamento, y demás disposiciones relativas y aplicables; sin perjuicio de lo anterior en los casos que resulte procedente, "SHF" y "LAS EMPRESAS" se sujetaran a lo establecido en el *"DECRETO por el que se establecen las acciones administrativas que deberá implementar la Administración Pública Federal para llevar a cabo la conciliación o la celebración de convenios o acuerdos previstos en las leyes respectivas como medios alternativos de solución de controversias que se susciten con los particulares"*, así como a los *Lineamientos* que la autoridad competente en la materia emita, y

u) Las demás que, en su caso, se contemplen en los anexos de este Contrato.

En caso de que "LAS EMPRESAS" incumplan con alguna de las obligaciones contempladas en este Contrato, y en especial con las contenidas en esta cláusula, la "SHF" podrá iniciar en cualquier momento el procedimiento de rescisión que corresponda, en los términos del artículo 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Todas las obligaciones contenidas en este Contrato y sus anexos y, en lo específico, las descritas en esta cláusula, se deberán ejecutar por medio de "LAS EMPRESAS", sin que "SHF" tenga la posibilidad de dirección, vigilancia o capacitación sobre los empleados, trabajadores o personal que destinen "LAS EMPRESAS" para la prestación de "LOS SERVICIOS". En este sentido, cualquier facultad o prerrogativa que deriven a favor de "SHF" por la prestación de "LOS SERVICIOS" materia de contratación, o por virtud de este Contrato o de cualquier normatividad que exista o pudiera existir, se entenderá que siempre ejercerá dicha facultad o hará valer dicha prerrogativa, por conducto del ejecutivo de cuenta o personal de contacto que para tales efectos determinen "LAS EMPRESAS", sin que pueda nunca ejercer dichas facultades o prerrogativas de manera directa "SHF" sobre los empleados, trabajadores o personal que "LAS EMPRESAS" destinen para la prestación de "LOS SERVICIOS".

TERCERA.- "SHF" se obliga a pagar a "LAS EMPRESAS" en concepto de precio, por la completa y total prestación de "LOS SERVICIOS", a entera satisfacción de "SHF", a mes vencido, las cantidades que resulten por periodo, de acuerdo a lo establecido en el anexo "A", ajustándose a los presupuestos mínimos y máximos referidos en la cláusula Primera anterior, a más tardar dentro de los 20 (veinte) días naturales siguientes a la prestación de "LOS SERVICIOS", previa presentación de la factura correspondiente, en la cual venga la relación de horas efectivas prestadas y que comprenda en forma desglosada el Impuesto al Valor Agregado, debidamente requisitada y suscrita por "LAS EMPRESAS", en la que aparezca el visto bueno de "SHF" y siempre que estas hubieran cumplido con sus obligaciones contractuales, en los términos de los anexos de este Contrato y de conformidad con el artículo 93 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En este sentido, la "SHF" realizará, a través de la unidad administrativa solicitante, dentro de los 5 (cinco) días hábiles bancarios siguientes a la prestación de "LOS SERVICIOS" determinará si "LAS EMPRESAS" cumplieron con todos los requerimientos establecidos en este instrumento y sus anexos. "LAS EMPRESAS" aceptan en este acto que, en tanto la "SHF" no lleve a cabo la revisión referida, "LOS SERVICIOS" no se tendrán por aceptados.

"LAS EMPRESAS" se obligan a entregar a la "SHF" dentro de los 10 (diez) días naturales posteriores a la fecha de firma de este Contrato, una póliza de fianza expedida por una institución

Bestel
Jurídico

legalmente autorizada para operar en el ramo, a favor y a satisfacción de la "SHF", por la cantidad en moneda nacional equivalente al 10% (DIEZ POR CIENTO) del importe máximo total de este Contrato, sin incluir la cantidad correspondiente al Impuesto al Valor Agregado, que garantice a ésta el fiel y exacto cumplimiento de las obligaciones que "LAS EMPRESAS" asumen con motivo de este Contrato, comprendiéndose entre éstas, la buena calidad de "LOS SERVICIOS" materia de este Contrato; la correcta y puntual prestación de éstos; la devolución de la cantidad que la "SHF" le haya cubierto a "LAS EMPRESAS", así como el reembolso por parte de "LAS EMPRESAS" a la "SHF" de los gastos en que incurran éstas en caso de que sea rechazado parte o la totalidad de "LOS SERVICIOS" materia de este Contrato por no cumplir con las cantidades, características y especificaciones que se contienen en los anexos de este Contrato; el pago de las cantidades que resulten conforme con lo pactado en las cláusulas de este Contrato, en especial, las que se establecen en sus cláusulas Primera, Segunda, Tercera Quinta, Sexta y Séptima; el pago de la cantidad derivada de los defectos o vicios ocultos de "LOS SERVICIOS" materia de contratación o de cualquier otra responsabilidad en que "LAS EMPRESAS" hubieran incurrido; así como el exacto cumplimiento de las demás obligaciones consecuentes a lo aquí convenido, a la buena fe, al uso o a la ley. Dicha póliza estará en vigor hasta 30 (treinta) días naturales posteriores a la fecha en que la "SHF" acepte la totalidad de "LOS SERVICIOS" materia de contratación a su entera satisfacción y una vez que haya vencido la garantía a que hace referencia el inciso e) de la cláusula Segunda de este contrato, así como durante la substanciación de todos los recursos legales o juicios que se interpongan y hasta que se dicte resolución definitiva por la autoridad competente y para su cancelación se requerirá la autorización previa y por escrito de la "SHF".

La póliza de fianza referida en el párrafo anterior, es con independencia de las demás garantías de "LOS SERVICIOS" que se puedan establecer en el anexo "A" de este Contrato.

En ese orden de ideas, las partes convienen en que para el caso de que "LAS EMPRESAS" cumplan con las obligaciones contractuales estipuladas en el presente Contrato y sus anexos, el servidor público encargado de vigilar la administración y cumplimiento del Contrato, extenderá una constancia de cumplimiento de las obligaciones, conforme los procedimientos internos de la "SHF" y a través de las unidades administrativas que correspondan, a efecto de que esta última inicie los trámites de cancelación de la póliza de fianza de cumplimiento señalada en el párrafo que antecede.

Las partes convienen en que dentro del importe total por la prestación de "LOS SERVICIOS" materia de contratación, en los términos de esta cláusula, quedan comprendidos todos los gastos directos e indirectos que "LAS EMPRESAS" tuvieran que efectuar para la debida realización de la materia de este Contrato y sus anexos, por lo que no tendrá derecho a recibir ninguna otra cantidad por concepto de gastos o expensas; acordándose que el monto de contratación será fijo durante toda la vigencia del Contrato, por lo que no podrá sufrir ajuste alguno.

En caso de que "LAS EMPRESAS" no presten "LOS SERVICIOS" materia del Contrato conforme con lo previsto en este instrumento, y sin perjuicio de las sanciones expresadas en el mismo, la "SHF" podrá ordenar su reposición o corrección inmediata, misma que "LAS EMPRESAS" harán por su cuenta sin que tenga derecho a retribución por ello.

Las partes convienen en que la garantía que deba otorgar "LAS EMPRESAS", contendrá el texto del modelo que forma parte de los anexos de este Contrato. Asimismo, el inicio de la prestación de "LOS SERVICIOS", queda condicionado a que "LAS EMPRESAS" entreguen en el plazo previsto la garantía correspondiente.

CUARTA.- La "SHF" se reserva el derecho de inspeccionar en todo tiempo la prestación de "LOS SERVICIOS" y de hacer a "LAS EMPRESAS", por conducto de la persona o personas autorizadas por la primera al efecto, las observaciones que estime pertinentes en relación con el cumplimiento de este Contrato. Asimismo, "LAS EMPRESAS" se obligan a otorgar toda clase de facilidades y ayuda a las personas designadas por la "SHF" para que puedan llevar a cabo la inspección de que se trata.

"LAS EMPRESAS" se obligan desde ahora a atender todas las observaciones que le hiciere la "SHF" a través de las personas autorizadas, y en el caso de que adujera razones técnicas para no hacerlo, deberán ponerlas a la consideración de la "SHF", mediante comunicación escrita, a fin de que ésta resuelva en definitiva.

Bestel
Jurídico

Asimismo, "LAS EMPRESAS" se obligan a sustituir, alguna o algunas de las personas destinadas para la prestación de "LOS SERVICIOS", cuando la "SHF" así lo solicite por escrito, en el entendido de que la nueva persona designada por "LAS EMPRESAS" deberá cumplir con los mismos requisitos de experiencia y capacidad que tenía la persona originalmente destinada para la prestación de "LOS SERVICIOS".

QUINTA.- "LAS EMPRESAS" se obligan a defender a la "SHF", sin cargo alguno para éstas, de las reclamaciones de terceros basadas en que "LOS SERVICIOS", o el resultado de éstos, constituyen trasgresión a algún derecho de autor, o bien, invasión u otra trasgresión a alguna patente, marca, licencia, o que viola registro de derechos, o cualquiera otro relativo a la propiedad intelectual o industrial, siempre y cuando la "SHF" le dé aviso por escrito de tales reclamaciones en un plazo no mayor de 5 (cinco) días hábiles bancarios contados a partir del día siguiente en que se hubiere practicado el emplazamiento o notificación. Asimismo, en ese plazo la "SHF" deberá entregar la información y asistencia del caso o establecer las causas por las cuales esté impedida de proporcionarlas. En este mismo supuesto, la "SHF" se obliga a efectuar las gestiones necesarias a fin de que "LAS EMPRESAS" puedan representarla en el proceso o procedimiento respectivo.

En el caso de que se dictara sentencia definitiva en contra de la "SHF", con o sin intervención de "LAS EMPRESAS", estas últimas se obligan a pagar las sumas a que sea condenada la "SHF", o las cantidades que se deriven del arreglo que se tuviere con el tercero, pero no serán responsables por ninguna cantidad derivada de compromisos contraídos por el citado arreglo si ésta no cuenta con el previo consentimiento de "LAS EMPRESAS" dado por escrito, el cual deberá otorgarse invariablemente dentro de los 5 (cinco) días posteriores a aquel en que tenga conocimiento del pretendido arreglo.

En todo caso, "LAS EMPRESAS" se obligan a tomar las medidas necesarias para que la "SHF" continúe recibiendo "LOS SERVICIOS" en los plazos y condiciones convenidos.

SEXTA.- "LAS EMPRESAS" se hacen responsables ante la "SHF" de la conducta y eficiencia de la persona que, en su caso, destine para la prestación de "LOS SERVICIOS". Igualmente, en el evento de que "LAS EMPRESAS" no cumplan con alguna de las obligaciones que en virtud de este Contrato, del uso, de la buena fe o de la ley son a su cargo, serán responsables de los daños y perjuicios que su incumplimiento cause a la "SHF" o a terceros. Sin perjuicio de lo anterior, la "SHF" podrá rescindir administrativamente este Contrato sin responsabilidad alguna a su cargo, o bien, exigir su cumplimiento haciendo en su caso efectiva la pena convencional que se menciona en la cláusula Segunda de este instrumento.

Las partes convienen en que la "SHF" podrá exigir el cumplimiento de este Contrato a "LAS EMPRESAS" conforme con lo expresado en esta cláusula, y en el evento de que continuaran los incumplimientos, podrá rescindir administrativamente este instrumento, sin perjuicio de hacer efectiva la garantía otorgada, de conformidad con lo dispuesto en la cláusula Tercera de este instrumento.

En caso de que "LA EMPRESAS" fallen en la prestación de "LOS SERVICIOS" materia de contratación, la "SHF" tendrá el derecho de adquirirlos o contratarlos, por sí o por medio de terceros, con cargo a "LAS EMPRESAS, independientemente de que se aplicarán las sanciones previstas en la cláusula Segunda o de que se pueda hacer efectiva la garantía a que se refiere la cláusula Tercera de este instrumento de forma proporcional al monto de las obligaciones incumplidas.

En el evento de que "LAS EMPRESAS" hubieren faltado a la verdad en relación con lo expresado en el inciso j) de la Declaración II de este Contrato, la "SHF" dará por rescindido administrativamente este instrumento en la forma convenida en el mismo.

SÉPTIMA.- "LAS EMPRESAS" se constituyen, por su carácter de patrón, son responsables únicas de las relaciones entre ellas y las personas que destinen en la prestación de "LOS SERVICIOS", además de las dificultades o conflictos que pudieran surgir entre ellas y dichas personas o de estas últimas entre sí. También serán responsables de los accidentes que se originen con motivo de la prestación de dichos servicios y responderán, asimismo, de todos los daños y perjuicios que se llegaren a ocasionar a la "SHF" o a terceros, con motivo o como consecuencia de la prestación u omisión en la prestación de los referidos servicios, si el accidente es imputable a la persona que destine "LAS EMPRESAS" para la prestación de "LOS SERVICIOS".

Bestel
Jurídico

Anzures, Código Postal 11590, Delegación Miguel Hidalgo, Ciudad de México, México.

A la atención del Ingeniero Gregorio Linares Urenda, Director de Tecnologías de la Información.

Asimismo, el Ingeniero Miguel Ángel Olvera Rincón, Subdirector de Ingeniería de Sistemas, será el servidor público responsable de administrar y vigilar el cumplimiento de este Contrato, de manera coordinada con el servidor público indicado en el párrafo anterior.

Por parte de la "SHF" a "LAS EMPRESAS" en Montecito 38, piso 28 oficina 1, Colonia Nápoles, Código Postal 03810, Delegación Benito Juárez, Ciudad de México, México.

A la atención de la Señora María Teresa Rodríguez Romo y el Señor César Gerónimo Jiménez Cervantes, apoderados legales de ambas empresas.

DÉCIMA SEGUNDA.- "LAS EMPRESAS" no podrán traspasar o ceder total o parcialmente la materia de este Contrato. Se exceptúan de lo anterior, los derechos de cobro derivados de este instrumento, previa conformidad de la "SHF" dada por escrito.

Sin perjuicio de lo estipulado en el párrafo anterior, "SHF" manifiesta desde ahora su conformidad para que "LAS EMPRESAS", únicamente puedan ceder sus derechos de cobro a favor de un Intermediario Financiero mediante operaciones de Factoraje o Descuento Electrónico en el programa de Cadenas Productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo, en los términos de la normatividad relativa y aplicable.

DÉCIMA TERCERA.- "LAS EMPRESAS" reconocen que la información y documentación que la "SHF" le proporcione, así como los datos y resultados obtenidos de "LOS SERVICIOS", son confidenciales y/o reservados y propiedad de la "SHF"; por tal razón, " LAS EMPRESAS " se obligan a guardar y mantener en absoluta confidencialidad y/o reserva toda la información, tangible e intangible, que llegaran a obtener referente a la "SHF" y cualquier otro tercero, para la realización y prestación de "LOS SERVICIOS", así como los resultados y/o productos derivados de su ejecución. Por lo que deberán mantener el secreto profesional a que están obligadas "LAS EMPRESAS" por la prestación de "LOS SERVICIOS".

"LAS EMPRESAS" se obligan a utilizar la información confidencial y/o reserva únicamente para la realización y cumplimiento de este Contrato, quedándole estrictamente prohibido, divulgarla por cualquier medio a terceros o darle un uso diverso al establecido en este instrumento, ni aún a nivel curricular, salvo autorización previa y por escrito de la "SHF", y en términos de la legislación aplicable.

"LAS EMPRESAS" se obligan a manejar la información confidencial y/o reservada propiedad de la "SHF", y cualquier otro tercero, igual o mejor que su propia información confidencial.

A la terminación o rescisión de este Contrato, "LAS EMPRESAS" se obligan a devolver a la "SHF", toda la información obtenida y/o generada para la realización de "LOS SERVICIOS", así como a entregar los productos derivados de su ejecución, en los términos y condiciones que se describen en el anexo "A" del presente instrumento.

La obligación de confidencialidad a cargo de "LAS EMPRESAS" a que se refiere esta cláusula, permanecerá vigente con toda su fuerza y vigor aún después de terminada la vigencia de este Contrato, en términos de las disposiciones legales aplicables.

"LAS EMPRESAS" y su personal no podrán reproducir, alterar, transmitir o comercializar la información o los códigos que la "SHF" le proporcione, a efecto de llevar a cabo cualquier actividad que no se comprenda en la prestación de "LOS SERVICIOS". En caso de incumplimiento de esta obligación, "LAS EMPRESAS" atenderán a la responsabilidad civil, penal, administrativa y demás que resulten en su contra en términos de la normatividad aplicable.

"LAS EMPRESAS" deberán considerar en todo momento que la información que la "SHF" le proporcione para la prestación de "LOS SERVICIOS", por sí o través del o los terceros que al efecto designe, está en su caso clasificada como reservada y/o confidencial en términos de la Ley Federal de

Bestel

"LAS EMPRESAS", por su carácter de patrón para con sus trabajadores, se encargarán de delimitar legalmente que en ningún caso se deberá tomar a la "SHF" como patrón sustituto, obligándose desde este momento a que, si por alguna razón se le llegare a fincar alguna responsabilidad a la "SHF" por ese concepto, "LAS EMPRESAS" le reembolsarán a la "SHF" cualquier gasto en que, por tal motivo, incurriere ésta.

OCTAVA.- La vigencia de este Contrato es a partir del cuatro de abril de dos mil dieciocho, y hasta el tres de abril de dos mil veintiuno, conforme con los términos, plazos, condiciones, características, especificaciones descritas en este instrumentos y sus anexos.

Sin embargo, las partes previo al vencimiento de la fecha de cumplimiento y a sus ampliaciones o prórrogas a solicitud expresa de "LAS EMPRESAS", y por caso fortuito o fuerza mayor, o por causas atribuibles a la "SHF", podrán modificar el Contrato a efecto de ampliar la fecha para la entrega de "LOS SERVICIOS". En este supuesto deberá formalizarse el convenio modificatorio relativo y no procederá la aplicación de las penas convencionales respectivas.

Durante la vigencia pactada y, en su caso, durante la ampliación o ampliaciones así como a su prórroga o prórrogas que al efecto se convengan, la "SHF" podrá dar por terminado anticipadamente este Contrato, sin responsabilidad alguna a su cargo, entre otras causas, cuando no cuente con la autorización de la partida presupuestal correspondiente en términos de las disposiciones legales aplicables, mediante simple aviso escrito que dé a "LAS EMPRESAS" por lo menos con 5 (cinco) días naturales de anticipación a la fecha respectiva.

NOVENA.- Cuando en la prestación de "LOS SERVICIOS" se presente caso fortuito o fuerza mayor, la "SHF" podrá suspender la prestación de los mismos, en cuyo caso sólo se pagará a "LAS EMPRESAS" aquéllos que se hayan prestado efectivamente, para lo cual deberán levantar y suscribir acta circunstanciada en la que conste los motivos y plazo de la suspensión en términos del artículo 55-Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y numeral, de manera conjunta con "LAS EMPRESAS".

Cuando la suspensión obedezca a causas imputables a la "SHF", ésta pagará a "LAS EMPRESAS" los gastos no recuperables durante el tiempo de la suspensión, siempre que dichos gastos sean razonables, estén debidamente comprobados y se relacionen directamente con este Contrato, previa aprobación por escrito de la "SHF".

El pago de dichos gastos no recuperables se realizará dentro de los 20 (veinte) días naturales siguientes a la presentación de la documentación respectiva por parte de "LAS EMPRESAS".

DÉCIMA.- Los anexos que se mencionan en este Contrato, debidamente identificados con la firma de las partes se agregan a este instrumento como parte integrante del mismo. Asimismo, las partes se obligan a firmar todas y cada una de las páginas de este Contrato y sus anexos.

Las partes convienen que en el evento de que alguno o algunos de los términos y condiciones estipulados en las cláusulas de este Contrato difieran o existiera cualquier discrepancia con los términos y condiciones previstas en los anexos a que se refiere el párrafo precedente, prevalecerán las primeras sobre los segundos, para todos los efectos legales correspondientes.

En ese mismo sentido, las partes convienen que en el evento de presentarse alguna discrepancia entre el presente Contrato y los actos y/o documentos derivados del procedimiento de contratación, prevalecerán estos últimos sobre el primero; lo anterior, sin perjuicio de lo dispuesto en el clausulado de este Contrato.

DÉCIMA PRIMERA.- Las partes convienen en que las comunicaciones que se crucen, relativas al presente Contrato, deberán dirigirse por escrito a las personas y domicilios siguientes, en el entendido de que dichas comunicaciones deberán ser suscritas por personal con facultades suficientes para tratar la materia a que se refieran:

Por parte de "LAS EMPRESAS" a la "SHF", en avenida Ejercito Nacional número 180, Colonia

Bestel
Jurídico

Transparencia y Acceso a la Información Pública, y demás disposiciones jurídicas que de ella emanen, o que se encuentra protegida por el secreto regulado por el artículo 142 de la Ley de Instituciones de Crédito, o demás disposiciones jurídicas que de ella emanen; por lo que deberá extremar todas las medidas que sean necesarias para salvaguardar y mantener el carácter de dicha información; por lo que "LAS EMPRESAS" no podrán otorgar un uso distinto a la misma, diferente al objeto de este Contrato; siendo responsable además, por la violación de las disposiciones contenidas en dichos ordenamientos y disposiciones jurídicas.

DECIMA CUARTA. Las partes convienen que, en lo no expresamente previsto en este Contrato, serán aplicables las disposiciones relativas de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento, así como del Código Civil Federal, de la Ley Federal de Procedimiento Administrativo y del Código Federal de Procedimientos Civiles, y que para su interpretación y cumplimiento judicial, se someten a los tribunales competentes con jurisdicción en la Ciudad de México, renunciando al fuero que pudiera corresponderles en virtud de cualquier otro domicilio presente o futuro, o por cualquier otra causa.

Al efecto, las partes señalan como sus domicilios los siguientes: la "SHF", en avenida Ejército Nacional número 180, Colonia Anzures, Código Postal 11590, Delegación Miguel Hidalgo, Ciudad de México, México, y "LAS EMPRESAS en Montecito 38, piso 28 oficina 1, Colonia Nápoles, Código Postal 03810, Delegación Miguel Hidalgo, Ciudad de México, México.

Este Contrato se suscribe en dos ejemplares, en la Ciudad de México, México, el día cuatro de abril de dos mil dieciocho, y queda uno en poder de cada una de las partes.

"SOCIEDAD HIPOTECARIA FEDERAL,
SOCIEDAD NACIONAL DE CRÉDITO,
INSTITUCION DE BANCA DE DESARROLLO"

Lic. María Elena Zaldívar Sánchez.
Directora de Administración
y Apoderada Legal.

Ing. Gregorio Linares Urenda.
Director de Tecnologías de la Información
y Área Requirente.

"LAS EMPRESAS"

Sr. Luis Alberto de la Garza Aguirre
Apoderado Legal.

Sr. César Gerónimo Jiménez Cervantes.
Apoderado Legal.

Bestef
Jurídico

Propuesta Técnica que presenta Operbes. S.A. de C.V. a "Sociedad Hipotecaria Federal" para el "Servicio administrado de telecomunicaciones"
Anexo I

Introducción

OPERBES, S.A. DE C.V. tomó en consideración que SHF para cumplir con los objetivos previstos en el Plan Nacional de Desarrollo 2013-2018 tiene la necesidad de mantener comunicación permanente entre los diversos inmuebles que la conforman, para lo cual se requiere integrar una Red Privada Virtual MPLS, que permita la transmisión segura de voz, datos y video; logrando la homologación tecnológica en materia de comunicaciones.

Alcance del Documento

OPERBES, S.A. DE C.V. tomó en consideración que el propósito del presente documento es establecer las especificaciones y lineamientos técnicos para dar continuidad a los servicios actuales a través de la contratación del Servicio Administrado de Red Privada Virtual MPLS, que incluyen los siguientes apartados: "Servicio administrado de telecomunicaciones" MPLS, Servicio de Acceso a Internet, Servicio de Seguridad Perimetral, Servicio de Operación, Entrega de Servicios, Niveles de Servicios, Servicios Complementarios, Penas Convencionales y Deductivas, Anexo VIII. Matriz de Servicios.

Objetivo del "Servicio administrado de telecomunicaciones"

OPERBES, S.A. DE C.V. tomó en consideración que el objetivo es Implementar una red privada virtual multiservicio bajo un modelo de servicio administrado en demanda que comprende los servicios de transporte de voz, datos y video, acceso a internet, soluciones de seguridad, todo lo anterior con niveles de servicio.

Alcance del Servicio

OPERBES, S.A. DE C.V. integra en su proposición la administración del proyecto, el diseño, la implementación, la operación y en general la administración de todos los servicios ofertados que se requieren en el presente documento.

OPERBES, S.A. DE C.V. tomó en consideración que Cada uno de los servicios descritos en el presente documento, podrá ser contratado de manera individual bajo demanda con base a las necesidades de SHF.

Requerimientos Generales

A partir del inicio de vigencia del contrato, OPERBES, S.A. DE C.V. iniciará las actividades necesarias para proveer los servicios administrados en cada uno de los nodos indicados, considerando que a partir del día siguiente de la firma del contrato se llevará a cabo por parte de OPERBES, S.A. DE C.V. en caso de ser el Licitante ganador, el proceso de migración e implementación de los servicios requeridos por SHF, la cual realizará una revisión y validación de los servicios que OPERBES, S.A. DE C.V. entregue.

En la presente propuesta el hardware, software, infraestructura principal (routers), infraestructura auxiliar, medios, instalaciones, adecuaciones de instalaciones complementarias y todo el personal necesario para llevar a cabo la operación y administración de los servicios solicitados serán suministrados por OPERBES, S.A. DE C.V.

Todo el hardware y software que OPERBES, S.A. DE C.V. proporcione para la prestación del servicio quedará bajo su operación y responsabilidad ante cualquier eventualidad o contingencia que pudiera ocurrir, sin importar la causa u origen, para garantizar los niveles de servicio solicitados, será sin costo adicional para SHF.

Documentación Técnica Adicional

Especificaciones técnicas de todos los componentes que forman parte de la cotización

OPERBES, S.A. DE C.V. presentará copia impresa, de la información técnica ACTUALIZADA del equipamiento (hardware, software), elementos y/o componentes que formen parte de la solución propuesta, misma que Corresponderá con lo ofertado en su proposición. OPERBES, S.A. DE C.V. tomó en consideración que no será necesario entregar copia de todo el documento, si no sólo las partes donde se indique el cumplimiento de la especificación solicitada en el presente documento; y dicha información estará resaltada para su adecuada localización. Así mismo en caso de documentación obtenida en portales de Internet se indicará la dirección URL de donde se obtuvo dicha información y en caso de que la información se encuentre en un sitio de acceso controlado se proporcionarán las claves para su consulta y verificación.

OPERBES, S.A. DE C.V. integrará a su propuesta debidamente los Anexos 1.1 "Referencias Técnicas Soluciones de Seguridad" y 1.2 "Referencias Técnicas VPN" donde se indiquen las referencias para la revisión del cumplimiento de todas las especificaciones técnicas solicitadas por SHF. La Referencia deberá estar resaltada en las copias de la información técnica proporcionada en la propuesta del Licitante.

Actualización Tecnológica

Durante la vigencia del contrato, en caso de obsolescencia que impida brindar los servicios con los niveles de servicio solicitados por SHF, los equipos o soluciones utilizados por OPERBES, S.A. DE C.V., y en general todo el equipamiento y software que incluya OPERBES, S.A. DE C.V. en su proposición, será sustituido por uno de nueva tecnología, sin costo adicional para SHF.

Servicios de la Red Privada Virtual

Descripción del Servicio.

OPERBES, S.A. DE C.V. tomó en consideración que se requiere una solución estándar al transporte de información en una red privada IP, con la fiabilidad, calidad, y seguridad de los servicios de la MPLS con base a la calidad de servicio e ingeniería de tráfico.

OPERBES, S.A. DE C.V. tomó en consideración que el "Servicio administrado de telecomunicaciones" requiere de la interconexión de SHF a través de una red privada virtual sobre MPLS para la transmisión de voz, datos y video de acuerdo a las necesidades de SHF con los niveles de servicio solicitado, así como accesos remotos para la integración a la red.

Características Técnicas del Servicio

OPERBES, S.A. DE C.V. proporcionará a SHF el servicio de comunicación e interconectividad que integre todos los nodos descritos en el "Anexo VIII. Matríz de Servicios ", mediante la implementación de una Red Privada Virtual cuyo núcleo opere con protocolo IP soportada en una infraestructura de telecomunicaciones con plataforma MPLS, en la que el acceso a la nube de MPLS sea a través de comunicaciones punto a punto de acuerdo al estándar RFC4364.

La red RPV-MPLS de OPERBES, S.A. DE C.V. dispondrá de la flexibilidad de topologías tipo malla completa (Full Mesh), tipo estrella (Hub & Spoke) o combinación de ambas con mecanismos de encripción avanzada IPSec, cumpliendo lo siguiente:

Implementará encripción sobre la red MPLS entre todos los sitios de la institución sin necesidad de implementar túneles. Preservará todos los campos originales del encabezado IP con la finalidad de no afectar el tratamiento que se le puede dar a ese tráfico.

Implementará los mecanismos estándares de HMAC-SHA y SHA-MD5 para verificar la integridad de los paquetes, DES, 3DES y AES (128, 196, 256) bits para la confidencialidad de la información transmitida y RFC3547 para la implementación de seguridad en el plano de control.

OPERBES, S.A. DE C.V. incluye en su proposición un equipo de ruteo principal (servidor de llaves) en la red que distribuya las llaves de encripción y políticas a todos los routers de la red que estén autenticados y registrados como miembros del grupo. Este mecanismo de membresía y asignación de llaves de encripción se realizará con canales seguros sin túneles mediante la implementación del estándar RFC3547. Además de distribuir las llaves de encripción a todos los routers de la red que estén autenticados y registrados como miembros de la misma RPV, el servidor de llaves también será capaz de definir las políticas de encripción (protocolos, tráfico por encriptar, temporizadores, llaves) de manera centralizada para su posterior distribución a los routers autenticados y registrados en la RPV. OPERBES, S.A. DE C.V. considera en su proposición que SHF no aceptará soluciones equivalentes a las solicitadas.

OPERBES, S.A. DE C.V. implementará más de un servidor de llaves para incrementar la confiabilidad y disponibilidad del sistema de encripción.

El servidor de llaves enviará periódicamente nuevas llaves antes que las previamente asignadas expiren.

Se permitirá la capacidad de implementar más de un servidor de llaves de tal forma que cualquiera pueda fungir como respaldo en caso de falla. Estos servidores de llaves podrán implementarse en localidades diferentes.

El ruteador de cada sitio remoto detectará falla de conectividad hacia el sistema de servidores de llaves y cambiar su modo de transmisión de encripción a texto claro.

La solución podrá escalar hasta miles de sitios en topología de malla completa en un grupo único de encripción.

Los equipos CPE realizarán la encripción vía hardware.

Los equipos CPE incluirán el licenciamiento necesario para brindar las funcionalidades requeridas por SHF de acuerdo a lo descrito en la Matriz de Servicios.

Se incluirá toda la infraestructura necesaria para habilitar los esquemas de encripción y llaves. De tal manera que el añadir un nuevo sitio a la red RPV-MPLS del Licitante que lo requiera, no implicará el realizar ningún cambio significativo en la configuración de los sitios ya existentes.

OPERBES, S.A. DE C.V. será responsable de enrutar desde el nodo origen hasta el nodo destino el tráfico de voz, datos o video que se genere en las redes de área local de SHF.

OPERBES, S.A. DE C.V. tomó en consideración que durante la vigencia de la contratación, se requiere del servicio 7x24, SHF utilizará la RPV-MPLS para transportar cualquier tipo de tráfico a través del protocolo IP para establecer comunicaciones seguras entre los nodos que conformen la RPV-MPLS.

El protocolo de enrutamiento entre el equipo ruteador multiservicio provisto por OPERBES, S.A. DE C.V. y el equipo de conmutación de SHF, podrá ser estático y/o dinámico conforme a la solicitud de cada una de ellas, en el caso de tratarse de un enrutamiento dinámico se utilizarán los protocolos BGP4 u OSPF dependiendo de los requerimientos particulares para cada una de SHF, las cuales contarán con un identificador de red MPLS (RPV-MPLS _IDs) respetando, en su caso, los IDs actuales.

OPERBES, S.A. DE C.V. tomó en consideración que El ancho de banda solicitado para cada nodo de la RPV-MPLS se especifica en el "Anexo VIII. Matriz de Servicios", el cual podrá ser utilizado por los diferentes tipos de tráfico: voz, datos y video.

OPERBES, S.A. DE C.V. tomó en consideración que en caso de no transmitir alguno de estos tipos de tráfico (voz, datos críticos y video), se podrá utilizar el ancho de banda disponible, evitando reservar canales de comunicación exclusivos y procurando el uso eficiente de los recursos de comunicaciones, es decir, el ancho de banda no será dedicado en canales para el uso exclusivo de algún tipo de tráfico: voz, datos o video.

OPERBES, S.A. DE C.V. tomó en consideración que para el servicio solicitado en esquema fijo, garantizará un ancho de banda fijo, requerido por SHF, será simétrico y bidireccional, los anchos de banda incluidos se especifican en el "Anexo VIII. Matriz de Servicios".

OPERBES, S.A. DE C.V. tomó en consideración que para el servicio solicitado en esquema bajo demanda, teniendo en consideración los valores de ancho de banda mínimo y máximo expresados en el "Anexo VIII. Matriz de Servicios", así como la tabla de valores de ancho de banda que pueden requerirse y los niveles de servicio que se aplicarán en casos de incrementos o decrementos durante la vigencia del servicio.

OPERBES, S.A. DE C.V. tomó en consideración que el cobro del esquema bajo demanda será calculado por medio de la regla de percentil 95 que consiste en monitorear el tráfico cursado por el cliente, descartando los picos de tráfico generados: sobre los dos sentidos del circuito de interconexión, se toman de manera simultánea muestras cada 5 minutos escogiéndose para cada par de muestras la de valor superior, resultando en 12 muestras a la hora, 288 muestras al día, 8640 al mes. De la serie resultante al ordenar de mayor a menor esas 8640 muestras, se elimina el 5% más alto, es decir, los 432 valores máximos del mes. El valor máximo de la sub-serie resultante, redondeado a la unidad inferior por exceso y expresado en Mbps.

La RPV MPLS Propuesta por OPERBES, S.A. DE C.V. soportará al menos 4 niveles de calidad de servicio (QoS) TOMANDO COMO EL DE MAYOR PRIORIDAD QoS1, como se indica a continuación:

QoS1: Voz

QoS2: Video

QoS3: Datos Críticos

QoS4: Datos Normales

El incremento o decremento para cada QoS dentro del ancho de banda solicitado durante el tiempo de contratación no impactará en el precio ofertado.

Los anchos de banda de las calidades de servicio serán dinámicos y en tiempo real de menor a mayor criticidad.

La red RPV MPLS de OPERBES, S.A. DE C.V. permitirá flexibilidad, es decir, que las aplicaciones (puertos TCP) puedan asignarse dentro del ancho de banda solicitado para las calidades

de servicio mencionadas según las necesidades de SHF, sin tener un costo adicional dentro del ancho de banda total del puerto de RPV MPLS para cada nodo de SHF.

La red de OPERBES, S.A. DE C.V. será escalable, es decir, que tendrá la flexibilidad, eficiencia y transparencia suficientes para que en el momento que sea necesario, se puedan agregar nuevos sitios remotos o ampliar los anchos de banda sin afectar la operación de la red misma.

"Latencia:" Ésta 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. La medición de la latencia se realiza considerando una trayectoria de ida y vuelta entre el punto origen y destino (round trip).

OPERBES, S.A. DE C.V. tomó en consideración que la latencia máxima aceptada de los enlaces será de: 100 ms para voz y datos.

La red y los equipos tendrán propuestos por OPERBES, S.A. DE C.V. la flexibilidad para soportar estándares tales como:

RFC2544 (Network Interconnect Devices)
RFC4364 (MPLS)
RFC2685 (RPV)
RFC2917 (CORE MPLS)
RFC3031 (MPLS Architecture)
RFC4182 (MPLS Label Stack Encoding)
RFC3036 Procesamiento del Tiempo de Vida (TTL)
RFC4762 (VPLS)
RFC3647 (Seguridad)

OPERBES, S.A. DE C.V. tomó en consideración que recibirá por parte de SHF la lista de los puertos TCP y UDP que emplean las aplicaciones bajo cada calidad de servicio, sirviendo esto como mecanismo para identificación del tipo de tráfico.

OPERBES, S.A. DE C.V. tomó en consideración que se entiende por nodo, al conjunto de los elementos que conforman la solución integral, que de manera enunciativa más no limitativa son: medios, ruteadores multiservicio, interfaces de voz, switches, firewalls de estado, IPS's, hasta el punto de demarcación definido y sobre el cual se determinará el nivel de disponibilidad; por lo que si alguno de los elementos que lo integran no ofrece el servicio solicitado, se considerará que dicho nodo no está disponible.

En los nodos donde SHF solicite un nivel de criticidad alta, OPERBES, S.A. DE C.V. proporcionará redundancia en medio, CPE y nodo, ésta será a través de centrales o puntos de presencia distintos, con diversidad de rutas y diversidad de medio. En el "Anexo VIII. Matriz de Servicios", se indican los nodos y el nivel de disponibilidad del servicio de cada uno y los domicilios que requieren de elementos adicionales como parte del nodo.

Para los nodos críticos OPERBES, S.A. DE C.V. tomó en consideración que operará con balanceo de cargas definido por SHF en ambos enlaces. En caso de falla conmutará automáticamente el tráfico al enlace que se encuentre operando correctamente. Dicho balanceo de cargas se realizará mediante técnicas de ruteo sin que sea necesario el considerar una solución o apliance de propósito dedicado. Para los nodos de criticidad media y estándar se considerará un solo enlace.

OPERBES, S.A. DE C.V. presenta carta o escrito en papel membretado expedido por el o los fabricantes, o representantes únicos en México de los elementos que conforman la solución propuesta, en la que manifiesta que los servicios solicitados estarán soportados durante la vigencia del contrato por expertos de cada fabricante o representante, manteniendo por ende un nivel de escalamiento directo con los fabricantes o representantes y sus respectivas áreas de desarrollo y soporte; así mismo que avalen que la solución propuesta por OPERBES, S.A. DE C.V. integra las últimas versiones en Software y Hardware liberadas por el fabricante y forma parte de los documentos obligatorios a presentar por OPERBES, S.A. DE C.V.. OPERBES, S.A. DE C.V. tomó en consideración que ésta carta no aplica para los elementos de infraestructura auxiliar.

OPERBES, S.A. DE C.V. integrará y configurará los QoS a través de la red RPV MPLS el tráfico de voz, datos y video requeridos por SHF. OPERBES, S.A. DE C.V. tomó en consideración que las rutas y configuraciones para llevar a cabo dicha integración sólo serán proporcionadas al Licitante. Lo anterior y que no generará un costo extra por ningún motivo para SHF.

OPERBES, S.A. DE C.V. tomó en consideración que SHF será la responsable de definir el tráfico a cursar de las aplicaciones entre cada uno de los nodos de la misma red mallada, ya que el intercambio del tráfico será determinado por listas de acceso.

OPERBES, S.A. DE C.V. tomó en consideración que en su proposición que el ancho de banda será suministrado en un esquema en demanda para los sitios indicados en el "Anexo VIII. Matriz de

Servicios", donde se especificarán los anchos de banda y los pisos que se deberán considerar para cada sitio.

Equipo Terminal del Enlace RPV

OPERBES, S.A. DE C.V. incluye para el CPE de la RPV-MPLS:

La infraestructura a instalar por parte de OPERBES, S.A. DE C.V. se ubicará en el lugar que indique SHF y estará debidamente etiquetada en un lugar visible para su identificación.

OPERBES, S.A. DE C.V. incluye equipo nuevo (OPERBES, S.A. DE C.V. tomó en consideración que no se aceptará equipo de reuso). Aplica tanto para la instalación inicial como para los servicios adicionales que se requieran durante la vigencia del contrato. OPERBES, S.A. DE C.V. tomó en consideración que el plazo máximo para solicitar servicios adicionales es hasta 6 meses antes de la finalización del contrato. OPERBES, S.A. DE C.V. tomó en consideración que solo para el caso de solicitudes de servicio en los últimos 6 meses antes de la finalización del contrato se podrá entregar con equipo de reuso cumpliendo con los niveles de servicio establecidos en el contrato.

OPERBES, S.A. DE C.V. tomó en consideración que con el fin de contar con una red homogénea, los CPE's serán de la misma marca y de las familias más recientes en el mercado.

Capacidad para poder actualizar el software del equipo de manera remota. Podrá guardar múltiples configuraciones en el ruteador.

Tendrá la última versión de sistema operativo estable ya comprobado por el fabricante del equipo.

OPERBES, S.A. DE C.V. realizará las actualizaciones para todo el equipamiento, conforme se liberen nuevas versiones, durante la vigencia del servicio, apegándose al proceso de control de cambios de SHF.

Los CPE's que se propuestos por OPERBES, S.A. DE C.V. contarán con las interfaces, capacidad de procesamiento y memoria necesarios para cursar el tráfico requerido en cada nodo. OPERBES, S.A. DE C.V. tomó en consideración que si el uso del procesador en los CPE´s se encuentra entre el 70% y el 85% promedio de su capacidad, durante 10 días hábiles consecutivos en el horario de operación de las 10:00 a las 19:00 horas, OPERBES, S.A. DE C.V. ampliará la capacidad de procesamiento y/o memoria del CPE, sin costo adicional para SHF, en un plazo no mayor a tres días hábiles.

OPERBES, S.A. DE C.V. tomó en consideración que si el uso del procesador en los CPE´s es mayor del 85% promedio de su capacidad, durante 3 días hábiles consecutivos de operación normal en el horario de las 10:00 a las 19:00 horas, OPERBES, S.A. DE C.V. reemplazará el CPE, por la siguiente categoría superior, en un plazo no mayor a tres días hábiles.

El CPE tendrá al menos 4 ranuras para módulos de interfaces de red y puerto de servicios para crecimientos de acuerdo a las necesidades de SHF.

Bestal consideró en el equipo ruteador, denominado como equipo CPE, al menos dos Puertos Ethernet 10/100/1000 Mbps necesarios para conectar los elementos solicitados por cada nodo, de estos, se considera al menos un puerto para la conexión con la LAN de cada sitio.

OPERBES, S.A. DE C.V. tomó en consideración que para los puertos LAN se requiere FastEthernet o Gigabit Ethernet 10/100/1000 Mbps de acuerdo con las necesidades de SHF.

Manejo de BGPv4, RIP1, RIP2, OSPF, IPv4, IGMPv1, IGMPv2, IGMPv3, IPv6 y SNMP v3.

Manejo de PIM (Protocol Independent Multicast), en sus variantes: PIM-DM (Dense Mode), PIM-SM (Sparse Mode) y PIM-SSM (Source SpecificMulticast)

Manejará el protocolo VRRP o similar.

Contará con la capacidad de redireccionar tráfico de red.

Soportará la encapsulación de tráfico IPv4 e IPv6 en IPv4 de acuerdo al protocolo RFC2784.

En cuanto a las calidades de servicio (QoS) OPERBES, S.A. DE C.V. tomó en consideración que se requiere manejo de funciones de etiquetado por tipo de aplicación basado en IP precedente y DiffServ, funciones para conformado y monitoreo de tráfico (policing), basándose en IP precedente y DiffServ, gestión de colas (WFQ, CBWFQ y colas de alta prioridad PQ), control y manejo de congestión (WRED), fragmentación e intercalación (interleaving).

Soporte de estándares de encripción 128-bit AES-GCM y 256-bit AES-GCM; y de Hashing SHA-256, SHA-384 y SHA-512.

Manejará un mecanismo que garantice los niveles de jitter y retraso requeridos por aplicaciones en tiempo real, voz y video en el encolamiento con prioridad de paquetes permitiendo asignar ancho de banda compartido dentro de un mismo enlace para otras aplicaciones o tipos de tráfico con base a la clasificación previamente realizada y ante situación de saturación del enlace.

El CPE tendrá la funcionalidad operativa para garantizar que el tráfico de voz, datos y video sea tratado bajo las condiciones de Calidad de Servicio (QoS).

Soportará módulos E1 G.703/ G.704 (Qsig y/o R2 Modificado) y E&M (recEive and retrasMit, por sus siglas en inglés), FXS/FXO, de acuerdo al requerimiento de SHF.

OPERBES, S.A. DE C.V. incluye en el Apartado Descripción de los Equipos en la presente proposición un listado de los equipos que integran su solución indicando la marca, el modelo y las características de cada uno de ellos.

OPERBES, S.A. DE C.V. tomó en consideración que tendrá la libertad de seleccionar la manera de conectar el equipo CPE a la nube MPLS de acuerdo al RFC4364 (MPLS), considerando el cumplimiento de los Niveles de Servicio solicitados.

OPERBES, S.A. DE C.V. permitirá la implementación de múltiples contextos o instancias independientes de tablas ruteo que coexistan en el mismo ruteador de manera simultánea. De tal manera que no puede haber conflictos de traslape de direccionamiento con direcciones duplicadas entre estas instancias de ruteo independientes.

Los equipos CPE permitirán incluir listas de control de acceso como parte de su funcionalidad, de tal manera que únicamente los usuarios indicados por SHF podrán acceder a las aplicaciones, datos y servicios de estas mismas.

Contará con la capacidad de especificar listas de acceso para detectar tráfico de acuerdo a los criterios establecidos que pueden ser:

Dirección fuente y/o destino MAC, IPv4 o IPv6

Protocolo

Puerto fuente y/o destino TCP/UDP

Mensaje ICMP

Valor de la precedencia del encabezado IP

Soportará el protocolo de control de acceso para restringir el acceso de dispositivos no autorizados a los puertos LAN del ruteador de acuerdo al estándar IEEE 802.1x.

Manejará mecanismos de AAA (Authentication, Accounting y Authorizing por sus siglas en inglés).

Interactuará con servicios RADIUS y TACACS+.

Los CPE contarán con la funcionalidad de realizar la traducción de direcciones de red (NAT: Network Address Translation y PAT: Port Address Translation, por sus siglas en inglés).

Soportarán los estándares 802.1p (QoS) y 802.1q (Dot1q) hacia la red LAN de SHF.

Proveerán el protocolo para evitar la creación de bucles o loops en puertos switcheados en redes Ethernet de área local de acuerdo a los estándares IEEE 802.1d, IEEE 802.1w y IEEE 802.1s.

Permitirán la configuración de políticas de calidad de servicio para flujos de tráfico dirigidos hacia el plano de control del equipo de ruteo IP para la protección contra ataques de negación de servicios (DoS) dirigidos hacia el equipo.

Soportarán el protocolo DHCP en forma de servidor y relay.

La administración será a través del protocolo SNMPv3 y capacidad para soportar RMON o superior.

Capacidad de bloqueo de tráfico por dirección IPv4 e IPv6.

Manejarán el protocolo SSH v2

Contarán con puerto de consola.

Soportarán la funcionalidad estándar de sincronización de fecha y hora de acuerdo con el RFC5905.

Para enlaces con un ancho de banda de hasta 8Mb tendrá una capacidad de al menos 353,000 paquetes por segundo (PPS).

Para enlaces con un ancho de banda mayor a 8Mb tendrá una capacidad de al menos 480,000 paquetes por segundo (PPS).

Serán capaces de entregar métricas a un sistema de gestión centralizado que permita el monitoreo, reporteo y generación de alarmas facilitando la resolución de problemas y el análisis de capacidad.

Contarán con la capacidad de ejecutar un proceso de monitoreo de forma independiente con el fin de no comprometer la funcionalidad primaria ni desempeño del router.

Proporcionará las siguientes métricas, que serán integradas y visualizadas al 100% en el sistema de monitoreo y "Análisis de Tráfico (4.2.1):

Cantidad de Tráfico.

Clasificación de Tráfico por Aplicación.

Tráfico por Conversación de cada Aplicación.

Creará clasificaciones de tráfico para reflejar Aplicaciones personalizadas de diversas maneras, como puertos, direcciones IP de servers o URL's en el caso de Aplicaciones WEB.

Permitirá clasificar el tráfico en las interfaces del router ya sea por su QoS o por grupos de subredes para poder identificar subdivisiones de los nodos que sea relevantes al análisis.

Obtendrá las métricas, reportes y alarmas solicitadas acerca del tráfico Total, y las que se han solicitado en el punto anterior.

Contará con la funcionalidad de analizar la señalización para descubrir los protocolos que la componen y anomalías en los mismos, a la vez analizar el RTP para entregar métricas de Jitter y Packet Loss, así como alarmas relativas al mismo de tal manera que sea factible descubrir eventualidades que puedan poner en riesgo la entrega de servicios de VoIP y Video.

La captura se iniciará por comando del usuario con privilegios para tal fin o al presentarse alguna condición de red, tal como una alarma que le sirva de señal de disparo.

OPERBES, S.A. DE C.V. entregará una carta membretada por parte del fabricante la cual deberá estar firmada por el representante legal, que indique que el equipamiento propuesto tiene representación y soporte en México.

En el apartado Descripción de los Equipos se detallan los equipos propuestos.

Descripción del Switch de LAN

El Switch con capacidades de capa 2 del modelo de OSI y que formara parte de los equipos propuestos por OPERBES, S.A. DE C.V. para la conectividad de los componentes que conformen el nodo requerido por SHF, contará al menos con las siguientes características:

Integrará en el mismo chasis las necesidades de densidad de puertos de tecnologías Gigabit Ethernet, Fast Ethernet y Ethernet. Administración de tráfico en la capa 2.

El equipo tendrá un performance de 128 Gbps y 32 mpps. Contará por lo menos con 128 MB memoria DRAM, 32 MB en Flash Memory para soportar todas las funcionalidades solicitadas.

Soporte de Puertos de red: 10/100 BASE-T

El equipo soportará módulos Gigabit Ethernet que permita combinar interfaces 1000BASE-SX, 1000BASE-LX sin restricción alguna. .

Capacidad para configurar mínimo de 255 VLANs pudiendo utilizar al menos, direcciones IP, puertos físicos y protocolos.

IPv4, IGMP v2, IGMP Snooping, DHCP Relay, Radius client, 802.1D, 802.1w, 802.1p, 802.1Q, 802.1s, 802.3ad, 802.1x, 802.3x. (IGMP v2 e IGMP Snooping se soportan pero no se incluyen en el equipamiento)

Manejo de mecanismos de calidad de servicio como Shaped Round Robin, Weighted Tail Drop, DSCP.

Manejo de limitación de tasas de transferencia basada en dirección IP fuente y destino, dirección MAC fuente y destino, información de UDP y TCP y la combinación de estos parámetros.

Manejo de cuatro colas de prioridad por puerto

Manejo de IGMPv3 y/o snooping

Manejo de LACP.

Será capaz de limitar el número de direcciones MAC por Puerto.

Manejo de mecanismos de seguridad por Puerto tales como 802.1x.

Manejo de DHCP snooping, inspección dinámica de ARP, bloqueo de puertos que reciban paquetes BDPU no autorizados,

Manejo de mecanismos que prevengan que un switch ajeno a la red se quiera convertir en el switch raíz de spanning tree.

Manejo de listas de control de acceso por puerto

Manejo de SSH v2 y HTTPS

El equipo será montable en rack de 19" y sin modificaciones al rack ni al equipo. incluirá accesorios para montarlos.

Soportará tramas Ethernet de al menos 9000 bytes (Jumbo Frames).

Soportará SNMP v1, v2 y v3

Replicación de tráfico de un puerto a otro, incluso cuando el otro puerto esté ubicado en un switch remoto

Autenticación RADIUS y TACACS+

En el apartado Descripción de los Equipos se detallan los equipos propuestos.

Direccionamiento IP en la RPV-MPLS

OPERBES, S.A. DE C.V. tomó en consideración que tendrá la libertad de proponer la arquitectura, direccionamiento y el enrutamiento de la Red MPLS, considerando en todo momento el direccionamiento existente en las redes LAN de SHF con el fin de evitar conflictos por duplicidad de direccionamiento IP.

OPERBES, S.A. DE C.V. tomó en consideración a que será responsable del diseño del plan de direccionamiento IP de la Red Privada Virtual MPLS de acuerdo al RFC4364 respetando el direccionamiento LAN de SHF.

OPERBES, S.A. DE C.V. tomó en consideración a que existe la necesidad de interconexión entre RPV's MPLS de SHF, así como de terceros que tengan contratado el servicio red MPLS con OPERBES, S.A. DE C.V., para el acceso a aplicaciones de voz, datos y video sobre IP; por lo que la red de OPERBES, S.A. DE C.V. soportará la declaración de diferentes identificadores de red para controlar y aislar el tráfico de los diferentes nodos por lo que soportará el manejo de al menos un RPV-MPLS_ID para SHF.

En los casos que así se requiera y para evitar duplicidad en el direccionamiento, OPERBES, S.A. DE C.V. implementará un mecanismo de traducción de direcciones NAT.

El servicio de RPV-MPLS establecerá los mecanismos de control necesarios, para garantizar la asignación y uso de los recursos de comunicaciones para los servicios de SHF. Entre otras cosas, se evitarán las colisiones de direccionamiento y se garantizará el uso adecuado del ancho de banda destinado a un servicio.

OPERBES, S.A. DE C.V. tomó en consideración que el direccionamiento actual será proporcionado al ganador, el cual definirá si éste se conserva o se realiza un nuevo direccionamiento IP, en cuyo caso presentará su proposición a SHF para su revisión y en su caso, aprobación. En éste punto OPERBES, S.A. DE C.V. tomó en consideración que deberá interactuar con el Licitante de servicios de la RPV-MPLS actual, con la finalidad de homologar el direccionamiento IP.

OPERBES, S.A. DE C.V. tomó en consideración que para conocimiento y aprobación de SHF, el plan de direccionamiento será documentado y entregado previo a la puesta en operación de los servicios.

OPERBES, S.A. DE C.V., observará en todo momento los procesos y mecanismos para la liberación de la comunicación entre nodos de SHF, acordados durante la planeación de la implantación, de tal forma que se garantice la seguridad de manera individual para SHF.

Acceso Remoto RPV

OPERBES, S.A. DE C.V. incluye en la presente proposición clientes de acceso remoto a través de túneles de RPV, utilizando como medio a la red pública Internet, el cual cumple al menos con lo siguiente:

OPERBES, S.A. DE C.V. proporcionará las licencias y equipamiento necesario para soportar la cantidad de usuarios indicada por cada dependencia a través de VPDN (RPV sobre Internet) de forma simultánea.

La conectividad garantizará el acceso seguro y cifrado soportando IPSEC, DES y 3DES.

Proporcionará seguridad en el nodo de la RPV para el acceso a los clientes, mínimo hasta la capa 3 del modelo OSI, de la capa 4 a la 7 será responsabilidad de SHF, a través de la infraestructura de seguridad con la que cuenta.

OPERBES, S.A. DE C.V. tomó en consideración que el equipo central soportará a futuro la autentificación de las cuentas a través de un sistema Radius, Tacacs, Kerberos, o cualquier otro compatible con las funcionalidades requeridas, soporte para la emisión de certificados públicos y privados para la conexión.

OPERBES, S.A. DE C.V. tomó en consideración que SHF tendrá la capacidad de realizar la configuración de diferentes perfiles y direcciones IP destino.

La solución Contará con un control centralizado (administración en forma centralizada), OPERBES, S.A. DE C.V. proporcionará dicha herramienta para que a través de ésta, SHF realice dichas actividades de administración centralizada.

Soporte a futuro de conexiones RPV a través del protocolo SSL

SHF podrá realizar:

Cambios en los perfiles de usuarios.

Cambios en los privilegios y seguridad interna.

Bajas y altas de usuarios.

Monitoreo en línea de usuarios.

Definición de políticas de seguridad interna.

Instalación del cliente IPSEC en las computadoras remotas.

Soportará el transporte y la aplicación de la telefonía IP.

Soportará telefonía sobre IP.

En los clientes RPV (cliente de la aplicación de VPDN), se considera lo siguiente:

Se requiere de un software RPV cliente.

El cliente de RPV soportará plataformas a 32 bits y 64 bits para Windows XP y superiores, MAC OS10 y superiores, Android 2.2 y superior; IOS 4.5 y superior.

Contar con la última versión liberada por el fabricante.

Contar con los fixes del software liberados por el fabricante y probados por OPERBES, S.A. DE C.V. para su instalación en caso de vulnerabilidades.

Para cada Firewall solicitado por SHF, indicará el número de clientes VPDN que requiera.

Interfaz GUI.

Enlace LAN-to-LAN

OPERBES, S.A. DE C.V. proveerá, instalará y pondrá en operación a SHF, una solución basada en enlaces dedicados punto a punto, La cual cumplirá al menos con las siguientes características:

Modo Wire

Enlace Síncrono

Deberá entregarse en interfaz Ethernet (IEEE 802.3) con conectores RJ45 en cada una de sus puntas, siendo estos el punto de demarcación del servicio

Incluirá todo aquello que sea necesario para cumplir con el servicio con las características solicitadas hasta el punto de demarcación mencionado.

Manejará granularidad desde 5Mbps.

Con base inicial de 20 Mbps hasta un 1Gb

Realizará el transporte a nivel capa 2 del modelo OSI, es decir manteniendo el direccionamiento IP (extensión de la misma LAN de SHF)

Podrá transportar diferentes VLANs con encapsulación dot1q (IEEE 802.1Q) y transportar todo el tráfico de broadcast, unicast y multicast entre los dos extremos del enlace.

Garantizará el ancho de banda siendo simétrico y bidireccional

Comunicación Full-Duplex llevada a cabo para desactivar la detección de colisiones y funciones de loopback

Proveerá el servicio vía pago por uso bajo demanda.

Contará con una herramienta de monitoreo y medición de uso

Cumplirá con una disponibilidad de 99.90% (Criticidad Media) y latencia de 10 ms. y 99.98% (Criticidad Alta) de acuerdo a las necesidades de SHF, el cobro del esquema bajo demanda será calculado por medio de la regla de percentil 95.

La descripción del servicio propuesto se presenta en el Apartado Enlace Lan to Lan.

Servicio de Videoconferencia

OPERBES, S.A. DE C.V. tomó en consideración que como parte de la solución de la red de voz, datos y video SHF, podrá requerir el servicio de video conferencia. OPERBES, S.A. DE C.V. propone dos tipos de servicio, de Sala y de Escritorio, además se considera la posibilidad de realizar video conferencias punto multipunto con sesiones simultáneas de hasta el total de servicios de video conferencia (de sala o escritorio) para SHF.

El sistema de Videoconferencia ofertado será 100% compatible con sistemas de video conferencia basados en el protocolo IP.

Las características mínimas de los componentes de la solución propuesta se describen a continuación de manera enunciativa más no limitativa:

Establecimiento de llamadas

Todas las llamadas serán establecidas mediante los estándares H.323 y SIP. Para ello el sistema permitirá su registro en Gatekeepers H.323 y en SIP registrar.

El equipo contará con el mecanismo para que el usuario pueda iniciar y terminar las llamadas. Independiente del dispositivo de control propuesto que sea incluido en la solución presentada por OPERBES, S.A. DE C.V., éste permitirá:

Marcación a salas remotas mediante los siguientes mecanismos:

Directorio local

Directorio corporativo o global operado centralizadamente

Marcación a equipos que no se encuentren en ninguno de los directorios antes mencionados. Esta marcación será por alias E.164, H.323ID, dirección IP y URI .

Historial de llamadas hechas, recibidas

Envío de tonos DTMF

Llamadas Hold

Agregar participantes a la sesión, retener varias llamadas y transferirlas a la MCU central, función similar a la realización de una conferencia telefónica

Terminar la sesión

Seleccionar la transmisión de contenido, estará disponible en llamadas H.323 y SIP.

Ajuste de audio (subir/bajar), apagar micrófonos locales (Mute)

Control de cámara remota

Permitirá mostrar imagen local, remota y contenido en la misma pantalla

Operará con Firewall/NAT SIP Transversal H.460.18 y H.460.19 obligatorio ya que estos estándares son los que hacen referencia a la facilidad de cruce de Firewalls. OPERBES, S.A. DE C.V. tomó en consideración que será motivo de descalificación el solo soportar H.460.

Calidad de Video

El sistema propuesto permitirá el establecimiento de sesiones a diferentes velocidades y diferentes calidades de video.

Al establecer sesiones con otras salas operará con las siguientes resoluciones:

CIF, SIF

WCIF

4CIF, 4SIF

W4CIF o W576P

XGA

WSXGA 720p / 30fps

720p / 60fps

1080p / 30fps

Contará con mecanismos que permitan reducir el ancho de banda para el establecimiento de sesiones de al menos720p y 1080p. Esta función será compatible con la base instalada y equipos de otras marcas.

Permitirá establecer sesiones a velocidades de al menos 384 kbps.

Calidad de video a transmitir como contenido (segundo stream de video), soportará el protocolo H.239 para H.323 y BFCP para SIP.

La solución propuesta permitirá la transmisión de una segunda fuente de video al mismo tiempo que la cámara principal. Este segundo stream operará con resoluciones hasta 1080p y con un mínimo de 15 fps. soportará el protocolo H.239. Con un mecanismo similar en SIP para permitir compartir la transmisión de una segunda fuente de video.

Esta operará tanto en H.323 (H.239) como en SIP (Binary Floor Control Protocol, Protocolo de Control de Piso Binario BFCP, RFC4582).

Calidad de Audio

El sistema propuesto permitirá el establecimiento de sesiones empleando diferentes estándares de audio, como mínimo contará con:

G.711

G.722.1

Audio de al menos 20 kHz estéreo o superior

Seguridad de Llamadas

El sistema propuesto establecerá sesiones cifradas bajo el estándar H.235 v3. Estará disponible en llamadas H.323 y SIP.

Administración Remota

El sistema se operará mediante HTTPS. También operará con SNMP v3.

Características del CODEC

Establecer sesiones a velocidades de al menos 384 kbps.

Estándares de compresión de video: H.263++ o H.263 y H.263+

Estándares de compresión de audio: G.711, G.722.1 y audio de al menos 20 kHz o superior.

Firewall Transversal: H.460.18 y H.460.19. Contar, de acuerdo al mismo estándar soportará multiplexaje de puertos para operar con 5 puertos IP o menos sin importar el número de llamadas.

Encripción: de al menos AES 128 bits

Dual Stream: H.239 y BFCP

Al menos dos salidas de video HDMI. y una salida de alta definición DVI

Entradas de video: DVI-I para señal de PC, incluir cable terminado en conector VGA

Entrada para micrófonos de mesa

Entrada de audio adicional asociada a la entrada de PC

Para operar con 120 VCA a 60 Hz de suministro eléctrico.

Incluirá todo lo necesario para operar en modalidad multisesión (multipunto).

Facilidades en IP
Manejo de dirección IP fija o por DHCP
Soportará IPV4 e IPV6
Manejo de Calidad de Servicio QoS
Soporte DNS para configuración de servicios
Marcación URI por DNS
Gatekeeper automático y manual
Autenticación en Gatekeeper de acuerdo al estándar H.235
Soporte automático para NAT
Manejo de puertos dinámicos y fijos
Autenticación de red de acuerdo al estándar 802.1x
Manejo de VLAN 802.1q
Soportará para H.460.18 y .19 (Firewall Transversal)
Soporte de fecha y hora mediante NTP
Multipunto Interno

La solución propuesta contará con la opción de agregar o activar facilidad multipunto interna. Esta facilidad cumplirá con las siguientes características:

Operar con H.323 y SIP en la misma sesión

Permitir conectar a un mínimo de 3 sitios remotos de videoconferencia más 1 participante de audioconferencia adicionales al anfitrión

Operar con resoluciones de hasta 720p con 30 cuadros por segundo (fps).

Transcoding individual, cada sitio puede operar con su propia resolución de video y velocidad.

Soportar H.239 y BFCP

Actualización de Software Remota

El sistema contará con la capacidad de recibir actualizaciones de nuevas versiones de software a través de su puerto de red vía Internet/Intranet.

Características Generales del Equipo de Sala

El sistema de videoconferencia propuesto en cada localidad indicada en el "Anexo VIII. Matriz de Servicios", constará de un CODEC (no basado en PC), una cámara, un control remoto inalámbrico, dos monitores para la visualización del video y contenido transmitido, dos micrófonos digitales y un componente para transmitir el contenido de una PC en tiempo real.

El códec, cámara y los dos monitores requeridos, serán instalados en una base de 80 cm de altura al borde inferior de la pantalla, de material y dimensiones suficientes para dar soporte a dichos componentes. La base será auto soportado, sin soportes a pared o techo y la cámara estará posicionada en la parte superior de los monitores, tendrá ruedas para su movilidad con bloqueo.

Características generales del CODEC

Soporte de los estándares H.323, SIP, G.722 y H.239.

Soporte de video de alta definición de 720p y 1080p con 30 cuadros por segundo.

Soporte para la transmisión del contenido enviado desde una PC en tiempo real con una resolución XGA (1024x768)

Conexión a redes Ethernet a través de un puerto UTP de 10/100 Mbps.

El CODEC contará al menos con dos entradas para recibir las señales de audio, video, micrófonos, red y transmisión de contenido requeridos.

Soporte para operar con dos monitores, en donde en el primero se mostrará el video remoto y en el segundo el video local o el contenido enviado o recibido. Por lo que las salidas y entradas de video deberán ser en interfaz HDMI

Características de la Cámara

Cámara PTZ (Pan-Tilt-Zoom), con un campo visual de al menos 50°, con 180° de panorámica, zoom óptico de al menos 10x y movimiento vertical total de 40° o mayor; con movimiento de la cámara y zoom controlado vía inalámbrica a través del control remoto del sistema; memoria para predeterminar 5 posiciones al menos; con operación automática del foco, luminosidad y contraste.

La cámara operará con resoluciones hasta 1080p, 30fps. Contar con interfaz estándar para entregar el video hacia el CODEC u otros dispositivos de video.

Características Generales de los Monitores

Se integrará a la solución dos monitores a color de panel plano (flat panel) de al menos tecnología LED (light-emitting diode, diodo emisor de luz), de alta definición 1080p o superior, de al menos 42", con sintonizador integrado de HD (High Definition), relación de aspecto 16:9, ángulo de

visibilidad de al menos 160 grados, compatible con los formatos de video y entradas de audio y video del codec solicitado.

Bocinas con una potencia de audio de al menos 5W RMSx2.

Tres entradas HDMI

Características de los Micrófonos

Dos micrófonos digitales con cobertura de 360° para mesa, de tipo alámbrico, con capacidad de transmitir señales de audio de hasta 20 KHz, compatible con la calidad de audio y conectores del sistema de videoconferencia, con cancelación de eco automática, supresión de ruido, control de ganancia automática activada por voz, con capacidad de enmudecimiento (mute) manual.

Equipo para Transmisión de Contenido

Dispositivo para la transmisión del contenido mostrado en el monitor de una computadora personal (no ofertada por el prestador del servicio) a todos los participantes de la videoconferencia para su despliegue en sus respectivos monitores de visualización de contenido. La resolución de la imagen transmitida será al menos de tipo XGA (1024x768p). El servicio incluirá los cables requeridos para su conexión con la PC y con el sistema de videoconferencia.

Características del Control Remoto

Control remoto para el acceso a todas las funciones para cada uno de los componentes del sistema.

Características Generales del Equipo de Escritorio.

El sistema incluirá en un solo chasis: cámara, codec, pantallas, micrófono y dos bocinas.

Comunicación punto a punto con otras equipos del mismo tipo

Comunicación multipunto con otros sistemas, empleando MCU externa

Comunicación multipunto empleando MCU interna

Comunicación con sistemas de videoconferencia H.323 y SIP

Establecer sesiones de videoconferencia y telefonía.

Entrada y salida de audio para diadema

La solución presentada incluirá como mínimo los siguientes componentes o funcionalidades:

1 Cámara HD con resolución 1080p / 30 fps integrada a la pantalla.

1 Codec con soporte de resoluciones hasta 1080p y 30fps integrado a la pantalla. (OPERBES, S.A. DE C.V. tomó en consideración que no se aceptará un codec separado de la pantalla dado que los equipos estarán en movimiento entre sedes y no habrá especialistas técnicos dedicados para la conexión de los mismos)

Auricular para privacidad

Micrófono y altavoces integrados a la pantalla para operar en manos libres

La pantalla soportará resoluciones de hasta 1080p, ser de un tamaño al menos de 24 pulgadas diagonales.

Seguridad

Autenticación de contraseña segura.

Contraseña de Administrador.

Contraseña cifrada para acceso por interface Web.

Función de no molestar.

Capacidad de inhabilitar servicios como FTP, Telnet, HTTP.

Respuesta automática punto a punto (On/Off).

MCU Hosteado

El equipo MCU propuesto se ubicará en las instalaciones OPERBES, S.A. DE C.V., incluirá un enlace dedicado hacia la VPN-MPLS del Sector, el hardware y software necesario para operar sesiones de videoconferencia bajo los estándares H.323 y SIP, con salida a internet para establecer videoconferencias externas, transmitiendo una imagen de alta definición de 720p a 30fps, con un ancho de banda de al menos 384 kbps y audio de 20 KHz de respuesta en frecuencia, con capacidad de soportar usuarios a diferente velocidad o resolución (transcoding), que opere bajo el estándar de video H.264.

Las reuniones multipunto que se llevarán a cabo se realizarán tanto por activación de voz (video switching), en donde siempre se observa en pantalla a la localidad que hace uso de la palabra, por recuadros (presencia continua), en donde los participantes observan al participante activo y a los participantes más recientes de la sesión.

El equipo MCU contará con la capacidad de programar videoconferencias futuras mediante reservaciones, con códigos de acceso independientes para recibir las llamadas de los usuarios que requieran de su conexión, tendrá la capacidad de transmitir el contenido que se genere en tiempo real en una PC del lado cliente (endpoint) a todos los participantes de la sesión de videoconferencia vía el

protocolo H.239 y SIP. Con capacidad de conexión a redes Ethernet a través de un puerto UTP de 10/100/1000 Mbps

OPERBES, S.A. DE C.V. proporcionará acceso a la administración del MCU vía página web, vía red desde un equipo de cómputo de SHF con conexión a la red VPN-MPLS, a fin de que personal de SHF pueda monitorear las sesiones de videoconferencia en un horario de 7x24 horas, los 365 días del año. El software de administración contará con las siguientes funcionalidades:

Soporte para la creación de diferentes perfiles de usuario protegidos con nombre de acceso y su respectiva clave, que permita crear y administrar las videoconferencias, así como la administración completa de las funcionalidades del equipo.

Permitir a un operador crear reservaciones para la videoconferencia, monitorear en línea el estado de los participantes activos en una conferencia y poder mover a los participantes entre videoconferencias.

Diagnóstico de funcionamiento del MCU y del rendimiento en línea.

Consulta de alarmas y archivos de reporte de fallas.

Visualización de reportes de utilización y duración de las videoconferencias.

Compatibilidad con Windows 7 a 32 y 64 bits, y superiores.

Cumplirá con una disponibilidad de 99.93% (Criticidad Media).

En el Apartado Videoconferencia se detallan los equipos y solución propuesta.

Administración de Tráfico y Optimización de Aplicaciones.

OPERBES, S.A. DE C.V. tomó en consideración que con el fin de administrar el tráfico y optimizar el desempeño de las aplicaciones críticas de SHF, se requiere una solución, que permita un rendimiento superior en la utilización del ancho de banda mediante técnicas de compresión, donde se reconozcan los cambios o modificaciones que sufran por el uso de las aplicaciones, enviando solamente el incremental de la nueva información, al tiempo que también tendrá que permitir mejorar el tiempo de respuesta de las mismas; mitigando los efectos de la latencia sobre las diferentes aplicaciones, aplicando dichas técnicas incluso hasta la capa de aplicación del modelo OSI.

Esta será una solución solicitada por SHF en el momento que sea requerida, con las siguientes características mínimas:

Para una mayor eficiencia, la solución trabajará en modalidad simétrica. Entiéndase por tal, que las técnicas de optimización se aplicarán mediante dispositivos a ambos extremos del enlace WAN que se pretende optimizar.

Detectará de manera automática si los paquetes viajan por diferentes trayectorias físicas sin que afecte el proceso de aceleración.

El servicio soportará la optimización y aceleración del tráfico de SHF, sin necesidad de pasar por un sitio central para que el tráfico sea optimizado, haciendo uso de los beneficios de una red MPLS como la RPV.

Será brindada mediante dispositivos independientes y específicos; y OPERBES, S.A. DE C.V. tomó en consideración que no se aceptarán en esta instancia módulos agregables a los equipos existentes, así como tampoco soluciones de software instaladas en servidores multipropósito.

OPERBES, S.A. DE C.V. tomó en consideración que el servicio no manipulará la información vital de los paquetes, la razón de esto es que se pueda hacer uso transparente de muchas funcionalidades tales como QoS, ACLs, redundancia de router y enlace, etc. Brindará niveles de desempeño y disponibilidad alta. En caso de configuraciones de alta disponibilidad, los equipos involucrados sincronizarán sus datos automáticamente.

OPERBES, S.A. DE C.V. tomó en consideración que La aceleración del desempeño de aplicaciones en los enlaces WAN se considerará de acuerdo a las capacidades de los mismos.

OPERBES, S.A. DE C.V. tomó en consideración que si el desempeño del dispositivo (utilizando como métricas de desempeño CPU y Memoria) se encuentra entre el 70% y el 85% promedio de su capacidad, durante 10 días hábiles consecutivos en el horario de operación de las 10:00 a las 19:00 horas, OPERBES, S.A. DE C.V. ampliará la capacidad de procesamiento y/o memoria del equipo, sin costo adicional para SHF, en un plazo no mayor a tres días hábiles. Aplica únicamente para el desempeño del equipo asociado al servicio.

OPERBES, S.A. DE C.V. tomó en consideración que si el desempeño del dispositivo es mayor del 85% promedio de su capacidad durante 3 días hábiles consecutivos de operación normal, OPERBES, S.A. DE C.V. deberá remplazar el equipo, por la siguiente categoría, en un plazo no mayor a tres días hábiles.

Podrá auto descubrir los equipos para poder establecer una conexión optimizada sin la necesidad de establecer un túnel estático y ser capaz de establecer una malla dinámica entre las diferentes oficinas si se establece una conexión TCP entre ellas.

El tráfico enviado por la solución hacia la WAN cumplirá con el estándar RFC2581 de principios de congestión para TCP. La configuración inicial del equipo soportará el comienzo lento de TCP y manejar la congestión a razón de interactuar amigablemente con el tráfico pre-existente compartiendo la WAN.

La solución será transparente para los servidores de procesamiento y almacenamiento, así como también para los usuarios finales. Por ningún motivo modificar el enrutamiento normal de los paquetes o utilizar técnicas de túneles.

La solución propuesta permitirá especificar las técnicas de aceleración mediante políticas por host, subred y/o puerto TCP.

Para la evaluación de los equipos propuestos, OPERBES, S.A. DE C.V. comprobará los requerimientos técnicos específicos con los catálogos, manuales del hardware y software.

La solución propuesta deberá poder funcionar en modo físicamente en línea (Ethernet Bridge) o a través de redireccionamiento de tráfico como técnicas de WCCP o PBR.

La comunicación optimizada sobre la WAN (la comunicación entre los equipos optimizadores) mantendrá una conexión TCP optimizada independiente por cada uno de los clientes reales (esquema Proxy TCP).

La solución propuesta se integrará de manera transparente dentro de la infraestructura de ruteo IP existente. La solución será completamente transparente para los protocolos de ruteo existentes (Ej. OSPF, RIP, BGP, etc.). Todas las funciones de ruteo incluyendo "selección dinámica del camino" o cualquier otra decisión de ruteo permanecerá como responsabilidad del equipo que viene realizando dicha tarea ("router")

La solución propuesta soportará operar en VLAN (IEEE 802.1q) en las interfaces de intercepción.

La solución propuesta permitirá el curso normal del tráfico ante una falla que lo deje fuera de servicio y/o apagado del mismo sin necesidad de intervención por parte de los operadores (modo bypass). La solución propuesta permitirá al operador, conmutar manualmente al modo bypass.

Cuando sea superada la capacidad máxima de conexiones optimizadas, la solución propuesta continuará cursando tráfico sin optimizar a través del mismo de manera no optimizada.

La solución preservará los valores pre-existentes en el campo de QoS TOS/Diffserv al momento de enviar tráfico a través de la red WAN.

La solución propuesta contará con dos capas de optimización de Ancho de Banda: basada en diccionarios de patrones repetitivos y compresión de tráfico.

Basada en diccionarios de patrones repetitivos:

La solución propuesta permitirá el almacenamiento único en su disco duro y no deberá reducir su capacidad de almacenamiento a consecuencia de divisiones lógicas por la interconexión de los otros sitios donde existan optimizadores. En el disco duro se almacenarán los patrones de tráfico repetitivos de manera tal que puedan ser servidos localmente sin necesidad de que dicho tráfico curse por la red WAN cada vez que un usuario quiera accederlo. El diccionario de datos repetitivos se realizará en un disco rígido propio del dispositivo y persistirá en caso de reinicio del sistema o bien en casos de desconexión.

Los patrones de datos repetitivos se reconocerán a nivel de segmentos parciales de bytes, y reutilizarse para poder enviar las referencias por la WAN en lugar de la información completa. No se admitirán soluciones que solo permitan el caching a nivel de objetos completos y no por segmentos.

El algoritmo de de-duplicación basado en diccionarios funcionará de manera bi-direccional para garantizar la máxima eficiencia de ahorro de ancho de banda por transferencias sucesivas.

Los patrones de datos almacenados serán guardados en un repositorio universal de referencias que permita, independientemente de la aplicación, maximizar la eficiencia de almacenamiento en el disco duro. Esto se refiere por ejemplo: si un usuario baja un archivo por carpetas compartidas y posteriormente se envió por correo; el sistema universal de referencias guardará una copia del archivo a nivel de referencias que sea independiente a la aplicación.

El equipo censará de manera dinámica si el hecho de almacenar los segmentos ocasiona presión de escritura al disco duro a razón de realizar la de-duplicación a nivel de memoria y reducir la compresión de manera dinámica a razón de garantizar la mayor velocidad de segmentos antes de la optimización.

La solución propuesta tendrá la capacidad de cifrar la información optimizada entre los equipos a través de SSL o IPSec con los algoritmos 3DES, AES con Key Lenght de (128, 196, 256) bits.

Compresión de Trafico: Para todo tráfico optimizado la solución permitirá aplicar un algoritmo de compresión antes de cursar la información por la WAN. Este algoritmo después aplicará la técnica de de-duplicación basada en diccionarios.

Preservará el esquema de seguridad de Microsoft para el uso de SMB de acuerdo al sistema operativo, esto es NTLM para Windows 2003, XP o Vista y Kerberos para Windows 7.

En la optimización de Outlook permitirá la optimización de RPC sobre SSL de manera automática.

Cuando se realice una consulta a través de HTTP de un video bajo demanda de contenido generado a través de Microsoft Silverlight o adobe flash, el equipo será capaz de entregar el contenido a múltiples computadoras; donde para optimizar este tráfico sobre la WAN, solo se tendrá una sola sesión de video y no una relación 1 a 1 de sesiones por cada usuario que este revisando el video.

El equipo propuesto será capaz de poder realizar Calidad de Servicio de entrada o salida tráfico que permita una inspección de paquetes a nivel aplicativo (Deep Packet Inspection por sus siglas en inglés), en caso de que se requiera.

La solución será capaz de definir clases por tráfico de aplicación y aplicar calidad de servicio de acuerdo a políticas para cada clase.

La solución permitirá definir un mínimo de ancho a utilizar a cada una de las clases de las aplicaciones.

La solución será capaz de definir una máximo ancho de banda a ser utilizado por cada clase de tráfico y ser capaz de utilizarlo si ninguna de las otras clases lo está utilizando para maximizar la utilización del ancho de banda.

La solución será capaz de priorizar el encolamiento con el objetivo de poder priorizar flujo de paquetes para cada uno de las clases de tráfico de manera independiente.

La solución será capaz de aplicar políticas de calidad de servicios para todo el tráfico

La solución propuesta soportará un modelo jerárquico de calidad de servicio; capaz de alojar el ancho de banda aplicado no solamente para el ancho de banda local, sino capaz de administrar el ancho de banda para cada sitio remoto.

El acceso a los equipos propuestos de la solución para la conexión de administración será mediante protocolo HTTPS y SSH.

Tendrá soporte para integración en redes que utilicen un direccionamiento IPV6.

La solución propuesta podrá ofrecer los siguientes reportes al menos:

Optimización de ancho de banda (tráfico bidireccional, recibido en LAN y enviado a WAN y viceversa).

Coincidencia de datos recibidos contra datos referenciados en disco duro.

Ganancia de capacidades de red.

Reducción de datos en porcentaje y pico.

Reducción HTTP.

Reportes de reducción de NFS.

Estadísticas de reducción de tráfico SSL.

Tasas de transferencia de datos.

Resumen de reducción del tráfico por protocolos.

Conexiones actuales y del estado de las mismas.

Modelaje de QoS de clases especificadas.

Paquetes descartados debido al modelaje de QoS.

Histórico de conexiones.

Bitácora de conexiones TCP que han trasmitido más información, identificando las direcciones IP fuente y destino, así como el puerto de aplicación.

Sesiones TCP actuales e histórico de las 50 conexiones que han enviado más tráfico.

Los equipos de la solución propuesta, tendrán la capacidad de enviar de alertas sobre el estado del equipo vía traps SNMP; así como, Log de eventos y alertas del servicio consultables vía web.

Los logs serán capturados de manera individual hasta un periodo de 30 días.

Los equipos se podrán administrar a través de SNMP versión 3 a razón de poder establecer diferentes perfiles de administración para una seguridad.

Los equipos serán capaces de poder exportar información de sus conexiones a través de NetFlow V5 y/o Netflow V9 a un colector externo.

Para salvaguardar la inversiones realizadas, se comprobará que la solución propuesta es totalmente compatible con un agente de software para instalarse en laptops o PC's con sistema operativo XP, Vista, Windows 7 o MAC OS.

Los equipos de la solución propuesta tendrán su propia consola de administración y en serán capaces de ser administrados a través de la misma.

La solución propuesta será 100% administrada y se integrará de manera transparente a la solución de red RPV MPLS dentro de un mismo equipo.

Aceleración del desempeño de aplicaciones en enlaces WAN con equipos que soporten lo establecido por nodo según el "Anexo VIII. Matriz de Servicios".

La herramienta generará al menos los siguientes reportes:

Optimización de ancho de banda (tráfico bidireccional, LAN a WAN y viceversa).

Coincidencia de datos recibidos contra datos referenciados en disco duro.

Ganancia de capacidades de red.

Reportes de reducción de datos en porcentaje y pico.

Reportes de reducción HTTP.

Reportes de reducción de NFS.

Estadísticas de reducción de tráfico SSL.

Reportes de tasas de transferencia de datos.

Resumen de reducción del tráfico por protocolos.

Reportes de conexiones actuales y del estado de las mismas.

Histórico de conexiones.

Todos los reportes serán configurables en vistas de últimos minuto, cinco minutos, hora, día y rango de tiempo.

Envío de alertas sobre el estado del equipo vía traps SNMP.

Log de eventos y alertas del servicio consultables vía web.

En el Apartado Administración de Tráfico y Optimización de Aplicaciones se describe la solución propuesta

Continuidad de la Operación de los Servicios de la RPV-MPLS

Será responsabilidad de OPERBES, S.A. DE C.V., asegurar la continuidad en la operación de la RPV-MPLS y demás Servicios solicitados, esto es que todos los servicios se encuentren disponibles en todo momento, conforme a los niveles de servicio requeridos.

OPERBES, S.A. DE C.V. solucionará las contingencias que se presenten durante la vigencia del contrato, con el objeto de mantener en operación la RPV-MPLS. Para tal efecto, entregará a SHF previo a la puesta en operación de los servicios, los procedimientos de respuesta que incluyan la matriz de escalamiento, que se implementarán en caso de una contingencia.

OPERBES, S.A. DE C.V. diseñará, implementará y verificará los planes de continuidad de la operación de la RPV-MPLS y servicios asociados, así mismo realizará la prueba de los mismos en común acuerdo con SHF, con el fin de verificar los planes de continuidad y mantenerlos actualizados.

El plan de continuidad de operación de los servicios, considerará los siguientes rubros:

Análisis de los Riesgos en la infraestructura de la RPV-MPLS, estrategias de continuidad de la operación de la RPV-MPLS en caso de contingencia, Manejo del plan, Operación en modo de contingencia, Retorno a la operación normal.

Este plan de continuidad de operación de los servicios lo entrega OPERBES, S.A. DE C.V. en el Apartado Continuidad de la Operación.

Para efectos de elaboración y validación de los planes, OPERBES, S.A. DE C.V. considera al menos los siguientes escenarios:

Caída del Servicio del NOC.

Caída del servicio en una Central (afectación de múltiples nodos de SHF asociados a una misma central).

Caída de Medio de Transmisión en un nodo.

Caída de algún elemento del nodo.

Caída de los principales nodos definidos por SHF.

La validación de los planes se realizará en común acuerdo con SHF, a efecto no de interrumpir su operación.

Para cada escenario, el plan incluirá las acciones que OPERBES, S.A. DE C.V. realizará en caso de presentarse alguno de los escenarios.

Estrategia de Continuidad de la Operación RPV

OPERBES, S.A. DE C.V. elaborará la estrategia de continuidad de operación la cual será validada por SHF, así como los procedimientos de operación de la RPV-MPLS, con los cuales garantizarán técnicamente la continuidad de los servicios.

Adicionalmente, los procedimientos contendrán la siguiente información:

Estrategia de recuperación y continuidad basada en MAAGTIC-SI vigente o en su caso el que lo sustituya en la operación de los servicios de la RPV-MPLS.

Matriz de escalamiento para la declaración de la operación en modo de contingencia de los servicios de la RPV-MPLS.

Personal involucrado y descripción de su rol por parte de SHF, así como de OPERBES, S.A. DE C.V. en el proceso de operación en contingencia y retorno a la operación normal de los servicios afectados de la RPV-MPLS.

Proveedores involucrados en el proceso, para dar continuidad a los servicios de la RPV-MPLS con los principales datos para su localización.

La estrategia de continuidad de operación se mantendrá actualizada durante la vigencia del contrato.

Servicio de Acceso a Internet

Descripción del Servicio.

Se requiere acceso al servicio de red de redes denominado internet con servicios de seguridad y niveles de servicio a SHF.

Características Técnicas del Servicio de Acceso a Internet.

OPERBES, S.A. DE C.V. Proporcionará el servicio de acceso a Internet en los nodos identificados en el "Anexo VIII. Matriz de Servicios", en donde se detallan las características del servicio para cada uno de los nodos.

El servicio de acceso a Internet se proporcionará conforme a los niveles de servicio establecidos en el presente documento.

OPERBES, S.A. DE C.V. considera en su proposición que el ancho de banda será suministrado en un esquema en demanda para los sitios indicados en el "Anexo VIII. Matriz de Servicios", donde se especificarán los anchos de banda fijo y bajo demanda, con los pisos y techos que se considerarán para cada sitio.

Para la prestación de este servicio, se consideran las siguientes condiciones:

OPERBES, S.A. DE C.V. cuenta con al menos dos conexiones STM-16 directas a Tier 1 y garantizar que la salida a Internet cuenta con redundancia en su salida internacional; en los casos donde se encuentre un enlace de alta disponibilidad, la salida del Enlace Activo tenga una salida Internacional diferente a la del enlace de Respaldo, está información deberá documentarla mediante carta bajo protesta de decir verdad en la Propuesta Técnica.

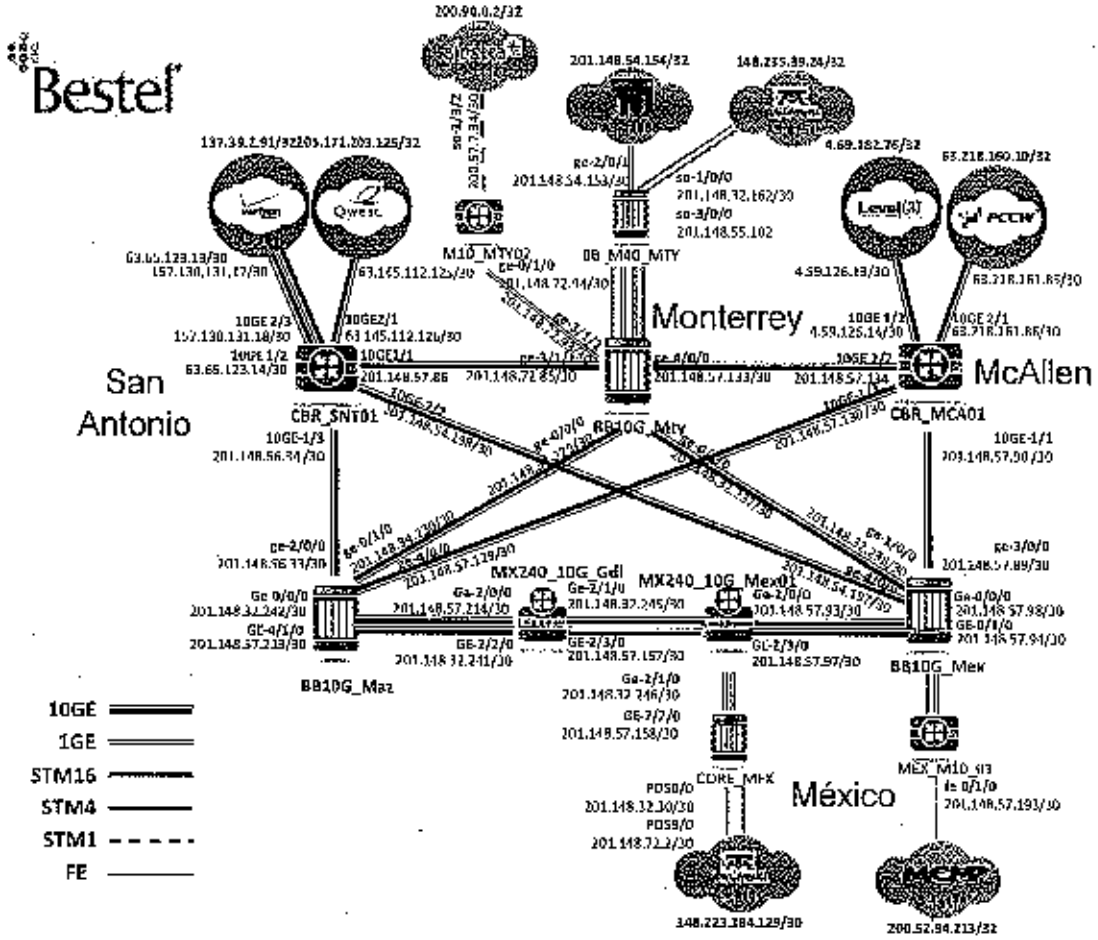


Diagrama del Backbone de internet de OPERBES, S.A. DE C.V.

Como puede verse en la arquitectura de referencia OPERBES, S.A. DE C.V. cuenta con las siguientes salidas a internet con las respectivas velocidades.

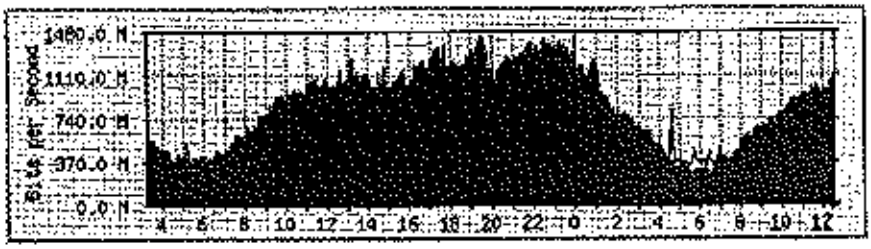
Ciudad	Proveedor	Velocidad
SAN ANTONIO	Verizon	10G bps
SAN ANTONIO	QUEST	10G bps
McAllen	PCCW	10G bps
McAllen	PCCW2	10G bps
McAllen	Level 3	10G bps
Nogales	Quest	10G bps
Nogales	Quest 2	10G bps

Conexion Qwest1

System: MX960_SNT in
Maintainer:
Description: xe-2/2/0 Conexion 10G QWEST ID:ETH10000-14647886
ifType: ethernetCsmacd (6)
ifName: xe-2/2/0
Max Speed: 1250.0 MBytes/s

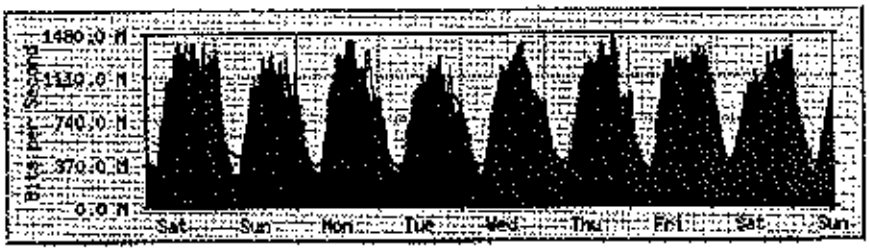
The statistics were last updated Sunday, 8 December 2013 at 12:36,
at which time 'MX960_SNT' had been up for 278 days, 16:13:35.

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	1447.2 Mb/s (14.5%)	852.9 Mb/s (8.5%)	1115.2 Mb/s (11.2%)
Out	1534.9 Mb/s (13.3%)	617.8 Mb/s (6.2%)	936.3 Mb/s (9.4%)

'Weekly' Graph (30 Minute Average)

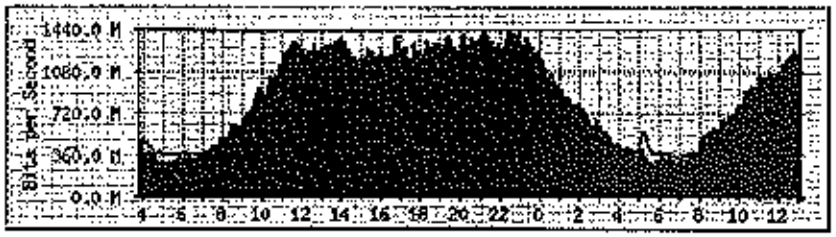


Conexion PCCW (1)

System: MX960_MCA in
Maintainer:
Description: xe-3/0/0 Conexion 10G PCCW 01 CIRCUITO_ID:BES003.0001.IX.21--SR039634
ifType: ethernetCsmacd (6)
ifName: xe-3/0/0
Max Speed: 1250.0 MBytes/s

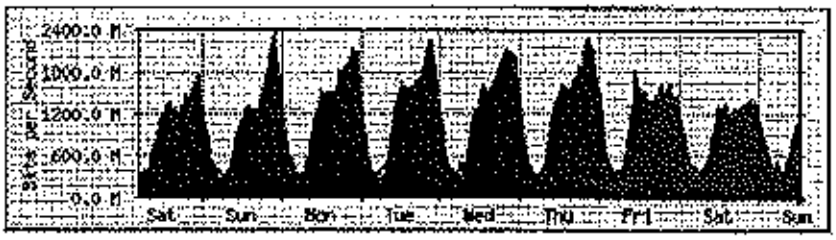
The statistics were last updated Sunday, 8 December 2013 at 13:06,
at which time 'MX960_MCA' had been up for 277 days, 15:33:37.

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	1416.3 Mb/s (14.2%)	886.7 Mb/s (8.9%)	1245.6 Mb/s (12.5%)
Out	874.6 Mb/s (8.7%)	607.1 Mb/s (6.1%)	738.0 Mb/s (7.4%)

'Weekly' Graph (30 Minute Average)

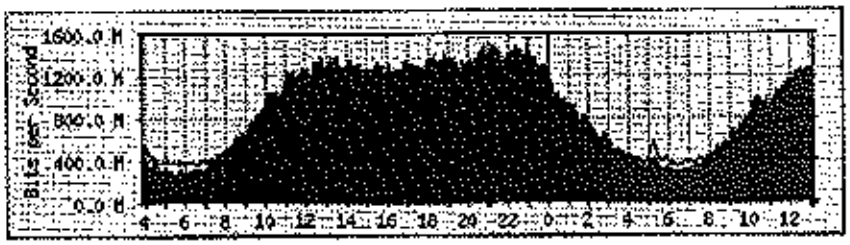


Conexion PCCW (2)

System: MX960_MCA in
Maintainer:
Description: xe-3/0/1 Conexion 10G PCCW 02 CIRCUITO_ID:BES003.0001.IX.26--SR47056
ifType: ethernetCsmacd (6)
ifName: xe-3/0/1
Max Speed: 1250.0 MBytes/s

The statistics were last updated Sunday, 8 December 2013 at 13:11,
at which time 'MX960_MCA' had been up for 277 days, 15:38:36.

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	1483.1 Mb/s (14.9%)	899.9 Mb/s (9.0%)	1268.2 Mb/s (12.7%)
Out	994.0 Mb/s (9.9%)	625.9 Mb/s (6.3%)	749.3 Mb/s (7.5%)

'Weekly' Graph (30 Minute Average)

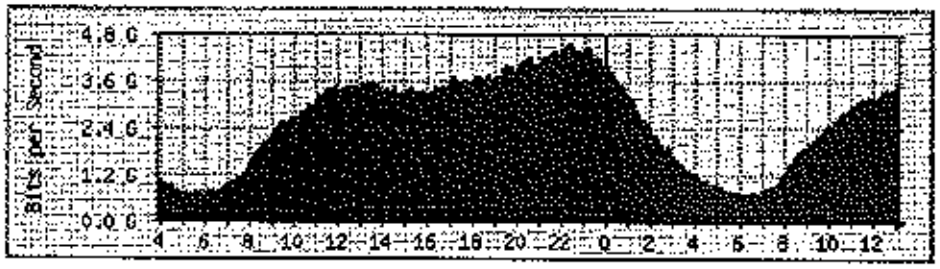
Interconexión 10GB con Tier-1 LEVEL 3

Conexion Level3 (1)

System: MX960_MCA in
Maintainer:
Description: xe-2/2/0 Conexion 10G LEVEL3 CIRCUIT-ID:BBGS3868
ifType: ethernetCsmacd (6)
ifName: xe-2/2/0
Max Speed: 1250.0 MBytes/s

The statistics were last updated Sunday, 8 December 2013 at 13:16,
at which time 'MX960_MCA' had been up for 277 days, 15:43:36.

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	4555.9 Mb/s (45.6%)	2592.0 Mb/s (25.9%)	3596.9 Mb/s (36.0%)
Out	367.3 Mb/s (3.7%)	200.5 Mb/s (2.0%)	245.6 Mb/s (2.5%)

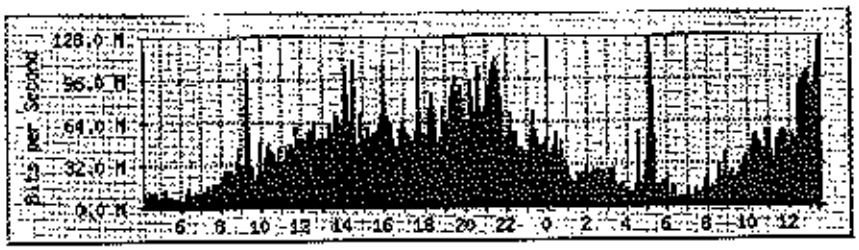
'Weekly' Graph (30 Minute Average)

CONEXION QWEST-01 10G

System: CBR_NOG01.bestel.com.mx in
Maintainer:
Description: TenGigabitEthernet1/2 CONEXION QWEST-01 10G ID: ETH10000-15962174
ifType: ethernetCsmacd (6)
ifName: Te1/2
Max Speed: 1250.0 MBytes/s

**The statistics were last updated Sunday, 8 December 2013 at 13:34,
at which time 'CBR_NOG01.bestel.com.mx' had been up for 10 days, 3:25:42.**

`Daily' Graph (5 Minute Average\)



	Max	Average	Current
In	125.0 Mb/s (1.3%)	42.5 Mb/s (0.4%)	99.9 Mb/s (1.0%)
Out	1200.0 b/s (0.0%)	752.0 b/s (0.0%)	183.0 b/s (0.0%)

`Weekly' Graph (30 Minute Average\)

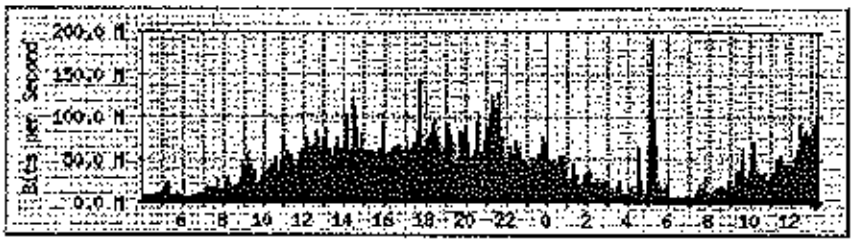
Interconexión 10GB con Tier-1 Qwest (2)

CONEXION QWEST-02 10G

System: CBR_NOG01.bestel.com.mx in
Maintainer:
Description: TenGigabitEthernet1/3 CONEXION QWEST-02 10G ID: ETH10000-16069713
ifType: ethernetCsmacd (6)
ifName: Te1/3
Max Speed: 1250.0 MBytes/s

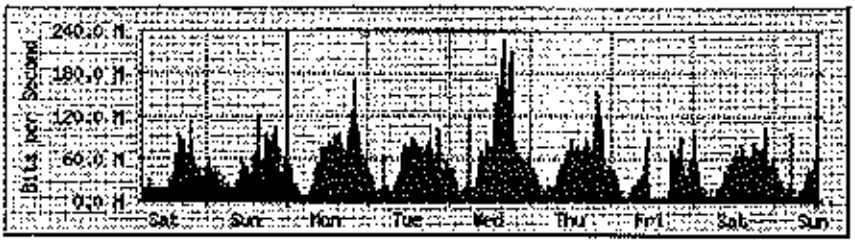
**The statistics were last updated Sunday, 8 December 2013 at 13:44,
at which time 'CBR_NOG01.bestel.com.mx' had been up for 10 days, 3:35:43.**

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	190.5 Mb/s (1.9%)	44.4 Mb/s (0.4%)	99.1 Mb/s (1.0%)
Out	368.0 b/s (0.0%)	72.0 b/s (0.0%)	72.0 b/s (0.0%)

'Weekly' Graph (30 Minute Average)



Listo

Además para la conexión del tráfico local OPERBES, S.A. DE C.V. cuenta con conexiones con los peerings nacionales que a continuación se mencionan.

Ciudad	Proveedor	Velocidad
Ciudad de México	UNINET	1Gbps
Distrito Federal	UNINET 2	1Gbps
Monterrey	UNINET	1Gbps
Monterrey	UNINET 2	1Gbps
Monterrey	TVI	1Gbps
Monterrey	Alestra	1STM1

Ciudad de México	MCM	50 Mbps

A continuación se presentan las gráficas del monitoreo de los enlaces mencionados.

PEERING'S NACIONALES

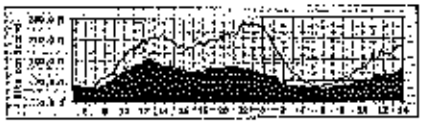
TELMEX MÉXICO (1GB Y 1GB):

1er-GE ENLACE PERRING UNINET

System: T1600_Mex-1a
Maintainer:
Description: 1er-GE ENLACE PERRING UNINET ge-3/0/3
ifType: ethernetCsmacd (6)
ifName: ge-3/0/3
Max Speed: 125.0 MBytes/s

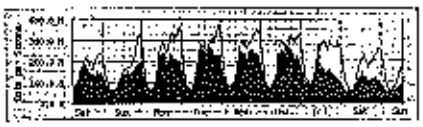
The statistics were last updated Sunday, 8 December 2013 at 14:05, at which time 'T1600_Mex' had been up for 298 days, 21:18:47.

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	143.6 MB/s (14.4%)	45.2 MB/s (9.0%)	100.8 MB/s (20.1%)
Out	268.1 MB/s (54.2%)	103.3 MB/s (41.3%)	187.3 MB/s (37.5%)

'Weekly' Graph (30 Minute Average)



2do-GE ENLACE PERRING UNINET

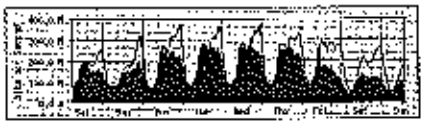
System: T1600_Mex-1a
Maintainer:
Description: 2do-GE ENLACE PERRING UNINET ge-3/1/6
ifType: ethernetCsmacd (6)
ifName: ge-3/1/6
Max Speed: 125.0 MBytes/s

The statistics were last updated Sunday, 8 December 2013 at 14:05, at which time 'T1600_Mex' had been up for 298 days, 21:18:47.

'Daily' Graph (5 Minute Average)

	Max	Average	Current
In	134.3 MB/s (13.5%)	50.1 MB/s (9.9%)	108.3 MB/s (21.8%)
Out	258.7 MB/s (51.5%)	105.0 MB/s (41.9%)	194.6 MB/s (37.7%)

'Weekly' Graph (30 Minute Average)



TELMEX MONTERREY (1GB Y 1GB):

1er-GE ENLACE PERRING UNINET

System: BBDG_Mty_re0-la
Maintainer:
Description: ge-3/3/0 PEER-INTERNET-UNINET GE02
ifType: ethernetCsmacd (6)
ifName: ge-3/3/0
Max Speed: 125.0 MBytes/s

The statistics were last updated Sunday, 8 December 2013 at 14:05, at which time 'BBDG_Mty_re0' had been up for 350 days, 7:21:53.

'Daily' Graph (5 Minute Average)

	Max	Average	Current
In	61.1 MB/s (6.1%)	19.2 MB/s (3.8%)	43.3 MB/s (8.7%)
Out	143.3 MB/s (28.7%)	70.3 MB/s (28.1%)	97.2 MB/s (19.4%)

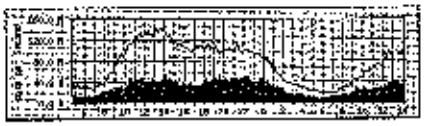
'Weekly' Graph (30 Minute Average)

2do-GE ENLACE PERRING UNINET

System: BBDG_Mty_re0-la
Maintainer:
Description: ge-3/3/1 PEER-INTERNET-UNINET GE02
ifType: ethernetCsmacd (6)
ifName: ge-3/3/1
Max Speed: 125.0 MBytes/s

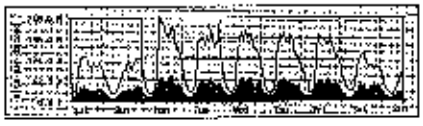
The statistics were last updated Sunday, 8 December 2013 at 14:05, at which time 'BBDG_Mty_re0' had been up for 350 days, 7:21:53.

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	71.3 MB/s (7.1%)	22.8 MB/s (4.6%)	51.7 MB/s (10.3%)
Out	145.8 MB/s (29.2%)	77.9 MB/s (31.2%)	110.2 MB/s (22.0%)

'Weekly' Graph (30 Minute Average)



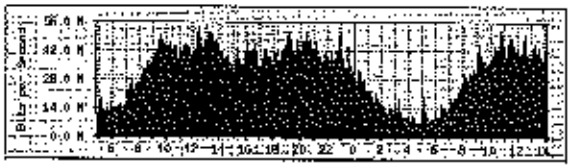
ALESTRA MONTERREY (1xSTM-1):

Alestra_Peering

System: M10_MTY02 in
Maintainer:
Description: so-1/3/2 Alestra_Peering_IPC_CDCAXCOSIPAA_33.PNXMPOPAA_00003
ifType: sonet (39)
ifName: so-1/3/2
Max Speed: 19.4 Mbytes/s

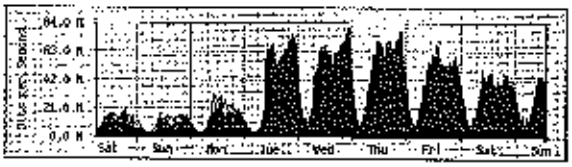
The statistics were last updated Sunday, 8 December 2013 at 14:11,
at which time 'M10_MTY02' had been up for 303 days, 14:00:44.

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	52.1 Mb/s (33.9%)	32.1 Mb/s (20.6%)	19.9 Mb/s (21.6%)
Out	25.6 Mb/s (16.5%)	11.5 Mb/s (7.3%)	15.4 Mb/s (9.9%)

'Weekly' Graph (30 Minute Average)



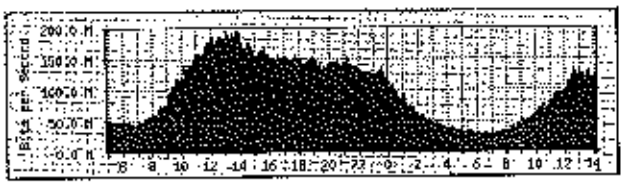
TVI MONTERREY (1xGB):

Enlace PEER TVI

System: BB_M40_MTY in
Maintainer:
Description: ge-2/0/1 ENLACE PEER A TVI BEST.MTY40.MTY33.00001
ifType: ethernetCsmacd (6)
ifName: ge-2/0/1
Max Speed: 125.0 MBytes/s

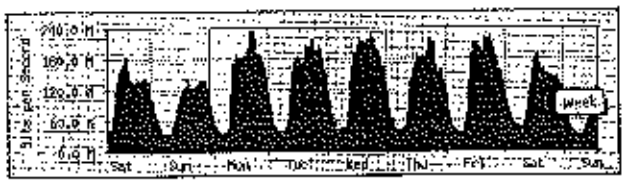
The statistics were last updated Sunday, 8 December 2013 at 14:10,
at which time 'BB_M40_MTY' had been up for 316 days, 3:38:26.

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	195.8 Mb/s (19.4%)	100.0 Mb/s (10.0%)	123.7 Mb/s (12.3%)
Out	21.3 Mb/s (2.1%)	11.1 Mb/s (1.1%)	11.4 Mb/s (1.1%)

'Weekly' Graph (30 Minute Average)



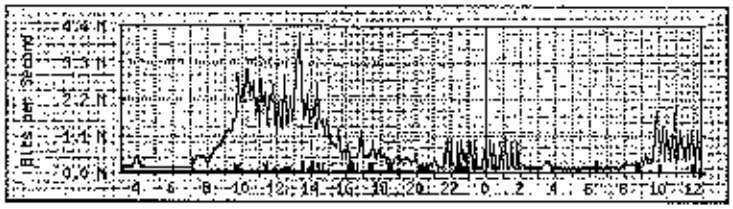
MCM MÉXICO (1xFE):

PEERING MCM 50M

System: MEX_M10_01 in
Maintainer:
Description: fe-0/1/0 PeeringMCM-BEST.DFO40.DFX01.00002
ifType: ethernetCsmacd (6)
ifName: fe-0/1/0
Max Speed: 12.5 MBytes/s

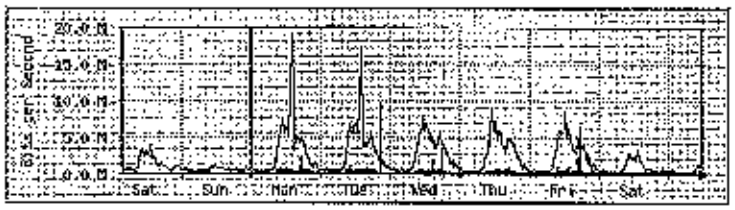
The statistics were last updated **Sunday, 8 December 2013 at 12:25.**
at which time 'MEX_M10_01' had been up for **8 days, 10:07:36.**

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	425.1 kb/s (0.4%)	43.1 kb/s (0.0%)	301.6 kb/s (0.3%)
Out	4092.4 kb/s (4.1%)	639.7 kb/s (0.6%)	1103.4 kb/s (1.1%)

'Weekly' Graph (30 Minute Average)



El tiempo de respuesta entre los equipos OPERBES, S.A. DE C.V. y de Internet Tier-1, no será mayor a 60 ms, desde el equipo de acceso OPERBES, S.A. DE C.V. de servicio hasta el Tier-1. OPERBES, S.A. DE C.V. integra como parte de su proposición el resultado del comando para respuesta de eco (ping) entre el equipo que asignará para el servicio de internet y el equipo de ruteo hacia el Licitante Internacional de Internet Tier-1.

A continuación se adjunta un Ping desde el equipo PE al cual se conectará el Sitio Central de SHF a internet, en él se pueden observar que la latencia promedio es de 30ms.

```
ASR1006_MTY01#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/30/31 ms
```

Resultado de los pings de latencia

OPERBES, S.A. DE C.V. manifiesta por escrito, que cuenta con Acuerdos de Peering con al menos dos de los Proveedores de Internet en México, lo anterior, con la finalidad de optimizar el intercambio del tráfico doméstico o Nacional entre los distintos Proveedores de Internet.

OPERBES, S.A. DE C.V. puede ofrecer 2 saltos a Internet Tier-1 en su plataforma, medidos desde su equipo de acceso (CPE) en su red hasta el Proveedor de Internet Internacional (Tier-1), presentando el resultado de la ejecución de comandos que lo comprueben, con un escrito manifestando lo anterior haciéndose sujeto a someterse a las pruebas técnicas necesarias para demostrarlo.

A continuación se anexa un tracert desde el equipo PE al cual se conectará el Sitio Central de SHF, se puede observar que presenta 2 saltos al router del Tier 1 el cual es Level 3

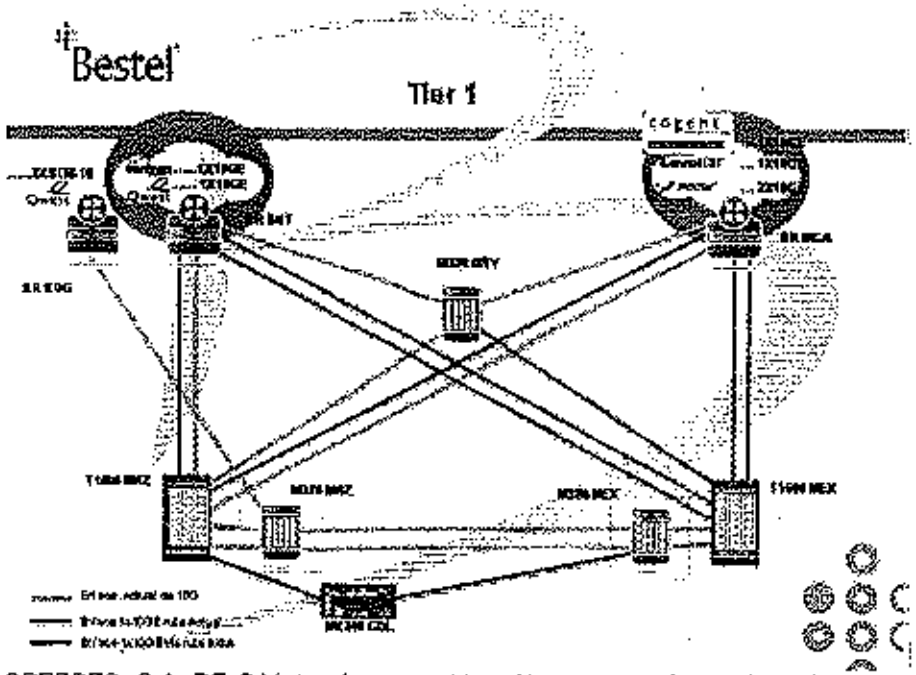
Ruteador de Acceso Cisco 7609 en Ciudad de México

C7609_MEX01#traceroute www.level3.com

Type escape sequence to abort.
Tracing the route to www.level3.com (4.68.90.77)

1 14.201-140-112.bestel.com.mx (201.140.112.14) [AS 3491] 16 msec 12 msec 16 msec
2 xe-11-0-0.bar2.Houston1.Level3.net (4.59.126.77) [AS 3356] 24 msec
xe-9-1-0.bar2.Houston1.Level3.net (4.59.126.25) [AS 3356] 24 msec
xe-11-0-0.bar2.Houston1.Level3.net (4.59.126.77) [AS 3356] 188 msec
3 ae-0-11.bar1.Houston1.Level3.net (4.69.137.133) [AS 3356] 28 msec 24 msec 28 msec
4 ae-13-13.ebr1.Dallas1.Level3.net (4.69.137.138) [AS 3356] 28 msec 28 msec 28 msec
5 ae-71-71.csw2.Dallas1.Level3.net (4.69.151.137) [AS 3356] 28 msec
ae-81-81.csw3.Dallas1.Level3.net (4.69.151.149) [AS 3356] 28 msec 36 msec
6 ae-62-62.ebr2.Dallas1.Level3.net (4.69.151.130) [AS 3356] 28 msec 28 msec
ae-72-72.ebr2.Dallas1.Level3.net (4.69.151.142) [AS 3356] 28 msec
7 ae-2-2.ebr1.Denver1.Level3.net (4.69.132.105) [AS 3356] 48 msec 44 msec 48 msec
8 ae-11-51.car1.Denver1.Level3.net (4.69.147.67) [AS 3356] 48 msec 44 msec 48 msec
9 ge-9-1.hsa1.Denver1.Level3.net (4.69.200.57) [AS 3356] 44 msec 48 msec 44 msec
10 4.68.94.26 [AS 3356] 44 msec 44 msec 44 msec
11 4.68.94.33 [AS 3356] 48 msec 48 msec 44 msec
12 eth2.l3hqdc7705.idc1.Broomfield1.Level3.net (4.68.92.2) [AS 3356] 48 msec 48 msec 44 msec
13 4.68.92.33 [AS 3356] 48 msec 48 msec 48 msec
14 * * *
15
C7609_MEX01#

Se adjunta un diagrama a bloques de nuestros proveedores de Tier 1



OPERBES, S.A. DE C.V. tomó en consideración que para los nodos críticos se operará con balanceo de cargas en ambos enlaces. En caso de falla se conmutará automáticamente el tráfico al enlace que se encuentre operando correctamente.

En caso de falla total del nodo crítico conmutará automáticamente el tráfico a través de la RPV MPLS al nodo más cercano con salida a Internet de SHF.

La administración de las políticas de acuerdo al tipo de solución de seguridad propuesta, tales como: Firewall, IPS, administración de ancho de banda y del filtrado de contenido será definida por SHF con OPERBES, S.A. DE C.V. durante las sesiones posteriores al inicio de la vigencia del contrato, mismas que estarán implementadas al inicio de la operación del servicio.

El ancho de banda propuesto se describe en el "Anexo VIII. Matriz de Servicios".

El servicio de acceso a Internet será en esquema bajo demanda, teniendo en consideración los valores de ancho de banda mínimo y máximo expresados en el "Anexo VIII. Matriz de Servicios", así como la tabla de valores de ancho de banda que pueden requerirse y los niveles de servicio que se aplicará en caso de incrementos o decrementos, ambos casos durante la vigencia del servicio. El uso de ancho de banda que se encuentre entre el piso y techo será dinámico, sin solicitud expresa de SHF.

SHF proporcionarán a OPERBES, S.A. DE C.V. el direccionamiento IPv4 así como el Sistema Autónomo para que sea propagado en su MPLS. El segmento es el siguiente:

Clase C (256 direcciones IP) direcciones IP homologadas para SHF.

Esta solicitud permitirá, cuando así sea solicitado por SHF, el incremento en bloques de 32 direcciones de IP homologadas por SHF, sin generar costos adicionales.

En el costo del Servicio de Acceso a Internet, OPERBES, S.A. DE C.V. considera todos los elementos que necesarios para prestar dicho servicio, que de manera enunciativa más no limitativa podrán ser: ruteador multiservicio, switches, enlaces.

Características de Seguridad para el Servicio de Internet

La infraestructura de Internet de OPERBES, S.A. DE C.V. como propuesta a SHF incluye un mecanismo para determinar en forma automática el comportamiento anómalo del servicio y tener la capacidad de alertar a SHF para mitigar cualquier actividad maliciosa que se presente como ataques de tipo Negación de Servicio Distribuido (DDoS, por sus siglas en inglés) y/o Negación de Servicio Dirigido (DoS, por sus siglas en inglés) generado por medio de la actividad de gusanos o de ataques de tipo botnets, basado en la tecnología Clean Pipes del fabricante Arbor.

Por lo tanto, el servicio integrará un sistema de gestión de amenazas que realice una inspección profunda de paquetes, que permitirá a OPERBES, S.A. DE C.V. como proveedor del servicio 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.

El sistema realizará el análisis del flujo de tráfico buscando patrones de tráfico anormales que indiquen la presencia de un ataque tipo DDoS y DoS.

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

El análisis del tráfico, la detección de anomalías y el proceso de mitigación de ataques de tipo DDoS y DoS, se llevará a cabo en la infraestructura de OPERBES, S.A. DE C.V., el objetivo es que el proceso de mitigación del tráfico de ataque se realice antes de que pueda llegar a las redes de SHF y acabar con los recursos de ancho de banda.

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

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.

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

Ataques de saturación de recursos SSL Ingeniería de tráfico inteligente:

Visibilidad escalable y análisis del tráfico con tecnología de "flujo" de la red.

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

Portal personalizable e independiente para SHF, el cual permitirá crear las plantillas para visualizar recursos específicos, reportes, ataques.

Iniciar mitigaciones y contadores de medidas para reducir el impacto de los ataques.

Para los ataques detectados se ofrecerá la opción de generar recomendaciones de listas de acceso basadas en cada ataque.

Por lo menos se proveerá acceso a los últimos 3 meses en línea de las alertas y las mitigaciones ocurridas.

A través de la misma página Web se permitirá la generación de Huellas digitales (Fingerprints) posteriores a los ataques existentes, que deben proveer información en texto de capa 3 y 4 en un formato legible de manera que permita identificar un ataque aunque cambie la heurística del mismo.

Permitirá a OPERBES, S.A. DE C.V. realizar al menos mitigaciones con:

Inyección de Blackhole de BGP.

Filtros con listas de acceso (ACLs).

Dispositivos de mitigación que ofrecerán una mitigación inteligente, filtrar tráfico malicioso mientras se permite el tráfico válido para alcanzar el elemento que está siendo atacado.

Permitirá a OPERBES, S.A. DE C.V. seleccionar la mitigación a aplicarse, así como, generar reportes y modificaciones en tiempo real dependiendo de los resultados de la mitigación.

Permitirá a OPERBES, S.A. DE C.V. generar reportes de las mitigaciones que fueron ejecutadas anteriormente, con detalles de tráfico descartado y transferido para cada uno de los medidores.

IP redundante para acceso al portal Web que se pueda dar de baja sin la intervención manual de OPERBES, S.A. DE C.V. en caso de falla de la dirección primaria, y sin pérdida de la información de la línea de base o estadística, para asegurar la alta disponibilidad del sistema para SHF.

Las notificaciones serán enviadas al menos vía correo electrónico desde el sistema para informar a OPERBES, S.A. DE C.V. y a SHF con opciones configurables para permitir una rápida reacción.

La mitigación tendrá al menos las siguientes características:

Mitigación de específico SYN Flood.

Mitigación del DNS (protocolo mal formado y basado en autenticación).

Mitigación con taza límite por cliente de HTTP Get Flood y por objeto.

Línea de base por recurso.

Detección de 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.

OPERBES, S.A. DE C.V. incluye a continuación en su proposición una descripción detallada de esta solución indicando los elementos que la integran, así como la descripción de los procesos de análisis de información, detección de anomalías y mitigación de ataques.

OPERBES, S.A. DE C.V. incluye 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 Operbes, S.A. de C.V. 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 Operbes, S.A. de C.V. mitigar cualquier actividad maliciosa que se presente en forma de ataques de tipo Denegación de Servicio Distribuido.

Operbes, S.A. de C.V. tomó 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 Operbes, S.A. de C.V.

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.

La solución detección, gestión y mitigación de ataques DoS/DDoS detectará cualquier condición anómala, 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 permanecerá siempre disponibles.

Operbes, S.A. de C.V. tomó 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 períodos 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. Operbes, S.A. de C.V. tomó 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 Operbes, S.A. de C.V. monitoreará el tráfico con el fin de detectar los ataques DDoS desde su ingreso a la infraestructura de Operbes, S.A. de C.V. para que este pueda 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 Operbes, S.A. de C.V. 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.

Contención de Ataques en el Perímetro de Internet.

OPERBES, S.A. DE C.V. tomó en consideración que en complemento con la seguridad en el servicio de acceso a internet, SHF requieren una solución que garantice la continuidad y disponibilidad de las aplicaciones críticas del negocio de manera perimetral, que proporcione una tecnología de detección, mitigación y neutralización automática de ataques de ancho de banda reducido antes de que afecten los servicios críticos de SHF, OPERBES, S.A. DE C.V. proporcionará un sistema de protección en el perímetro de SHF.

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

Será una caja de propósito específico dedicado a proporcionar disponibilidad; por lo que no se Proponen 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 .Será de la marca ARBOR que es la misma que la herramienta con la que se proporciona en la nube de Internet de OPERBES, S.A. DE C.V.

Las capacidades mínimas de los equipos se consideraron con base a la siguiente tabla:

Tipo	Inspección/ Throughput	Memoria	Conexiones por segundo	Rendimiento para paquetes pequeños	Interfaces
I	3 Gbps	18 GB	300,000	8.5 Mpps	Fibra y Cobre según las características de los Enlaces
II	2 Gbps	18 GB	300,000	7.5 Mpps	
III	1 Gbps	10 GB	100,000	1.5 Mpps	
IV	500 Mbps	10GB	100,000	1.2 Mpps	

Tabla: 2.2.1

OPERBES, S.A. DE C.V. tomó en consideración que para el caso de los equipos tipo 1 y tipo 2, si el rendimiento (medido en base al uso de memoria y CPU) se encuentra entre el 70% y 85% promedio de su desempeño, durante 10 días hábiles consecutivos o derivados de un ataque o incidente volumétrico, OPERBES, S.A. DE C.V. deberá ampliar la capacidad de dicho rendimiento, sin la necesidad de cambiar por un hardware nuevo y sin costo para SHF. Aplica únicamente para el desempeño del equipo asociado al servicio.

Si el rendimiento es mayor del 85% promedio durante 3 días hábiles consecutivos de operación normal, OPERBES, S.A. DE C.V. remplazará el equipo, por la siguiente categoría, en un plazo no mayor a tres días hábiles.

El sistema tendrá embebido el bypass físico en cada interface para garantizar la disponibilidad y continuidad de los servicios activándose en los siguientes casos:

Perdida de energía eléctrica.
Falla lógica en la interface de control.
Pérdida de conectividad con la tarjeta madre del dispositivo.
Colapso del sistema operativo.

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.

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".

El sistema soportará la implementación en modo "monitor" en el que no introduce ningún punto adicional de falla a la red.

El sistema será capaz de capturar tráfico directamente desde un puerto espejo (SPAN) en un enrutador, switch o tap.

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.

El sistema soportará redundancia completa para fuentes de alimentación.

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:

El sistema proporcionará documentación en línea para consulta vía Web para ayudar a SHF a comprender las funciones de cada pantalla.

OPERBES, S.A. DE C.V. proporcionará cuentas de solo lectura al sistema para la consulta y revisión de configuración. El acceso será vía Web y SSH.

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.

El sistema proporcionará la capacidad para crear y exportar paquetes de diagnóstico que contienen información del estado y configuración a utilizarse para resolver problemas.

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.

El sistema admitirá el control de su estado general a través de SNMP v3.

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.

El sistema proporcionará listas de control de acceso IP para todos los servicios remotos que estén accesibles.

El sistema proporcionará Acceso, Autentificación y Auditoria a los usuarios a través de una base de datos de: usuario local, RADIUS, TACACS+ o la configuración combinada de métodos.

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.

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.

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.

El sistema mostrará estadísticas de protección en tiempo real sobre tráfico permitido y bloqueado en bytes y paquetes, con estadísticas en bps y pps.

Proporcionará estadísticas detalladas y gráficos para mínimo los siguientes grupos de protección:

Servidores de Aplicaciones
servidores Web
servidores DNS
servidores VoIP

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.

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 parte de la solución la mitigación en la Nube de Internet de OPERBES, S.A. DE C.V. operará de la siguiente forma:

El sistema solicitará a través de un protocolo de señalización en la nube.

La funcionalidad del sistema de "señalización en la nube de OPERBES, S.A. DE C.V." soportará la solicitud de mitigación ascendente en la nube que proporciona la conectividad a Internet.

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.

El sistema automáticamente reportaár el estado y estadísticas durante una mitigación en la nube: iniciada por OPERBES, S.A. DE C.V. sin necesidad de una solicitud explícita de SHF.

El sistema será capaz de informar la cantidad de tráfico bloqueado en bps y pps durante una mitigación en la nube en curso.

El sistema será capaz de informar la cantidad de tiempo que una mitigación de nube lleva ejecutándose.

El sistema será capaz de informar el estado actual de una solicitud de mitigación de nube, informando si se ha activado correctamente o no.

El sistema enviará notificaciones acerca de cualquier cambio de la mitigación.

El sistema será capaz de reportar el estado de la conexión de señalización en la nube con el sistema del SOC de OPERBES, S.A. DE C.V., mostrando el estado, errores de conexión y cuando haya sido deshabilitado.

El sistema podrá proporcionar la capacidad para manualmente disparar una prueba de conexión de señalización en la nube con el SOC del Licitante.

La prevención de ataques soportará y operará de la siguiente manera:

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

Permitirá la configuración de listas de filtros que contengan expresiones FCAP para permitir o bloquear tráfico.

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).

Descartará paquetes según puertos TCP / UDP específicos y payloads que coincidan o no con expresiones regulares configurables.

Prevención de inundación suplantada de SYN's TCP que autentifiquen conexiones TCP desde los host origen.

Prevención de inundación suplantada de SYN's TCP será capaz de especificar los puertos TCP origen y destino a ser ignorados.

Prevención de inundación suplantada SYN's TCP proporcionará una forma de no impactar sesiones de usuarios legítimos HTTP a través de redirección HTTP subsecuente.

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.

Eliminación de sesiones TCP inactivas si SHF no envía una cantidad de datos configurable por OPERBES, S.A. DE C.V. dentro de un periodo de tiempo.

Soportará la capacidad de poner en listas negras a los host después de un número de conexiones TCP consecutivas inactivas configurables por OPERBES, S.A. DE C.V.

Soportará el bloqueo de solicitudes DNS malformadas en el puerto 53 que no cumplan con el estándar RFC

Autentificará solicitudes DNS desde el host origen y eliminar aquellas que no puedan ser autentificadas dentro de un tiempo específico

Limitará el número de consultas DNS por segundo a una velocidad configurable por el Licitante

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.

Configurará expresiones regulares para suprimir el tráfico DNS específico con los encabezados que coincidan con las expresiones.

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.

Bloqueará hosts que exceden un umbral configurable para el número total de operaciones por segundo, por servidor destino

Suprimirá paquetes HTTP específicos según los encabezados HTTP coincidentes con hasta 5 expresiones regulares configurables

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).

Detectará y bloqueará las inundaciones de SYN's TCP por encima de la tasa configurada.

Detectará y bloqueará las inundaciones ICMP por encima de la tasa configurada.

Bloqueará el tráfico procedente de fuentes que interrumpen reiteradamente solicitudes HTTP

Bloqueará el tráfico originado por BOT's según las firmas proporcionadas por el sistema.

Activará las nuevas técnicas de defensa actualizando las firmas que serán mantenidas por el equipo de investigación del fabricante 24x7

Actualizará automáticamente sus firmas de protección de ataques periódicamente a intervalos configurables o de forma manual.

Actualización de firma de protección de ataques a través de servidores proxy.

Configuración de protecciones predefinidas asociadas con servicios específicos, como Web, DNS, VoIP o un servidor genérico.

El sistema permititrá que los parámetros de protección sean cambiados mientras la protección está corriendo.

El sistema podrá bloquear tráfico por país de origen.

En el apartado contención de ataques en el perímetro de Internet, se describe la solución considerada

Administrador de Ancho de Banda

OPERBES, S.A. DE C.V. tomó en consideración que SHF requiere de una solución que permita administrar el ancho de banda de las aplicaciones internas y externas en tiempo real, asignando prioridades y recursos de red en función del puerto, el dispositivo y la identificación de las aplicaciones o el contenido en internet, con al menos las siguientes especificaciones:

Será una caja de propósito específico dedicado a proporcionar la administración de ancho de banda hacia el canal de Internet, alineándose a las necesidades de SHF y operar de manera conjunta con todos los elementos del nodo, de acuerdo a su criticidad.

Los requerimientos descritos y requeridos serán respaldados por documentación técnica del fabricante referenciado con catálogos, manuales y publicaciones en el sitio web del fabricante.

Las capacidades mínimas de los equipos se consideran de acuerdo a los requerimientos de ancho de banda de los enlaces de Internet solicitados por SHF.

OPERBES, S.A. DE C.V. incluye todos los elementos de hardware y software necesario para la correcta operación, así como lo necesario para su montaje en gabinetes.

La solución propuesta se integrará de manera transparente dentro de la infraestructura de red existente.

Soporte en modo de alta disponibilidad para SHF.

En caso de falla o falta de energía eléctrica en los equipos, estos no afectarán la comunicación (modo Bypass).

OPERBES, S.A. DE C.V. informará a SHF de actualizaciones, parches o mejoras de versiones aplicables a los equipos en cuestión, en un tiempo máximo de 15 días de haberse liberado por el fabricante.

Si el rendimiento de los equipos se encuentra entre el 70% y 85% promedio de su desempeño (utilizando como métricas de desempeño uso de memoria y CPU), durante 10 días hábiles consecutivos, OPERBES, S.A. DE C.V. ampliará la capacidad de dicho rendimiento, sin la necesidad de cambiar por un hardware nuevo y sin costo para SHF. Aplica únicamente para el desempeño del equipo asociado al servicio.

Si el rendimiento es mayor del 85% promedio durante 3 días hábiles consecutivos de operación normal, OPERBES, S.A. DE C.V. Reemplazará el equipo, por la siguiente categoría, en un plazo no mayor a tres días hábiles. Se evaluará el tráfico en las horas de mayor demanda de servicio, estableciéndose para ello el horario de las 10:00 a las 19:00 horas.

Asignará parámetros de "traffic shapping" por usuario, grupo, dirección IP, rango de direcciones IP, categoría, aplicación, prioridad.

Asignará 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 y prioridad.

Priorizar el tráfico por categoría, contenido web, IP o grupos de IP's para las aplicaciones críticas definidas por SHF, garantizando el ancho de banda.

Asignar ancho de banda por aplicación controlando el tráfico por tipo de prioridad.

Registrará el ancho de banda consumido por las aplicaciones y categorías de contenido web, tiempos de respuesta de las principales aplicaciones de red y el servidor de retraso, además de monitorear la salud, eficiencia y retransmisiones TCP en la red.

Identificará y clasificará las aplicaciones web, contenidas y amenazas Web. Controlando el rendimiento en tiempo real y reuniendo la evidencia para resolver problemas de rendimiento. Los modeladores no hacen funciones de seguridad, por lo que no detectan aplicaciones maliciosas por lo anterior ésta funcionalidad es opcional a través de un equipo externo como IPS FW.

Garantizará o controlará el ancho de banda al menos para los siguientes tipos de aplicaciones que se mencionan a continuación de manera enunciativa mas no limitativa:

Cliente Servidor
Colaboración
Entrega de Contenido
Base de datos
Directorio Activo
Correo Electrónico
Servidores de Archivos
Juegos
Mensajería
P2P
VoIP
Multimedia

Administración, Integración y Reporteo.

Administración por SSH, CLI, HTTPS.

Envío de eventos vía SNMP V3., en forma mínima.

Administración centralizada bajo las siguientes características:

Se cambiará la contraseña para tener acceso a la interface de administración, además de limitar el acceso a la misma.

Visualizará estadísticas numéricas y gráficas del uso del ancho de banda, en tiempo real, por hora, por día y por mes.

Incluirá una pantalla desde donde se puedan visualizar reportes por tipo, con rangos de fechas y su visualización en línea.

Los tipos de reportes requeridos, en línea al menos serán los siguientes:

Top por IP
Top por tipo de aplicación.
Top por prioridad
Top por calidad de servicio.
Top por protocolo

Realizará actualizaciones centralizadas del software, de forma remota.

En el Apartado Administrador de Ancho de Banda se describe la solución considerada.

Servicio de Domain Name Server (DNS)

OPERBES, S.A. DE C.V. proporcionará el servicio administrado de DNS. Los servicios de DNS Interno y/o Externo proporcionados por el Licitante deberán considerar:

El servidor de DNS de frontera (Externo) que brindará la resolución de dominios de Internet al esquema de DNS Internos de SHF con una disponibilidad del 99.98% mensual.

Resolución de nombres para los dominios de Internet de SHF.

El Servicio de DNS externo estará considerado en la solución de Internet y en las instalaciones de OPERBES, S.A. DE C.V.

SHF entregará a OPERBES, S.A. DE C.V. en caso de ser el licitante ganador el listado de los Dominios que deberá publicar.

El DNS Interno se ubicará en las Instalaciones de SHF y el DNS Externo se ubicará en las Instalaciones del Licitante.

El servicio de Resolución de Nombre de Dominio será una solución integrada por hardware y software conformado con una infraestructura que permita cumplir con la funcionalidad y los niveles de servicio descritos en el presente documento.

OPERBES, S.A. DE C.V. tomó en consideración que la propiedad de los nombres de Dominio ante el NIC quedará a nombre del responsable que indique SHF, fungiendo OPERBES, S.A. DE C.V. como punto de contacto técnico durante la vigencia del servicio, este trámite lo realizará SHF.

SHF contempla que el servicio de DNS administre los dominios y subdominios de Internet que sean requeridos durante la vigencia del contrato.

SHF entregará a OPERBES, S.A. DE C.V. en caso de ser el licitante ganador el listado de los Dominios que deberá publicar.

OPERBES, S.A. DE C.V. indica el o los servicios requerido en el "Anexo VIII. Matriz de Servicios".

Servicio de Integración a IPv6

Durante la vigencia del contrato OPERBES, S.A. DE C.V. tomó en consideración que se podrá solicitar la integración de direccionamiento IPV6, y se considera que los equipos propuestos soportan IPV6.

OPERBES, S.A. DE C.V. será responsable de realizar las actividades necesarias para la implementación del direccionamiento, la cual puede incluir las siguientes actividades siendo estas enunciativas más no limitativas:

Levantamientos de red.
Definición de direccionamientos
Plan de trabajo
Plan de migración
Definición de las reglas de convivencia entre el direccionamiento IPV4 e IPV6.
Definición, suministro, instalación y configuración de hardware adicional.
Actualizaciones de Hardware
Actualizaciones de Software
Maquetas
Pruebas
Memoria Técnica.

OPERBES, S.A. DE C.V. tomó en consideración que las actividades necesarias hasta su puesta en operación serán concluidas de acuerdo al Plan de trabajo definido conjuntamente entre OPERBES, S.A. DE C.V. y SHF, a partir de la solicitud vía oficio.

OPERBES, S.A. DE C.V. tomó en consideración que La operación de IPV6 garantizará el cumplimiento de los niveles de servicio solicitados para IPV4.

Servicio de Seguridad Perimetral

Descripción del Servicio.

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; OPERBES, S.A. DE C.V. implementará la infraestructura de seguridad necesaria para proteger las aplicaciones.

OPERBES, S.A. DE C.V. implementará los diferentes Servicios de Seguridad Perimetral con el objetivo de garantizar niveles de confianza para un control de acceso a las redes RPV-MPLS, Internet e Intranet, así como la definición de políticas en zonas desmilitarizadas (DMZ) donde se alojarán los servicios y/o aplicaciones expuestas a Internet.

OPERBES, S.A. DE C.V. considera en la presente propuesta los servicios profesionales por parte del Fabricante para el diseño de la arquitectura, instalación, configuración, parametrización, pruebas, puesta en operación y ajuste fino de todas las soluciones integradas para el desarrollo del servicio. El diseño estará basado en mejores prácticas.

Se consideran al menos 3 meses de operación asistida por parte del fabricante una vez que se dé por terminada la instalación y configuración de los equipos propuestos.

Se considera la asistencia por parte del fabricante de al menos 2 eventos al año en caso de que algún incidente o falla no permita brindar los niveles de servicio solicitados, requerido soporte en sitio y sin costo para SHF.

OPERBES, S.A. DE C.V. incluirá todos los elementos de hardware y software necesario para la correcta operación así como lo necesario para su montaje en gabinetes.

SHF podrá elegir cualquiera de los servicios mencionados en la siguiente tabla según sus necesidades de manera independiente.

COMPONENTES	Nomenclatura
FIREWALL	FW
IPS	IPS
WAF	WAF
MULTIFUNCIONAL	MF
PROTECCIÓN CONTRA MALWARE WEB	PCM
CORRELACIONADOR DE EVENTOS	CE

Tabla: 3.1

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

Servicio de Firewall

OPERBES, S.A. DE C.V. considera para esta solución de equipos de propósito específico solo con la tecnología de Firewall, las cuales incluirán y operarán al menos con las siguientes características:

Si el rendimiento de los equipos se encuentra entre el 70% y 85% promedio de su desempeño (usando como métricas de desempeño el uso del CPU y memoria), durante 10 días hábiles consecutivos, OPERBES, S.A. DE C.V. ampliará la capacidad de dicho rendimiento, sin la necesidad de cambiar por un hardware nuevo y sin costo para SHF. Aplica únicamente para el desempeño del equipo asociado al servicio.

Si el rendimiento es mayor del 85% promedio durante 3 días hábiles consecutivos de operación normal, el OPERBES, S.A. DE C.V. reemplazará el equipo, por la siguiente categoría, en un plazo no mayor a tres días hábiles, el monto del cambio de equipamiento será cubierto por SHF en base a la lista de precios unitarios proporcionada por OPERBES, S.A. DE C.V., esto aplica únicamente para el caso de cambio de equipamiento.

La siguiente tabla muestra las características generales que al menos se consideran para la tecnología de Firewall.

IPO	Throughput	Memoria	Throughput VPN	Sesiones Concurrentes	Interfaces
	10 a 12 Gbps	6 a 8GB	2 -3 Gbps	3,000,000 a 5,000,000	8-10/100/1000
I	6 a 9 Gbps	2 a 4 GB	1- 2 Gbps	1,500,000 a 3,000,000	6-10/100/1000
II	1 a 5 Gbps	1 GB	400 a 800 Mbps	500,000 a 1,000,000	4-10/100/1000
V	500 a 800 Mbps	500 MB a 1GB	200 a 500 Mbps	200,000 a 450,000	3-10/100/1000
	200 a 450 Mbps	250 a 500 MB	35 a 100 Mbps	50,000 a 150,000	2-10/100/1000

Tabla: 3.1.1

Características técnicas mínimas incluidas:

Aceleración por hardware.

2 fuentes de poder redundantes para los Firewall tipo I Y II.

Los Firewalls tipo I y II soportarán interfaces 10G y estarán disponibles en caso de que SHF lo requiera al inicio del proyecto o bajo demanda.

Disco duro de al menos 250 GB para los Firewalls tipo I Y II

Implementación en modo transparente y Gateway.

Balanceo de cargas y alta disponibilidad sin incluir software y/o hardware de terceros y sin costo adicional.

Operar en alta disponibilidad en modo Activo/Activo y Activo/Pasivo.

Protocolos LAN: 802.3ad, , 802.1q

Ruteo dinámico en IPv4 e IPv6, con por lo menos los protocolos OSPF, BGP y RIP, así como Multicast, Policy-based routing. RIPv1 y 2, RIPng, IGMP (1 y 2), PIM SM.

NAT (incluyendo para VoIP) y PAT.

Tecnología IPv6; Dual Stacking firewall y VPN, Túneles IPv4 to IPv6, Túneles IPv4 desde IPv6
Tecnología de QoS basada en colas inteligentes, tales como Diffserv, TOS.
Monitoreo gráfico en tiempo real del tráfico de QoS que está circulando por el equipo.
Permitir modificar el MTU para evitar problemas de fragmentación de paquetes encriptados
Soportar valores de MTU mayores a 1500 bytes, para incrementar el rendimiento de interfaces gigabit, permitiendo modificar el MSS
Definir límites en el ancho de banda para restringir aplicaciones no críticas en la red.
Contará con alguna de las siguientes certificaciones:
Certificación de NSSLabs.
Certificación ICSA Labs
Common Criteria EAL4
FIPS 140. Será reconocido como líder o competidores (challengers) dentro del cuadrante mágico de Gartner para el rubro de Enterprise Networks Firewalls, el más reciente divulgado a la firma del contrato.
Dentro del mismo Firewall contará con 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, SCCP/Skinny)
Servicios de Videoconferencia.
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).
Cross-Side Scripting.
Además de gusanos como Code Red, Nimda, bugbear, Slammer y otros.
Los ataques contra los que se protege serán actualizables en línea (vía Internet) y esta capacidad estará incluida e integrada dentro del mismo Firewall.
Dentro del mismo Firewall contará con detección de ataques a servicios Web implementados en:
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.
Detección de código ejecutable en tráfico HTTP.
Soportar el tráfico de Video RFC4582
Proteger Implementaciones de VoIP, soportando H323 en todas sus versiones, SIP. MGCP y SCCP.
Soportar implementaciones de Video, H.323 (H.239), SIP.
Basado en la tecnología conocida como "Stateful Inspection"
La comunicación entre los servidores de administración y los equipos, será cifrada y autenticada.
Método para bloqueo sobre mensajería instantánea de al menos las siguientes opciones:
video.
voz
aplicaciones compartidas
transferencia de archivos
asistencia remota
Protección a los clientes de ataques IP-spoofing.
Métodos de Autenticación

Métodos de autentificado por usuario y cliente para el firewall.

Autentificación para los usuarios que no utilicen plataforma de Windows, además de dispositivos móviles.

Métodos necesarios para la identificación de los usuarios sin agente y haciendo búsquedas en el Directorio activo o portal cautivo.

Autenticar sesiones para cualquier servicio; es decir cualquier protocolo y/o aplicación que se ejecuten bajo los protocolos TCP/UDP/ICMP

Control de acceso que incluya el soporte de al menos 1000 aplicaciones, servicios y protocolos predefinidos

Integración con Directorio Activo u Open LDAP para crear reglas de control de aplicaciones por:

Usuarios,
Grupos de Usuarios,
Equipos de cómputo,
Dirección IP,
Redes
Y todas las opciones combinadas.

Soportará al menos los siguientes esquemas de autenticación de usuarios:

Tokens
TACACS+
RADIUS, password del sistema operativo
Password propio del Firewall
Directorio LDAP
Certificados digitales o dispositivos biométricos
SSH, SSL/TLS
Nativo IPsec
VPN

Soporte para esquemas VPN site-to-site en topologías "Full Meshed" (todos-contra-todos), Estrella (oficinas remotas hacia una oficina central), "Hub and Spoke" (tráfico entre oficinas remotas, pasando por inspección central), además de VPNs client-to-site (VPNs de Acceso Remoto).

VPNs SSL sin cliente para acceso remoto, soportando al menos el número de usuarios requeridos por SHF según el "Anexo VIII. Matriz de Servicios".

Soporte para que se puedan establecer VPN usando clientes tipo L2TP.

Conexión de dispositivos móviles soportando al menos las siguientes plataformas: IOS, Android, y Windows.

Algoritmos de cifrado simétrico: AES (128, 196, 256) bits, DES, 3DES.

Algoritmos de llave pública: RSA, Diffie-Hellman.

VPNs SSL debiendo ser capaz la solución de verificar la legitimidad del cliente remoto efectuando un escaneo del equipo, pudiendo detectar aplicaciones maliciosas como malware y spyware, impidiendo el acceso del usuario en caso de que se detecten dichas aplicaciones.

CA Interna o una CA externa provista por un tercero.

Integración con certificados digitales (PKI) de terceros, que cumplan con los estándares X.509, PKCS #11 y PKCS #12, para no-repudiación de transacciones por VPN.

Integrar 4 diferentes autoridades certificadoras.

VPNs tipo "domain based" y "route based", usando al menos BGP y OSPF.

Aplicación de reglas de control de tráfico, al interior de la VPN.

Compresión de datos, tanto para las VPNs site-to-site como para las VPNs client-to-site realizadas con los clientes propios.

Doble factor de autenticación e incluir todo lo necesario en hardware, software y licenciamiento según las especificaciones del "Anexo VIII. Matriz de Servicios".

Los dispositivos móviles (smartphone y tabletas) contarán con su propio portal de acceso

Mecanismo de inyección de rutas (RIM) para la propagación del dominio de encriptación a través de ruteo dinámico.

Mecanismo que permita seleccionar qué enlace utilizar para tráfico de VPN entrante y saliente, además de escoger la mejor ruta para dicho tráfico.

Manejo de nombres para los servidores de aplicaciones.

Soportar al menos el número de usuarios con base a los requerimientos de SHF descritos en la Matriz de servicios.

Administración, integración y reporteo

Administración de forma centralizada a través de una sola consola de administración y monitoreo de políticas de firewall, VPN y QoS, en un solo equipo central con funcionalidades de monitoreo en tiempo real y reporteo, dicha consola será independiente para SHF.

Capacidad de definir administradores con diversos roles, con distintos permisos dentro de la consola para poder delegar funciones administrativas.

Autenticación fuerte (certificados) de manera nativa en la solución, para los administradores de la consola.

Seguimiento a los cambios realizados en las políticas de seguridad, de modo que sea posible revisar qué administrador hizo qué modificaciones, así como fecha, origen e impacto de la modificación.

Generar bitácoras, que permitan obtener fácilmente un reporte completo del estado de la seguridad de la red.

Interface gráfica de usuario (GUI), para hacer administración de la solución; además de una interface basada en línea de comando.

Interface basada en Web para el acceso remoto considerando que la comunicación será cifrada vía SSL al dispositivo firewall.

Se proporcionará al menos tres cuentas de solo lectura para el personal responsable que SHF designe.

Instalación la interface gráfica, en un equipo diferente de la consola central de administración para realizar administración remota, como en la consola misma.

Realizar una integración transparente y certificada con directorios tipo LDAP.

Soportar una autoridad certificadora interna que pueda emitir certificados para comunicación segura entre consola de administración y dispositivo de control de acceso.

Revisión de bitácoras en tiempo real.

Generar versiones de la política de seguridad, y poder regresar a versiones anteriores de la misma.

Administración remota a través de CLI, SSH, SSHv2, SSL, SNMP V3, HTTP y Serial.

Monitoreo en tiempo real del tráfico circulando por todos los Firewalls, sesiones y estado de cada equipo.

Realizar mediciones de conexiones por segundo, conexiones concurrentes y paquetes por segundo que están pasando a través del firewall y desplegarlas a cualquier usuario en tiempo real desde la interface de administración.

Generar reportes sobre el estado de los componentes, tráfico de red, y de las políticas de Firewalls; además de poder personalizar dichos reportes y desplegar varios tipos en una sola ventana.

Presentar reportes del estado de Túneles de VPN en tiempo real y en reportes históricos.

Graficar en tiempo real los "top N" de los servicios más utilizados y de los equipos que más están consumiendo recursos.

Generar acciones y/o alertas en función de determinados eventos como cambios de políticas o valores críticos en contadores como uso de al menos CPU, Memoria% de espacio libre en disco y sesiones por segundo y concurrentes.

Monitoreo y reacción sobre comportamiento de usuarios, detectando actividades sospechosas como intentos de acceso no autorizados, permitiendo el bloqueo de las conexiones detectadas.

Realizar actualizaciones centralizadas del software, de forma remota.

Hacer actualizaciones de software tipo "One-Click" en tiempo real.

Hacer actualizaciones de software de firewalls sin importar que la versión sea menos reciente que la actual versión de la consola de administración.

Envío de eventos como mínimo por SNMP v3.

Diferenciar entre logs de usuarios regulares y logs propios de la administración.

Asociar cada IP correspondiente a usuarios internos con su correspondiente nombre de usuario tomando esa información del Active Directory, sin necesidad de instalar ninguna aplicación en el Domain Controller ni en las PCs de los usuarios.

Grabar las vistas de tráfico y contadores del sistema a un archivo, para posteriormente poder verlo en cualquier momento.

Reconocer funcionamientos inadecuados y problemas de conectividad entre dos puntos conectados a través de una VPN, alertar y crear logs cuando el túnel de VPN se encuentre abajo.

Visión de las políticas de seguridad a través de un navegador que permita: administrar logs y usuarios dando acceso a gerentes y auditores sin necesidad de tener acceso total a la consola. Se Proporcionará al menos tres cuentas de solo lectura para el personal responsable que SHF designe.

Forzar al administrador a que deba requerir la aprobación del personal responsable que SHF designe antes de permitir la instalación de políticas.

Sistema de control de cambios integrado.

Generar reportes de cambios realizados durante una sesión, para control del administrador y de los auditores

.En el Apartado Firewall se describe la solución propuesta.

Servicio de IPS

OPERBES, S.A. DE C.V. considera para esta solución de equipos de propósito específico solo con la tecnología de IPS para protección de ataques orientados a conexiones internas y externas.

Características técnicas

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

Basado en hardware para hacer inspección a profundidad, no será únicamente 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.

Si el rendimiento de los equipos se encuentra entre el 70% y 85% promedio de su desempeño (tomando como métricas de desempeño el uso de CPU y Memoria), durante 10 días hábiles consecutivos, OPERBES, S.A. DE C.V. ampliará la capacidad de dicho rendimiento, sin la necesidad de cambiar por un hardware nuevo y sin costo para SHF. Aplica únicamente para el desempeño del equipo asociado al servicio.

Si el rendimiento (medido en base al uso de memoria y CPU) es mayor del 85% promedio durante 3 días hábiles consecutivos de operación normal, OPERBES, S.A. DE C.V. remplazará el equipo, por la siguiente categoría, en un plazo no mayor a tres días hábiles, el monto del cambio de equipamiento será cubierto por SHF en base a la lista de precios unitarios proporcionada por OPERBES, S.A. DE C.V., esto aplica únicamente para el caso de cambio de equipamiento.

La siguiente tabla muestra las características generales que OPERBES, S.A. DE C.V. consideró para la tecnología de IPS.

CAPACIDAD	Throughput Real	Sesiones Concurrentes	Interfaces
I	10 a 12 Gbps	3,000,000 a 5,000,000	6-10/100/1000
II	6 a 8 Gbps	1,500,000 a 4,000,000	4-10/100/1000
III	1 a 5 Gbps	500,000 a 1,000,000	4-10/100/1000
IV	500 a 800 Mbps	200,000 a 450,000	3-10/100/1000
V	200 a 450 Mbps	50,000 a 150,000	2-10/100/1000

Tabla: 3.2.1

Características Técnicas

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

Latencia bajo carga de red menor a 150 microsegundos.

HA en modos activo-activo y activo-pasivo.

Modo activo-activo.

Los IPS tipo I y II soportarán interfaces 10G y estarán disponibles en caso de que SHF lo requiera al inicio del proyecto o bajo demanda.

Alta disponibilidad en modo de protección y simulación.

Opción de permitir el paso del fráfico 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:

Pérdida de energía eléctrica

Falla lógica en la interface de control,

Pérdida de conectividad con la tarjeta madre del dispositivo.

Colapso del sistema operativo.

Ruteo asimétrico, además de soportar el monitoreo de redes MPLS.

VLANs, incluyendo frames 802.1q y Sensores Virtuales internamente en el equipo.

Políticas de seguridad específicas de acuerdo a la posición de la plataforma de IPS en la red y de que dispositivos estará protegiendo (Core, Perímetro, DMZ).

Interface de monitoreo en modo stealth, sin stack de TCP/IP en la interfaz.

No requerirá la modificación de los routers o switches para su implementación, funcionando como un puente en la red.

Interfaces de red necesarias para su operación protegiendo todas las zonas del Firewall (LAN, WAN, DMZ).

Translación de VLANs. Es decir la capacidad de inspeccionar y traducir el tráfico entre diferentes VLAN o interfaces VLAN.

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.

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.

Contará con las siguientes certificaciones:

Certificación de NSSLabs

Está reconocido como líder dentro del cuadrante mágico de Gartner para el rubro de Network Intrusion Prevention Systems 2012.

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.

Realizará un monitoreo transparente para los usuarios donde de forma automática bloquee ataques maliciosos y preservando la disponibilidad del ancho de banda de red.

Filtros/firmas en modo bloqueo sin necesidad de periodos de aprendizaje ni afinación por parte del operador.

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.

Inspeccionará simultáneamente cargas útiles tanto en IPv4 como en IPv6.

Inspeccionará IPv6 con VLANS y MPLS.

Inspección de tráfico IPv4 para Redes Móvites (2G/3G/4G). La inspección de tráfico se realizará sobre equipos con tecnologías 2G/3G/4/G conectados a la red inalámbrica de SHF

Basado en la tecnología conocida como "Stateful Inspection".

Funcionamiento activo semejante al de prevención en línea, pero sin bloquear tráfico. Sólo alerta que eventos serían bloqueados.

Creación de reglas y filtros de acceso, por Adaptador, VLAN, Protocolo, Origen y Destino.

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.

Protección para servidores Web contra ataques de inyección de SQL.

Tecnología de detección de Reputación de Archivos, IP, aplicaciones y protocolos.

Detección de ataques independiente del sistema operativo.

Se mostrará para cualquier evento el origen y el destino del ataque o incidente de seguridad.

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).

Protocolos y tipos de archivos los cuales de mencionan de manera enunciativa mas no limitativa:

SIP
IP
TCP
UDP
Java script
HTML
MSRPC, HTTP

Detección de ataques desconocidos o variaciones de ataques conocidos a partir de firmas basadas en vulnerabilidades.

Reensamblado de paquetes y sesiones fragmentadas.

Detección de anomalías de tráfico a partir de análisis estadístico.

Operará sobre firmas definidas por el usuario mediante el uso de expresiones regulares.

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

Activará la captura de paquetes para protecciones específicas con el fin de tener análisis forenses.

Bloqueará propagación de gusanos, virus, backdoors, port sweep, port scanning, troyanos, previniendo la infección de otros equipos y consumo de ancho de banda.

Reconocerá anomalías de tráfico como: umbrales de protocolos (paquetes, bytes, conexiones, etc.), análisis de patrones de tráfico, análisis de paquetes anormales.

Protección para sistemas SCADA y tener la capacidad de proteger al menos los siguientes protocolos como DNP3, MODBUS, ICCP, MMS.

Protección contra ataques en capas aplicativas contra PHP (include, inyección, evasión etc.), Cross Site Scripting y filtros contra inyección de SQL.

Filtros contra ataques VoIP incluyendo los protocolos SIP, H225, H323, Skinny, MGCP y servicios de Videoconferencia.

Técnicas de detección basadas en anomalías de protocolos.

Detección de ataques DOS/DDoS.

Detectará y protegerá contra anomalías estadísticas, protocolos y aplicaciones.

Protección contra ataques de inundaciones de conexiones establecidas y conexiones por segundo.

Capacidad de realizar los siguientes filtros:

Plataforma Oracle

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

Instalarse y proteger contra ataques en ambientes asimétricos.

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

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

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.

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

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

Detectará anomalías o fragmentaciones ilegales en los protocolos y paquetes de Video.

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

Administración, Integración y Reporteo

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

Integración de Syslog (número ilimitado de dispositivos).

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

Correlación de datos de vulnerabilidades.

Comunicación de datos en forma cifrada.

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 al Licitante.

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

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.

Arquitectura modular, distribuida y multicapa.

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

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

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.

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.

Realizará automáticamente actualizaciones de software vía remota o Web para asegurar una protección en tiempo real. Las actualizaciones aplicadas no deben requerir de la reinicialización del equipo.

Proveerá información adicional sobre el evento recibido con una descripción del ataque y una liga de referencia.

Mandará un TCP Reset asociado con un evento.

Proporcionará reportes de los TOP más significativos de tráfico.

En el Apartado IPS se describe la solución propuesta.

Servicio de WAF (Firewall para Aplicaciones Web)

OPERBES, S.A. DE C.V. considera 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. El servicio será a solicitud de SHF.

Características Generales

La tecnología incluirá y operará al menos con las siguientes características.

Medidas de seguridad a nivel de los flujos de transacciones HTTP y HTTPS de los servicios públicos en internet, sobre la capa de Aplicación.

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.

Si el rendimiento de los equipos se encuentra entre el 70% y 85% promedio de su desempeño (considerando como métricas de desempeño el uso del CPU y memoria), durante 10 días hábiles consecutivos, OPERBES, S.A. DE C.V. ampliará la capacidad de dicho rendimiento, sin la necesidad de cambiar por un hardware nuevo y sin costo para SHF en un plazo no mayor a tres días hábiles. Aplica únicamente para el desempeño del equipo asociado al servicio.

Si el rendimiento (medido en base al uso de memoria y CPU) es mayor del 85% promedio durante 3 días hábiles consecutivos de operación normal, en el horario de las 10:00 a las 19:00 horas, OPERBES, S.A. DE C.V. remplazará el CPE, por la siguiente categoría, en un plazo no mayor a tres

días hábiles, el monto del cambio de equipamiento será cubierto por SHF en base a la lista de precios unitarios proporcionada por OPERBES, S.A. DE C.V., esto aplica únicamente para el caso de cambio de equipamiento.

TIPO	Throughput	Transacciones por segundo
I	1.5 a 2 Gbps	50,000 a 70,000
II	800 Mbps a 1 Gbps	30,000 a 40,000
III	300 a 500 Mbps	15,000 a 25,000

Tabla: 3.3.1

Características Técnicas

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

Las soluciones tipo I y II contarán con fuentes de poder redundantes.

Con las siguientes Opciones de implementación:

Capa 2 de manera transparente para un mejor desempeño

Proxy inverso y proxy transparente

Fuera de Línea con la finalidad de mantener monitorización y análisis

Alta disponibilidad

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.

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

Inspeccionará y auditará trafico SSL identificando errores de aplicación.

Inspeccionará y auditará todo el tráfico HTTP identificando errores de aplicación.

Hacerá balanceo de cargas para los servidores de aplicaciones en diferentes redes (capa 3).

Mitigación de ataques automatizados como robots, a gran escala con la capacidad de bloquear de manera rápida y precisa las conexiones sospechosas.

Listas Blancas/Negras de URL´s e IP's , para inspeccionar o bloquear peticiones a URL´s e IP´s especificas

Reputación de IPs y geolocalización.

Normalización de datos codificados.

Generará eventos y alertas pero que no realice ningún bloqueo real, para facilitar la afinación y prueba de nuevas políticas.

Creación de políticas de seguridad usando como criterio cualquier combinación de la menos los siguientes elementos:

URL
HTTP
Header HTTP
Response
País de origen
Usuario Web
Cookies
Tiempo y tamaño de la respuesta HTTP.

Soportar al menos los siguientes métodos de autentificación

De doble factor

LDAP Directorio Activo
Certificación de clientes SSL
Métodos de HEALTH CHECK tales como:
PING
ICMP
HTTP
Interfaz de usuario web HTTP, HTTPS.
Registro y monitorización SNMP
Syslog
Notificaciones vía correo electrónico
Capacidad de graficar
Consola de eventos en tiempo real
Al menos contará con la certificación ICSA LABS de WEB APPLICATION FIREWALL (WAF)
Administración, integración y reporteo
Administración por SSH, CLI, HTTPS SNMP v3 proporcionando al menos tres cuentas de solo lectura para el personal responsable que SHF designe.
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 día, 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.
Proporcionaár 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 éste reporte en un componente distinto del servicio WAF
Top por severidad
Top por acción tomada por el equipo
En el Apartado WAF se describe la solución propuesta
Servicio Multifuncional de Seguridad Perimetral
OPERBES, S.A. DE C.V. ofrecerá una solución que permita la protección a los recursos de internet con las características de un equipo multifuncional (UTM) el cual incluirá filtrado web, IPS, DLP, Control de Aplicaciones y Control de Ancho de Banda; con la finalidad de proteger las redes de SHF.
Esta tecnología será totalmente adaptable a las necesidades de seguridad de SHF y se administrará, en su totalidad centralizadamente desde una única consola, con la finalidad de reducir al máximo posible la complejidad y sobrecarga operacional.
Dicha solución será 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 contemplerá al menos los siguientes módulos de seguridad y administración: Firewall, IPS, Filtrado web, control de aplicaciones, control de ancho de banda, anti malware 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 incluirá y operará al menos con las siguientes características.
Si el rendimiento de los equipos se encuentra entre el 70% y 85% promedio de su desempeño (tomando como métricas de desempeño el uso de CPU y Memoria), durante 10 días hábiles consecutivos, OPERBES, S.A. DE C.V. ampliará la capacidad de dicho rendimiento, sin costo adicional para SHF, en un plazo no mayor a tres días hábiles. Aplica únicamente para el desempeño del equipo asociado al servicio.
Si el rendimiento (medido en base al uso de memoria y CPU) es mayor del 85% promedio durante 3 días hábiles consecutivos de operación normal, en el horario de las 10:00 a las 19:00 horas, OPERBES, S.A. DE C.V. remplazará el CPE, por la siguiente categoría, en un plazo no mayor a tres

días hábiles, el monto del cambio de equipamiento será cubierto por SHF en base a la lista de precios unitarios proporcionada por OPERBES, S.A. DE C.V., esto aplica únicamente para el caso de cambio de equipamiento.

Integrará el soporte a la tecnología de aceleración por hardware.

Soportará Alta disponibilidad en sus modos Activo-Activo o Activo-Pasivo.

La solución contará con las siguientes certificaciones:

ICSA

Common Criteria EAL4 o superior

FIPS 140 –Level 2 o superior

Está 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.

Para las soluciones tipo I y II según la tabla 2.13.4.1. Soportará y operará con al menos las siguientes tecnologías de red: Ethernet, Fast Ethernet, Gigabit Ethernet y 10G Ethernet.

La siguiente tabla muestra las capacidades que se consideraron para dimensionar dicha tecnología.

TIPO	Throughput	Memoria	Sesiones Concurrentes	Interfaces
I	6 a 8 Gbps	2 A 4 GB	1,500,000	8-10/100/1000
II	2 a 5 Gbps	1 A 2 GB	800,000	6-10/100/1000
III	500 Mbps a 1 Gbps	500 a 800 MB	300,000	4-10/100/1000
IV	50 a 250 Mbps	128 a 256 MB	150,00	2-10/100/1000

Tabla: 3.4.1

Módulo Firewall

El módulo incluirá y operará al menos con las siguientes características:

Tecnología de QoS basada en colas inteligentes, Diffserv, TOS.

Capacidad de integración transparente de tráfico marcado (diferenciado) en redes MPLS.

Monitoreo gráfico en tiempo real del tráfico de QoS que está circulando por el equipo.

Modificar el MTU para evitar problemas de fragmentación de paquetes encriptados

Soportar valores de MTU mayores a 1500 bytes, para incrementar el rendimiento de interfaces gigabit, permitiendo modificar el MSS

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.

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)

Cross-Side Scripting

Además de gusanos como Code Red, Nimda, bugbear, Slammer y otros.

Los ataques contra los que se protege serán actualizables en línea (vía Internet) y esta capacidad estará incluida e integrada dentro del mismo Firewall.

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:

Video

Voz

Aplicaciones compartidas
Transferencia de archivos
Asistencia remota
Protegerá a los clientes de ataques IP-spoofing.
Basado en la tecnología conocida como "Stateful Inspection"
Protegerá implementaciones de VoIP, soportando en todas sus versiones, SIP. MGCP, SCCP y servicios de Videoconferencia.
Contará con el licenciamiento necesario para la activación de los siguientes protocolos de enrutamiento en IPv4 e IPv6: RIP, OSPF, BGP y MULTICAST para IPv4.
Protocolos LAN: 802.3ad, 802.1q
Tecnología IPv6; Dual Stacking firewall y VPN, Túneles IPv4 desde IPv6.
La solución contará con terminadores de túneles VPN y traducción de direcciones (NAT, PAT).
Implementará y operará reglas aplicadas a intervalos de tiempo específicos.
Controlará los accesos por medio de políticas específicas.
Almacenará una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
Integrará la solución con Directorio Activo u Open LDAP para crear reglas de control de aplicaciones en usuarios, grupos de Usuarios, maquinas, dirección IP, redes y todas las opciones combinadas
Conectarse en modo transparente (bridged mode).
Controlar el acceso a archivos compartidos de Microsoft usando CIFS.
Poner en cuarentena a equipos que se consideren maliciosos a través de la política del firewall.
Mecanismos de alarmas y avisos, ante violaciones a políticas o eventos del sistema.
Módulo de Filtrado de Contenido
El módulo incluirá y operará al menos con las siguientes características
Basado en categorías y se podrá incluir como un bloque más.
Permitirá únicamente el tráfico explícitamente autorizado por SHF hacia Internet.
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
Las URL's estarán clasificadas según su contenido diario, es decir, en el caso de que el contenido de una URL sea cambiado, máximo en 24 horas naturales estará reclasificada bajo la categoría que refleje su nuevo contenido.
SHF podrán solicitar la reclasificación de URL's, las cuales serán ejecutadas en un máximo de 24 horas naturales.

Mecanismo que permitan al administrador, negar o permitir URL's específicos, que no necesariamente están definidos en una categoría, para poder ser utilizados en la definición de nuevas reglas

Bloqueo de páginas que pertenezcan a categorías permitidas, pero cuya URL posea ciertas palabras clave.

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.

Técnicas para detectar código malicioso en archivos que se estén descargando y cancelar la descarga, informándolo al usuario.

El servicio de navegación segura contendrá el análisis dinámico (en tiempo real) de contenido de sitios web

Opción de modificar la notificación de bloqueo, y re direccionar al usuario a otra página Bloquear granularmente sitios basados en Web 2.0.

Identificará y bloqueará herramientas de "proxy bypass" sobre protocolos estándar y no estándar (sin la necesidad de instalar un agente en los hosts o licencias adicionales)

Bloqueará Malware sobre sitios Web.

Método dinámico en la nube para la categorización de los sitios Web existentes y nuevos sitios emergentes.

Inspeccionará el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL. El módulo de Filtrado de URL hará dicha inspección como si fuera texto claro, sin la necesidad de utilizar herramientas de terceros, servidores, licencias adicionales o agentes.

Cifrar las autenticaciones de usuarios con: LDAP y AD.

Módulo de IPS

Opción de permitir el paso del tráfico en el segmento de red sin afectar el funcionamiento de la red (Bypass).

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.

La actualización de las nuevas definiciones de spyware, virus y variantes se aplicará sin interferir en la operación del equipo y sin necesidad de reiniciarlo.

Realizar un monitoreo transparente para los usuarios donde de forma automática bloquee ataques maliciosos y preservando la disponibilidad del ancho de banda de red.

Filtros/firmas en modo bloqueo sin necesidad de periodos de aprendizaje ni afinación por parte del operador.

Inspeccionar IPv6 con VLANS.

Inspección de tráfico IPv4 en dispositivos Móviles (2G/3G/4G).

Detectará y bloqueará tráfico peer-to-peer incluso si la aplicación utiliza cambio de puertos

Detectará y bloqueará aplicaciones que realicen control remoto incluyendo aquellas capaces de hacer Tunneling.

Funcionamiento activo semejante al de prevención en línea, pero sin bloquear tráfico. Sólo alerta que eventos serían bloqueados.

Creación de reglas y filtros de acceso, por Adaptador, VLAN, Protocolo, Origen y Destino.

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.

Protección para servidores Web contra ataques de inyección de SQL.

Tecnología de detección de Reputación de Archivos, IP, aplicaciones y protocolos

Detección de ataques independiente del sistema operativo.

Tendrá la información de contacto de los usuarios que están siendo atacados

Los eventos de seguridad mostrados revelarán el usuario que está generando o recibiendo el ataque y generar una alerta o tomar acciones en base al perfil del usuario en cuestión.

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).

Protocolos y tipos de archivos soportados los cuales de mencionan de manera enunciativa mas no limitativa:

SIP
IP
TCP
UDP
Java script
HTML

Detección de ataques desconocidos o variaciones de ataques conocidos a partir de firmas basadas en vulnerabilidades.

Reensamblado de paquetes y sesiones fragmentadas.

Detección de anomalías de tráfico a partir de análisis estadístico.

Operará sobre firmas definidas por el usuario mediante el uso de regular expressions.

Activará la captura de paquetes para protecciones específicas con el fin de tener análisis forenses.

Bloqueará propagación de gusanos, virus, backdoors, port sweep, port scanning, troyanos, previniendo la infección de otros equipos y consumo de ancho de banda.

Reconocerá anomalías de tráfico como: umbrales de protocolos (paquetes, bytes, conexiones, etc.), análisis de patrones de tráfico, análisis de paquetes anormales.

Protección para sistemas SCADA y tener la capacidad de proteger al menos los siguientes protocolos como DNP3, MMS.

Protección contra ataques en capas aplicativas contra PHP (include, inyección, evasión etc.), Cross Site Scripting y filtros contra inyección de SQL

Filtros contra ataques VoIP incluyendo los protocolos SIP, H323, Skinny, MGCP y servicios de Videoconferencia.

Técnicas de detección basadas en anomalías de protocolos.

Detectar y proteger contra anomalías estadísticas, protocolos y aplicaciones

Ofrecer protección contra ataques de inundaciones de conexiones establecidas y conexiones por segundo.

Instalarse y proteger contra ataques en ambientes asimétricos

Podrá soportar trafico IP de-fragmentado y tendrá la capacidad de reensamblar los paquetes antes de enviarlos a su destino

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.

Módulo de Control de Aplicaciones

El módulo incluirá y operará al menos con las siguientes características

Controlar y bloquear en tiempo real aplicaciones independientemente del puerto que utilicen.

Identificará, autorizará, bloqueará y limitará el uso de aplicaciones. Contará con una base de datos mínimo 1000 aplicaciones.

Controlará y bloqueará al menos las siguientes aplicaciones; las cuales se mencionan de manera enunciativa más no limitativa:

BOTNET
ECONÓMIA Y NEGOCIOS
MENSAJERIA INSTANTANEA
EMAIL
JUEGOS
MEDIA
SOCIAL MEDIA
NETWORK-SERVICE
P2P
PROXY
ACCESO REMOTO
VOIP
WEB
UPDATE

El control y bloqueo de protocolos permitirá la definición de políticas mínimo por usuario, grupo y rango de direcciones IP.

Controlará y bloqueará las siguientes excepciones de los protocolos:

Creación de protocolos personalizados.

Soportar la apertura de otros puertos cuando sea requerido 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

Contener descifrado de SSL/HTTPS para revisión del contenido.

Módulo de Control de Ancho de Banda

El módulo incluirá y operará con al menos las siguientes características

Asignará parámetros de "traffic shapping" por usuario, grupo, dirección IP, rango de direcciones IP, categoría, aplicación.

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.

Priorizar el tráfico por categoría, contenido web, IP o grupos de IP's para las aplicaciones críticas definidas por SHF, garantizando el ancho de banda.

Asignar ancho de banda por aplicación controlando el tráfico por tipo de prioridad.

Módulo de Prevención de Fuga de Información Perimetral (DLP)

Será 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

Trabajará 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.

Se integrará la solución con directorio activo y base de datos de LDAP.

Proveerá visibilidad de la situación actual de la red, mostrando eventos de seguridad importantes asociados a los sistemas críticos de la organización.

Contará 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.

La solución se instalará en el mismo equipo Firewall como una solución integrada.

Contará 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.

Soportará categorías de tipos de datos y grupos de tipos de datos.

Creará 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

Definirá umbrales de coincidencias, es decir que rebasando cierto número de incidencias el DLP tomará la acción definida en la política.

Soportará definición propia de datos

Hará inspección recursiva de contenido de archivos como: zip, RAR, tar, etc.

Definirá un tamaño máximo de archivo que pueda ser procesado por detección de contenido

Identificará tráfico HTTP/HTTPS sobre puertos no estándar.

Permitirá manejo de cuotas por incidentes, para al menos los protocolos SMTP, HTTP, HTTPS y FTP.

Permitirá cambiar o modificar las notificaciones hacia el usuario.

Podrá definir acciones, para los protocolos HTTP, HTTPS, FTP y SMTP, que permitan la continuidad de la operación bajo condiciones extremas de carga.

Definirá tipos de datos, basado en los atributos de un tipo de archivo, por ejemplo atributos específicos Office, vCalendar, Open Office, Quatro, Corel Draw, etc.

Módulo de Antivirus y Antispyware de Internet

El módulo incluirá y operará con al menos las siguientes características:

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.

Se basará en patrones previniendo contra software espía y gusanos.

Permitirá al administrador elegir la acción (block o pass) para al menos 50 diferentes tipos de archivos. La detección del tipo de archivo no será basada en la extensión del mismo.

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.

Escanear archivos de cualquier tamaño aun comprimidos con la opción de configurar un tamaño más pequeño de archivo. El administrador podrá decidir el límite de tamaño de archivo antes de bloquearlo, o pasarlo sin ningún tipo de scan.

Descompresión de archivos, con la opción de poder configurar el máximo nivel de anidación y de compresión para evitar ataques DoS.

Ofrecerá al administrador la posibilidad de decidir qué tipos de archivos pueden usar las descargas continuas, y cuáles será escaneados, en su totalidad, antes de iniciar la transferencia al cliente.

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.

Escaneo en tiempo real tanto de antivirus como de antimalware.

Tomará acciones cuando el escaneo de archivos falle o haya sobre carga en el motor de antivirus.

Inspección sobre tráfico encriptado y descifrar los protocolos PPTP, L2TP, IPSec, SSL

Detección host infectados con bots, analizando el tráfico de la red utilizando una tecnología multicapa.

Módulo de identificación

Proveerá una forma de autentificación para los usuarios que no utilicen plataforma de Windows, además de dispositivos móviles.

Proveerá configuración de acceso basado en tiempo para que los usuarios puedan entrar a los recursos de la red.

Distinguir entre cuentas de servidores de aplicación y cuentas de usuario.

Método de integración con el directorio activo sin usar las credenciales del administrador.

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

Retener la identidad de los usuarios aun cuando estos cambien la dirección IP.

Solicitar a los usuarios la re autentificación después de un intervalo de tiempo.

Verificar el estado de los controladores de dominio vía consola de comandos.

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.

Integración con otras soluciones como: control de aplicaciones y filtrado de URL

VPN´S IPSEC Y SSL

VPNs SSL sin cliente para acceso remoto, soportando al menos el número de usuarios requeridos por SHF según el "Anexo VIII. Matriz de Servicios".

Soportar túneles IPSEC de tipo sitio a sitio.

Soportar los sistemas operativos Windows en todas sus versiones a 32 bits y 64 bits, IOS y Android.

Soportar certificados PKI para la construcción de VPN´S cliente a sitio.

Soportar algoritmos de cifrado: AES, DES y 3DES.

Soportar distintos portales SSL que sirvan como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la plataforma.

capacidad de restringir las aplicaciones que pueden ser ejecutadas en el escritorio virtual.

Soportará al menos el número de usuarios con base a los requerimientos de SHF descritos en la Matriz de servicios.

Módulo de Administración, Integración y Reporteo

Se incluirá y operará con al menos las siguientes características

Administración de forma centralizada a través de una sola consola de administración y monitoreo de políticas de Firewall, Filtrado, Control de Aplicaciones, Control de ancho de banda, IPS antimalware/antispyware y protección contra fuga de información; en un solo equipo central con funcionalidades de monitoreo en tiempo real y reporteo independiente para SHF.

Capacidad de definir administradores con diversos roles, con distintos permisos dentro de la consola para poder delegar funciones administrativas

Autenticación a través de certificados de manera nativa en la solución, para los administradores de la consola

Seguimiento a los cambios realizados en las políticas de seguridad, de modo que sea posible revisar qué administrador hizo qué modificaciones, así como fecha, origen e impacto de la modificación.

Generará bitácoras, que permitan obtener fácilmente un reporte completo del estado de la seguridad de la red

Interface gráfica de usuario (GUI), para hacer administración de la solución; además de una Interface basada en línea de comando

Interface basada en Web para el acceso remoto considerando que la comunicación será encriptada vía SSL al dispositivo.

Instalará la interface gráfica, tanto en equipo diferente de la consola central de administración para realizar administración remota, como en la consola misma.

Integración transparente y certificada con directorios tipo LDAP.

Autoridad certificadora interna que pueda emitir certificados para comunicación segura entre consola de administración y dispositivo de control de acceso.

Revisión de bitácoras en tiempo real.

Generar versiones de la política de seguridad, y poder regresar a versiones anteriores de la misma.

Administración remota a través de CLI, SSH, SSHv2, SSL, SNMP V3, HTTP y Serial

Monitoreo en tiempo real del tráfico circulando a través de los módulos administrados, monitoreo de sesiones además de monitorear el estado de cada uno de los puntos de refuerzo que se encuentren en toda la red, en tiempo real.

Mediciones de conexiones por segundo, conexiones concurrentes y paquetes por segundo que están pasando a través del equipo y desplegarlas al usuario administrador en tiempo real desde la interface de administración (no mediante línea de comando)

Generará reportes sobre el estado de los componentes, tráfico de red, y de las políticas del dispositivo; además de poder personalizar dichos reportes y de poder desplegar varios tipos de reportes en una sola ventana

Graficará en tiempo real de los "top N" servicios más utilizados y de equipos que más están consumiendo ancho de banda

Generará acciones y/o alertas en función de determinados eventos como cambios de políticas o valores críticos en contadores como uso de al menos CPU, Memoria, y Disco.

Monitoreo y reacción sobre comportamiento de usuarios detectando actividades sospechosas como intentos de acceso no autorizados permitiendo el bloqueo de las conexiones detectadas

Realizará actualizaciones centralizadas del software, de forma remota.

Hará actualizaciones de software tipo "One-Click" en tiempo real

Hará actualizaciones de software de firewalls sin importar que la versión sea menos reciente que la actual versión de la consola de administración

Envío de eventos como mínimo por SNMP

Diferenciará entre logs de usuarios regulares y los logs propios de la administración.

Realizará un cambio automático de logs, basados en programaciones de tiempo o del tamaño del archivo.

Asociará 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.

Por cada coincidencia de una regla, se podrá configurar alguna de las siguientes opciones: Log, Alert, Send and SNMP trap, send and email

Proveerá al menos la siguiente información por cada equipo: Sistema Operativo, Uso de Memoria, CPU.

Proveerá el status de cada uno de los componentes del equipo (firewall, VPN, cluster, antivirus, etc.).

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. tendrá la opción de generar gráficas personalizadas.

Grabará las vistas de tráfico y contadores del sistema a un archivo, para posteriormente poder verlo en cualquier momento.

Posibilidad de ver las políticas de seguridad a través de un navegador, administrar logs y usuarios dando acceso a gerentes y auditores sin necesidad de tener acceso total a la consola, proporcionando al menos tres cuentas de solo lectura para el personal responsable que SHF designe

Programar backups en uno o más gateways.

Incluirá un sistema de control de cambios integrado al servidor de administración.

Generará reportes de cambios realizados durante una sesión, para control del administrador y de los auditores

La solución propuesta se describe en el Apartado UTM

Servicio de Protección Contra Malware

OPERBES, S.A. DE C.V. Ofrece de una solución que permitirá proteger y neutralizar los ataques desde y hacia Internet a través de la inspección profunda de paquetes, descartando las amenazas conocidas basadas en firmas, aplicando heurística agresiva en busca de objetos Web maliciosos y códigos ejecutables de manera que permita examinar, capturar y confirmar la existencia del malware de día cero y ataques específicos, evitando en lo posible los falsos positivos y falsos negativos, corriendo el malware sospechoso en un ambiente controlado Sandbox local que permitirá simular el impacto de la amenaza que pudiera descargarse en los dispositivos finales de SHF.

Para dicha solución se contemplará al menos lo siguiente:

TIPO	Objetos por día
I	100,000
II	80,000
III	60,000

Tabla: 3.5.1

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

Se considera una caja de propósito específico dedicado a proporcionar protección contra los ataques como descargas de archivos maliciosos y malware conocido y de día cero.

Ejecutará código sospechoso, adjuntos, URL's y diversos tipos de archivos en un entorno de inspección Sandbox que evalúe los ataques de tal manera que permita identificar los falsos positivos. podrá crear imágenes de sandbox con los sistemas operativos y las aplicaciones que utiliza la institución, el cual también puede procesar muestras enviadas de forma manual.

El posible malware detectado será inspeccionado y examinado en el sandbox, permitiendo la ejecución de ataques conocidos y de día cero, escalación privilegios y funciones de ataque de nueva generación.

El sandbox será local y controlado por SHF que así lo requieran, respetando la confidencialidad de los datos analizados.

Registrar y almacenar evidencia de la ejecución de malware en el sandbox proporcionando la siguiente información:

Direcciones IP

Protocolos empleados

Puertos utilizados por el malware

Proceso de ejecución y comunicación del malware

El sandbox será capaz de emular el comportamiento del malware como si se tratara del equipo host comunicándose a los servidores web que intentan infectar al equipo.

La solución será capaz de analizar al menos lo siguiente:

Archivos Ejecutables

Archivos Adobe PDF, Microsoft Word, Microsoft Excel, COM, EXE, entre otros.

Archivos comprimidos como son ZIP y RAR

Contará con la capacidad de mitigación y notificación vía correo electrónico en caso de la detección de incidentes graves. Soportará reglas estáticas de análisis.

El análisis virtual será capaz de entregar todos los hallazgos de malware en un archivo comprimido como evidencia y para posibles análisis forenses posteriores.

Contará con un servicio de actualización sobre nuevos hallazgos, que operará a nivel mundial y permitirá la sincronización entre dispositivos sobre el malware detectado.

Analizará repositorios de información compartidos de archivos en busca de documentos infectados con malware.

Permitir la inspección de diversos tipos de archivo como son PDF, documentos Office, archivos comprimidos, contenidos multimedia, entre otros.

Contará con la capacidad de notificar a un servicio de información en la nube sobre los nuevos hallazgos, permitiendo así contar con una base de conocimiento actualizada.

Administración y Reporteo

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.

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.

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.

Capacidad para generar reportes estándar y ejecutivos donde refleje la operación de la solución.

La solución propuesta se describe en el apartado PCMW

Servicio de Correlación

OPERBES, S.A. DE C.V. ofrece 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 realizazará la administración de toda la información de seguridad generada por todos los dispositivos de la infraestructura de red de distintos fabricantes y de OPERBES, S.A. DE C.V., 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 estará basada en una arquitectura escalable con capacidad de crecimiento en caso de requerirse la correlación de más dispositivos de la red y para dimensionamiento inicial tomó en cuenta al menos las siguientes características con base a las tablas.

Correlacionador de Eventos:

Tipo	Eventos por segundo sostenidos	Almacenamiento de Gestión
I	15,000	10 TB
II	10,000	10 TB
III	5000	10 TB

Tabla: 3.6.1

Tipo	Eventos por segundo sostenidos	Almacenamiento de Gestión
C-I	5,000	1 TB
C-II	2,000	1 TB
C-III	500	500 GB

Tabla: 3.6.2

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

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.

Contará con sistemas de tolerancia a fallas tales como fuentes de poder duales y configuración de arreglo de discos.

Correlación en tiempo real y en memoria sin necesidad de consultar la base de datos para este propósito.

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.

Configuración ilimitada de reglas de correlación.

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
Correo electrónico como: Microsoft Exchange 2003 o posteriores.
Aplicativos y bases de datos.
Servidores y estaciones de trabajo
Para otros dispositivos no listados o que la solución no soporte, permitirá el desarrollar integraciones de nuevos dispositivos.
Permitirá la normalización y categorización de eventos.
Cifrar la comunicación entre los módulos de colección de eventos y el correlacionador, en caso necesario.
Controlará el flujo de los eventos a través de la compresión, procesamiento y agregación, evitando la saturación de enlaces de datos y privilegiando el paso de eventos productivos.
El manejo y tratamiento de log's tendrá métodos de seguridad que permitan la inviolabilidad de la información y su auditoria en el momento en el que sea requerido.
Garantizará la integridad de los eventos, confidencialidad, disponibilidad y cadena de custodia a través de firmas digitales y marcas de tiempo, sellando el evento cada vez que pasa por un componente de la solución.
Proveerá la cadena de custodia desde la etapa de colección, proceso de análisis de eventos hasta los procesos de almacenamiento y retención de eventos.
Búsqueda rápida de eventos con la capacidad de realizar y combinar métodos de búsqueda para el análisis de eventos dentro una interfaz unificada.
Las alertas críticas serán generadas en tiempo real.
Auto auditar su estado de desempeño.
Realizará en tiempo real la correlación de eventos de los diferentes dispositivos o fuentes de información. En donde se analicen los eventos de interés recibidos por los colectores y pueda generar alertas de amenazas. Detectar los eventos de seguridad que generen falsos positivos y falsos negativos
Evaluará las amenazas que recolectan la información de los roles de usuarios, activos críticos, información de vulnerabilidades, información de zonas, exposición al ataque y listas de observación en tiempo real y en memoria, utilizando estos elementos para reducir los falsos positivos.
Identificará y rastreará comportamiento base de los eventos recibidos, identificando cualquier incremento en la actividad, ya sea del atacante, destino, protocolo o cualquier otro campo bajo un umbral de tolerancia
Antes de realizar la tarea de correlación agregará al evento información de contextualización, puntaje o 'score', como la siguiente:
Puntaje basado en la firma de severidad del evento.
Peso relativo con base a la ubicación del dispositivo que detecte o registre el evento.
Valor del activo
Vulnerabilidades del activo que pudieran ser detectadas a través de escaneos.
El módulo de correlación de eventos permitirá con base a reglas o aplicaciones de correlación que se ejecutarán de manera concurrente, el descubrir en sus etapas iniciales ataques, amenazas en el que al final se pueda comprometer la seguridad de un activo, intentos de intrusiones o ataques reales.
La solución tendrá la capacidad de poder importar la información de herramientas de detección de vulnerabilidades para modificar el riesgo asociado con cada entrada de ataque. El módulo de correlación soportará al menos las siguientes herramientas de vulnerabilidades:
Foundstone foundscan
Nessus
Permitirá la configuración de las funciones de los módulos de colección y correlación de eventos, las cuales serán enviadas a éstos módulos bajo el control del administrador u operador de la solución.

Realizará correlación en tres dimensiones teniendo la habilidad de unificar y correlacionar eventos, información proveniente de herramientas de análisis de vulnerabilidades y criticidad de los activos o dispositivos que permita eliminar falsos positivos y evaluar de forma dinámica el nivel de riesgo considerando los factores mencionados.

El motor de correlación estará basado en firmas de seguridad y detección de comportamiento anómalo mediante correlación estadística a través de cálculos de promedio, desviación y varianza.

Contará con un módulo integrado en el licenciamiento que permita realizar análisis histórico de datos, identificando patrones de comportamiento bajo distintos criterios mediante análisis heurístico y técnicas de minado de datos, permitiendo la definición de reglas de correlación que permitan detectar ataques de evasión así como ataques previamente desconocidos (de día cero).

Permitirá probar las reglas de correlación sobre eventos históricos con una ventana de tiempo configurable, que permitan afinar puntualmente las reglas de correlación previo a su despliegue en ambientes productivos.

Integrará en el proceso de análisis en tiempo real, eventos de correlación, es decir, adicional a los eventos base recibidos por los colectores de eventos, analizar los eventos de correlación previamente identificados, a fin de identificar amenazas o patrones más complejos.

Evaluación del nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores:

Importancia del evento

Criticidad del activo

Vulnerabilidades asociadas

Antecedentes previos sobre el origen, destino o ambos.

Se incluyen herramientas para el monitoreo gráfico sobre el uso y activación de las reglas de correlación.

Se utilizará un motor de almacenamiento propietario optimizado para la correlación, retención y búsqueda sobre tasas de eventos.

Contará con un único repositorio para el almacenamiento de todos los eventos enviados y normalizados desde su origen por los conectores, éste repositorio guardará en su totalidad los distintos elementos de cada evento en campos específicos independiente del tipo de dispositivo

La consola de administración estará basada en web y soportará su acceso a través del SSL Contará además con una interfaz gráfica y con una interfaz de línea de comando para su administración.

Proveerá un control de acceso de usuario y manejar la seguridad basada en roles.

Configurará, asegurará y controlará el acceso para limitar quién puede acceder o visualizar información del sistema.

Permitirá que los dispositivos o sistemas se puedan agrupar de múltiples formas, simultáneamente, con base a procesos de negocio, aplicación, ubicación geográfica, tipo de plataforma.

El sistema de administración permitirá configurar o ampliar la información de los eventos con base a:

Selección de prioridades de los activos

Selección de prioridades de "red-localidad" de los dispositivos reporteados en la red

Cambiar el nivel de severidad de las categorías

Crear nuevas categorías y asignar niveles de prioridad

La respuesta a alertas que la herramienta utilice permitirá configurarse por el operador y de forma automática. Estas acciones o respuestas a alertas deberán:

Enviar un trap de SNMP (envió de notificación)

Enviar un mensaje de SMTP

Ejecutar un script específico

Capturará todos los eventos y enviarlos periódicamente al sistema de administración de bitácoras completas.

El acceso a la herramienta será vía HTTPS, mediante cuentas con rol de solo lectura tanto de forma interna a la red de SHF como de forma externa (a través de internet), permitiendo a los responsables asignadas por SHF, consultar los diversos incidentes registrados por el sistema y generar reportes personalizados del mismo.

Se incluye en la propuesta los manuales, guías, orientación, referencias y transferencia de conocimiento necesarios, sin costo adicional para SHF.

Respuestas automáticas o iniciadas por un operador con base a las alertas de los eventos correlacionados.

Realizará una evaluación de amenazas recolectando información de roles de usuarios, activos críticos, información de vulnerabilidades, información de zonas, exposición al ataque y listas de observación en tiempo real y en memoria, utilizando estos elementos para reducir los falsos positivos.

Identificar cualquier incremento en la actividad, ya sea del atacante, destino, protocolo o cualquier otro campo bajo un umbral de tolerancia de tal forma que sea posible identificar usuarios anómalos o comportamiento en el uso de aplicativos.

Para la Administración, Integración, Monitoreo y Reporteo:

OPERBES, S.A. DE C.V. llevará a cabo las siguientes actividades:

Configuración centralizada de log's operativos y de auditoría.

Registro de acciones administrativas.

Revisión local de cumplimiento con las políticas de seguridad.

Identificación de activos.

Amenazas identificando vulnerabilidades.

Capacidad de acceso para al menos 3 usuarios en la misma consola.

Administrar bitácoras completas de los dispositivos para poder realizar un análisis forense que permita construir un caso sólido, las cuales serán manejadas y almacenadas en un histórico de hasta 3 meses en línea y fuera de línea durante la vigencia del contrato, debido a que podrá ser solicitada y/o acceder en cualquier momento para efectos de supervisión o forense. Por lo OPERBES, S.A. DE C.V. conisdera el almacenamiento necesario que se requiera para dicho efecto.

Administración de manera remota y de acuerdo a los incidentes registrados se realizarán los procedimientos correspondientes para su notificación, seguimiento y en su caso, mitigación.

Será capaz de generar reportes de los diversos eventos de seguridad o incidentes que se presenten, indicando el incidente ocurrido, fecha, duración, origen del mismo. Así OPERBES, S.A. DE C.V. informará de las acciones que se hayan realizado para su mitigación y/o para evitar que sucedan nuevamente.

Llevará a cabo la comparación de los eventos registrados en todos los dispositivos correlacionados contra un patrón de incidentes ya establecido para confirmar la existencia o no de patrones de tráfico anormales, comportamientos indebidos y actividades que puedan poner en riesgo los activos de SHF para así catalogarlos como incidentes de seguridad. También se realizarán las recomendaciones necesarias para erradicar la actividad sospechosa. Éste dictamen contendrá la información detallada, suficiente y necesaria para la plena identificación del origen del ataque o actividad sospechosa, así como del destino del ataque; no será suficiente informar la dirección IP origen o destino del ataque.

OPERBES, S.A. DE C.V. incluye los componentes necesarios que le permitirán ajustarse a las características propias de la infraestructura de red de SHF y detectar amenazas basadas en el comportamiento de la misma abarcando dispositivos de seguridad, dispositivos LAN, servidores y aplicaciones en general a manera de identificar los falsos positivos provocados por aplicaciones o procesos normales de la red.

Con la correlación de la información que le reporten los diferentes dispositivos se detectará rápidamente los incidentes y alertar a los responsables designados por SHF o a un tercero que esta designe, para que aplique la mitigación correspondiente.

Monitoreo del comportamiento de la red mediante baseline
Monitoreo de los componentes de la infraestructura de seguridad (hardware y software)
Monitoreo de ataques y respuestas en tiempo real
Monitoreo de los sistemas de red
Monitoreo de los sistemas de seguridad
Detección, identificación y reportes de cambios y eventos
Applets de Integración para desarrollo de scripts para captura de log's
Asistentes o alertas operacionales de los elementos monitoreados
Capacidad de auto auditoría de comportamiento y visibilidad de su nivel
Módulo de remediación
Análisis forense
Análisis post mortem de eventos
Manejador de alertas
Alertas en tiempo real
Colección, correlación de eventos y cambios
Análisis de estados
Plantillas predefinidas de reportes
Reportes de indicadores clave de performance

Reportes en la detección de anomalías en el comportamiento de la red

Reportes de eventos

OPERBES, S.A. DE C.V. considerará un enlace independiente para recolección de eventos con el fin de no consumir el ancho de banda de los enlaces de SHF.

OPERBES, S.A. DE C.V. considera un Ingeniero certificado en la solución para la administración de la misma; este estará en sitio y será el encargado de administrar, dar atención, seguimiento y generación de reportes de eventos en el correlacionador.

En el Apartado Correlacionador se presenta la solución propuesta.

Servicio de Operación

Descripción del Servicio

OPERBES, S.A. DE C.V. tomó 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.

Mesa de ayuda

OPERBES, S.A. DE C.V. implementará una Mesa de Ayuda, La cual será identificada por SHF como "Mesa Especializada de Servicios "MES", con capacidad para atender todos los tickets que se generen y que le lleguen apegándose en todo momento al proceso de Administración y seguimiento de solicitudes, requerimientos, Incidentes y problemas, del MAAGTIC-SI vigente o en su caso el que lo sustituya.

La MES es el centro de atención de OPERBES, S.A. DE C.V. ubicado en sus instalaciones, mediante el uso de herramientas para monitoreo y de manera dedicada para el servicio proporcionado a SHF, con el propósito de cumplir con los requerimientos de nivel de servicio sin que esta interconexión genere gastos adicionales para SHF.

OPERBES, S.A. DE C.V., alineará todos sus procesos relacionados con la administración del servicio provisto a SHF al MAAGTIC-SI vigente o en su caso el que lo sustituya, lo anterior considera a la Mesa Especializada de Servicios 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.

La Mesa Especializada de Servicios de OPERBES, S.A. DE C.V. será responsable en todo momento de la satisfacción de los usuarios en materia de los servicios proporcionados por el Proyecto, asegurando que los incidentes y problemas reportados sean resueltos dentro de los niveles de servicio establecidos, realizando o emprendiendo acciones para eliminar las causas raíz y/o para prevenir fallas potenciales.

Se requiere que la solución sea implementada, puesta a punto, en un máximo de 60 días naturales posteriores a la fecha del inicio del contrato derivado de este proceso licitatorio. Así como integrada a la mesa de ayuda de SHF.

Para seguimiento de reportes, OPERBES, S.A. DE C.V. implementará durante la vigencia del contrato y sin costo adicional para SHF, una herramienta de gestión, que tenga la capacidad de generar y compartir registros históricos, consultas, generación de reportes y seguimiento a los eventos presentados y la solución correspondiente, la cual contará con acceso a la información para La Mesa Especializada de servicios (MES), La Mesa de Ayuda de SHF y los Responsables del Proyecto que SHF designe. Para gestionar en todo momento los reportes desde su apertura, atención, solución y cierre, OPERBES, S.A. DE C.V. generará cuentas de lectura para el acceso.

Considera que la herramienta de gestión de la Mesa de Ayuda propuesta se sincronizará con la herramienta de gestión de SHF. Dicha sincronización estará concluída en las fechas que se establezca, en caso de no cumplirse se aplicarán las deductivas establecidas en el Capítulo: Deducciones. Se realiza la aclaración de que la herramienta de la Mesa de Ayuda con que cuenta SHF es: CA Service Desk v12

OPERBES, S.A. DE C.V. hará la transferencia de conocimiento sobre el manejo de la herramienta de Mesa Especializada de Servicios al menos a tres servidores públicos por SHF, previo a la puesta en operación de los servicios.

OPERBES, S.A. DE C.V. tomó en consideración que las Funciones generales de la Mesa Especializada de Servicios:

Apegarse a lo establecido en el manual administrativo de aplicación general en las materias de tecnologías de la información y comunicaciones y de seguridad de la información MAAGTIC-SI vigente o en su caso el que lo sustituya

Cumplir con los niveles de servicio definidos por SHF para la atención de los reportes, solicitudes de servicio, incidentes y problemas.

La solución de software estará basada en el manejo de procesos del MAAGTIC-SI vigente o en su caso el que lo sustituya y administrar como mínimo los módulos de: Recepción de reportes, solicitudes de servicio o de información, incidentes y problemas, manejo de incidentes, manejo de problemas y reportes de estadísticas e indicadores.

Proporcionar atención y soporte para mantener la operación de la RPV-MPLS, conforme a los niveles de servicio establecidos.

Iniciará operaciones al inicio de los servicios.

Operará con un horario de servicio 7x24x365, brindando la atención de acuerdo a los niveles de servicio establecidos.

OPERBES, S.A. DE C.V. tomó en consideración que los responsables del proyecto designados por SHF, podrán levantar incidentes y notificar a la MES vía telefónica y/o correo electrónico para la pronta solución de este.

Las tareas mínimas que OPERBES, S.A. DE C.V. realizará con SHF son: recibir, registrar, analizar, resolver y canalizar los reportes de incidentes, dar seguimiento, solución y cierre a los incidentes informando a los responsables asignados por SHF, para que a su vez se informe al usuario final oportunamente.

La atención y soporte se realizará con la interacción y comunicación permanente entre SHF y la Mesa Especializada de Servicios.

La Mesa Especializada de Servicios tendrá la capacidad suficiente para almacenar y recuperar todos los reportes que se presenten durante la vigencia del contrato, clasificados por tipo de evento, por mes y por año.

Los datos mínimos requeridos en un reporte para el control de eventos e incidentes serán:

Identificador del reporte o número de incidente o evento.

Identificador del usuario que reporta, (estos son los datos que identifican al usuario que levantó el reporte), al menos nombre, teléfono, correo electrónico y ubicación. La definición final de estos datos se acordarán con OPERBES, S.A. DE C.V..

Hora en que se presenta el evento reportado.

Hora en que se reporta el problema por parte del usuario autorizado.

Tiempo de solución del incidente y restablecimiento del servicio.

Descripción del ticket.

Solución del ticket.

Cuando se presenten interrupciones, fallas, errores en alguno de los enlaces, degradaciones en el desempeño en alguno de los equipos del servicio solicitado, OPERBES, S.A. DE C.V. informará al personal técnico de SHF a través de un correo electrónico, llamada telefónica y mensaje de texto la falla del servicio que requiera atención.

Una vez resuelto el problema reportado, el personal asignado por OPERBES, S.A. DE C.V. informará al personal técnico de SHF, la causa del problema y la solución de la misma, con el fin de validar que el servicio fue restablecido y cuente con la información para generar las estadísticas de disponibilidad del servicio de acuerdo a los niveles de servicio requerido.

Una vez recuperado el servicio, OPERBES, S.A. DE C.V. documentará las acciones aplicadas para el cierre del reporte.

A solicitud del personal técnico de SHF OPERBES, S.A. DE C.V. entregará un diagnóstico documentado y un plan de solución definitiva a los problemas que generaron interrupción general o parcial de la red RPV, Internet y solución de seguridad en los nodos o equipos involucrados, así como en degradaciones en el desempeño en alguno de los equipos del servicio solicitado.

OPERBES, S.A. DE C.V., en conjunto con SHF, definirá, actualizará y difundirá el catálogo de servicios que proporcionará la Mesa Especializada de Servicios.

La información deberá poder fluir en forma bidireccional de una hacia otra mesa, es decir, considerar al menos las siguientes operaciones: Importar, exportar y actualizar, lo que permitirá realizar de manera enunciativa más no limitativa las siguientes actividades:

Generar un reporte en la MES desde la Mesa de Ayuda de SHF.

Retroalimentar desde la MES a la mesa de ayuda de SHF información sobre la atención de un ticket.

Retroalimentar desde la MES a la mesa de ayuda de SHF la documentación de resolución del ticket.

Notificación de la mesa de ayuda de SHF a la MES del cierre del ticket.

Alertas de notificación por intercambio de información de la mesa de ayuda de SHF a la MES y viceversa.

Los campos de información que serán enviados o recibidos de SHF hacia la MES y viceversa para solicitudes e Incidentes, se proporcionarán al Licitante.

SHF podrá realizar auditorías de los reportes de la solución de la MES en el momento que así lo requiera y revisar los niveles de servicio, para lo cual se Proporcionará a SHF las cuentas de solo lectura personalizadas de acceso y contraseñas al personal que se designe.

OPERBES, S.A. DE C.V. Proporcionará a SHF al menos una clave de acceso de solo lectura a los equipos de ruteo en los CPE's de la solución, con el propósito de que se pueda revisar los parámetros de operación del equipo, entre los que incluyen: uso de procesador y memoria, estado de las interfaces seriales y Ethernet, fast Ethernet, gigabit Ethernet, bits o bytes transmitidos y recibidos por cada interface, así como ejecutar los comandos de pings y traceroute.

OPERBES, S.A. DE C.V. configurará al menos una comunidad SNMP v3 con derechos de lectura, independiente a la comunidad que OPERBES, S.A. DE C.V. utilice para el monitoreo de los diferentes equipos de comunicaciones que formen parte de su servicio y se encuentren en instalaciones de SHF. Esta comunidad tendrá como objetivo, monitorear todos estos equipos desde un sitio diferente al NOC/SOC, con uno o más servidores de SHF (o un tercero definido por ésta). En estos servidores se recibirá la notificación automática de incidentes y envío de traps SNMP, según parámetros establecidos por SHF, que permitan tener visibilidad sobre variables importantes de desempeño en la RPV MPLS. El número de comunidades será al menos uno.

Contará con la opción de extraer e interpretar datos relacionados con el estado y el desempeño de los dispositivos que componen la red de SHF.

Los registros generados por las herramientas de monitoreo implementadas por OPERBES, S.A. DE C.V. serán los que se utilizarán para validar los niveles de servicio proporcionados por OPERBES, S.A. DE C.V., de acuerdo a los requerimientos de SHF y bajo los niveles de servicio definidos en el apartado de Niveles de Servicio.

En caso de controversia, la información recibida a través del protocolo SNMP en los centros de monitoreo de SHF, será utilizada como referencia para determinar si existen diferencias respecto a lo reportado por el NOC, y en su caso, ser reconocidas como elementos de juicio para establecer un punto de acuerdo. Ésta opción solo será prerrogativa de SHF más no de OPERBES, S.A. DE C.V..

OPERBES, S.A. DE C.V. proporcionará, previo a la puesta en operación de los servicios, una matriz de escalamiento, la cual contenga al menos la información de los contactos (nombre, puesto, teléfono oficina, teléfono móvil) para su localización en todo momento, así como los tiempos establecidos para pasar al siguiente nivel.

Centro de Operación de la Red (NOC)

El NOC propuesto por OPERBES, S.A. DE C.V. considera, al menos, las siguientes tareas en servicios de gestión y monitoreo:

OPERBES, S.A. DE C.V. tomó en consideración que SHF deberá contar

datos y video.

OPERBES, S.A. DE C.V. generará las notificaciones de todas las incidencias de los nodos, equipamiento y servicios de la red de SHF de forma inmediata a una dirección de correo electrónico, llamada telefónica y mensaje de texto definidos por SHF y en ese momento iniciar el procedimiento de solución. El Licitante debe absorber los costos que se generen para la entrega de este servicio. con acceso de sólo lectura en los equipos de comunicaciones utilizados para la prestación del servicio con el fin de poder supervisar y evaluar la configuración de los mismos. OPERBES, S.A. DE C.V. proporcionará las herramientas necesarias y el acceso simultáneo para tres personas designadas por SHF, con el fin de que éstas puedan monitorear en línea el consumo de ancho de banda, analizar el tráfico del enlace, disponibilidad de servicios, medición de los acuerdos de niveles de servicio y aplicaciones descritas en este anexo, observando sus funciones principales, desempeños, bitácoras, alarmas, eventos y reportes para conservar su mejor funcionamiento y desempeño todo el tiempo posible.

El NOC operará en paralelo a la integración de cada uno de los servicios en la red de voz,

El cierre de cada incidencia o requerimiento, se realizará de manera coordinada entre personal de SHF y el personal designado por OPERBES, S.A. DE C.V. para tal efecto. La incidencia sólo será

cerrada cuando sea corroborada su solución y aceptada por SHF. OPERBES, S.A. DE C.V. considera que el tiempo de validación de la solución de la incidencia o requerimiento será independiente al de la solución del mismo siempre y cuando se valide que ya no exista afectación y/o se envíe evidencia de que los requerimientos fueron realizados, apegandose siempre a los niveles de servicio solicitados por la Convolcante.

La solución a incidencias, será de manera remota o en sitio, según se requiera, así como la realización de las tareas de mantenimiento preventivo en sitio que sean necesarias para cumplir los niveles de servicio.

OPERBES, S.A. DE C.V. entregará dentro de los primeros cinco días hábiles de cada mes durante la vigencia del contrato, los reportes de las incidencias ocurridas en el servicio en CD o algún otro medio electrónico clasificadas como:

Reporte detallado de incidencias por cada sitio y su tiempo de solución, donde se refleje el número de horas y/o minutos sin servicios (voz, datos y video) imputables a OPERBES, S.A. DE C.V. y los imputables a SHF (energía eléctrica, equipo apagado, etc.) o a causas de fuerza mayor en el sitio afectado (tormentas eléctricas, huracanes, inundaciones, etc.)

Reporte del número de incidencias clasificadas por tipo y severidad.

Reportes de desempeño de equipos, servicios y aplicaciones, especificando:

Utilización de CPU

Utilización de memoria

Utilización de ancho de banda

Latencia

OPERBES, S.A. DE C.V. entregará un resumen en forma impresa y/o electrónica, donde incluya el control de los cambios.

En caso de Incidentes o daños en el hardware de los equipos del centro de soporte y monitoreo, el OPERBES, S.A. DE C.V. será el responsable de contar con procedimientos para mantener los niveles de disponibilidad y servicio solicitados.

La herramienta de monitoreo utilizada por OPERBES, S.A. DE C.V. no interferirá en el desempeño de la red y/o ancho de banda de cada nodo, no mayor al 5% de la capacidad del enlace.

OPERBES, S.A. DE C.V. integrará una punta a la MPLS para el monitoreo, gestión y correlación de los equipos así como la comunicación de voz el cuál no deberá exceder del 70% del uso del ancho de banda para éste servicio durante la vigencia del contrato, quedando siempre bajo su responsabilidad.

El sistema de monitoreo contará con la capacidad de graficar por día, semana, mes, semestre y año, SHF podrá seleccionar el periodo de tiempo a su elección para generar reportes.

La información estará disponible en línea con resolución de al menos: 5 minutos por día, resolución de 15 minutos por semana, resolución de 60 minutos por 90 días, resolución de 1 día hasta la vigencia del contrato.

Prevenir problemas potenciales a través del monitoreo proactivo.

Aislar y solucionar los problemas presentados en los elementos de los nodos y la prestación de los servicios.

Cuando la herramienta de monitoreo detecte los problemas del incidente en la red y/o los equipos, ésta enviará vía correo electrónico la notificación de forma automática al personal designado por SHF.

La Herramienta de monitoreo será capaz de monitorear equipos a través de los siguientes protocolos: SNMP v3, JMX, WMI, ICMP.

El servicio contará con una herramienta que permita descubrir automáticamente todos los elementos de red que tengan una dirección IP con la finalidad de obtener un inventario de la infraestructura instalada.

Permitirá realizar peticiones bajo demanda de una prueba mediante un OID (Object Identifier, Identificador de Objeto) en específico.

Permitirá configurar umbrales por cada elemento y variable monitoreada en cada uno de los dispositivos.

La herramienta de monitoreo permitirá el acceso remoto vía HTTPS solo de lectura al personal de las SHF, con la finalidad de verificar el estado de los servicios y la actividad de los enlaces.

OPERBES, S.A. DE C.V. contará con una herramienta en sus instalaciones de monitoreo que permitirá obtener el estado de operación de los enlaces de los sitios remotos y el nodo central de SHF al menos a través de un navegador web y alguna otra interface de administración.

Se requiere que el monitoreo de cada uno de los enlaces y del nodo central, así como los CPE, considere los siguientes aspectos:

Consumo de ancho de banda en tiempo real.
Visualización del estado del enlace en línea
Notificar en forma automática los problemas en la red y/o los equipos.
El sistema de monitoreo entregará los siguientes tipos de reportes vía web y en forma gráfica, para la medición del desempeño de la red.
% utilización de CPU y memoria.
Consumo de ancho de banda (entrada, salida y promedio) por enlace.
Consumo de ancho de banda por QoS (bits entrada, salida y descartados).
Paquetes perdidos por errores y descartes
Para la administración de los incidentes generados de la red:
Fecha y hora de la última alarma del sitio.
Tiempo promedio de solución y respuesta
Relación de incidencias del mes
Clasificación de reportes por tipo de incidentes
Frecuencia y tipo de Incidentes
Identificación de problemas
Plan de acción para corregir desviaciones en los niveles de servicio
Casos abiertos y cerrados
La solución con la que se preste el servicio de monitoreo de infraestructura y medición de Niveles de Servicio tendrá la capacidad de ajustar el tiempo de poleo de cada una de las métricas colectadas.
El poleo de cada una de las métricas será de 5 minutos, teniendo la capacidad de generar poleos de hasta un minuto en caso de así convenir a la operación a solicitud expresa de SHF.
El servicio contará con una interface en la cual se podrán visualizar, configurar y dar de alta los diferentes niveles de servicio (SLA por sus siglas en inglés), mediante la correlación de las diferentes variables que se estén monitoreando. Esta interface tendrá al menos las siguientes características:
Configurar el periodo del nivel de servicio de forma diaria, semanal o mensual
Configurar con qué frecuencia se lleva a cabo la correlación de las métricas
Configurar las fórmulas y umbrales de cada uno de los niveles de servicio, solicitados en el punto (Niveles de servicio)
La solución mostrará el tiempo de cumplimiento de cada uno de los SLA.
El servicio contará con una interface en la que se puedan visualizar de forma gráfica las métricas monitoreadas por cada dispositivo, es decir, para visualizar un esquema de conexión de equipos (capa 7), el monitoreo se podrá realizar por medio de protocolos de capa 2 (de manera enunciativa más no limitativa: ARP, RARP, Ethernet, etc) y de capa 3 (de manera enunciativa más no limitativa: IP, ICMP, RIP, IGMP, SNMP,etc).
Existirá una interface que permita visualizar un esquema de conexión de equipos mediante protocolos de capa 2 y capa 3.
La disponibilidad de los equipos de la infraestructura será medido con base al protocolo ICMP.
Las lecturas se podrán actualizar en línea y contarán con la facilidad de generar mediante filtros: reportes que representen informes del comportamiento de la red por días, semanas, meses.
Procedimientos de escalamiento de niveles de atención (tiempo estimado entre cada escalamiento de nivel.
El Licitante deberá llevar un proceso de control de cambios que se sujete a la aprobación de un comité conformado por los responsables de cada servicio tanto de SHF como de OPERBES, S.A. DE C.V.. El control de cambios se apegará al MAAGTIC-SI vigente o en su caso el que lo sustituya.
OPERBES, S.A. DE C.V. considera los siguientes tipos de control de cambios.

Tipo de Cambio	Definición	Tiempo de Solución
Urgente	Son todos los cambios a un componente de infraestructura 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, los cuales implican una interrupción sustantiva en el servicio.	Con autorización de la ventana por SHF
Estánd	Son todos los cambios a un componente de	4 hrs. después de

Tipo de Cambio	Definición	Tiempo de solución
ar	infraestructura, que no representan ningún riesgo de afectación.	la solicitud de SHF

Tabla: 4.2.1

Análisis de Tráfico

OPERBES, S.A. DE C.V. proporcionará una herramienta de monitoreo de tráfico con capacidades de analizador de protocolos, capaz de recolectar información del funcionamiento de la voz, datos y video que cursen hacia y desde la RPV MPLS, VPNs, internet, LAN, servidores u otros. Con una amplia variedad de patrones de uso.

OPERBES, S.A DE C.V basa su propuesta en la tecnología Netscout la cual se describe a continuación

DESCRIPCIÓN DE LA SOLUCIÓN DE NETSCOUT

Es una solución de monitoreo de aplicaciones y protocolos que utiliza los paquetes capturados (tráfico) para determinar la salud de las mismas dentro de la red. Por medio del módulo de Ngenius Voice & Video Manager, Netscout permite monitorear el entorno de VoIP.

Por medio de la habilitación de puertos espejo, la herramienta nGenius NetScout recibe el tráfico que será monitoreado en los equipos colectores llamados InfiniStream, y analiza las transacciones que existen a nivel IP entre los elementos involucrados de las aplicaciones y protocolos que cruzan a través de la red. Otra fuente de colección de datos es la que se entrega en los Routers ISR Cisco de segunda generación, debido a que NetScout cuenta con un Agente integrado 100% compatible con estos equipos, lo que garantiza que no se comprometen las funcionalidades primarias del Router. El Agente Integrado nGenius es un software que habilita el módulo de servicios del Router como una sonda virtual para la captura y análisis del tráfico. Su funcionalidad principal es la de entregar visibilidad detallada del tráfico que entra y sale de las oficinas remotas que tengan el Router ISR como medio de acceso hacia la red WAN. De esta manera; se incrementa considerablemente la visibilidad del tráfico que fluye a lo largo de la red con un enfoque punto a punto desde la oficina remota y hasta el Centro de Datos.

El Agente Integrado nGenius es alojado en la plataforma Cisco UCS de los Routers ISR G2 que incluye, el blade server Cisco Services Ready Engine (SRE) x86 y la plataforma Cisco Services Ready Engine Virtualization (SRE-V) que está basada en el VMware vSphere Hypervysor (ESXi). El módulo de servicios Cisco SRE provee procesamiento e interfaces de red dedicadas que no afectan el desempeño ni los recursos del router mismo. Una vez instalado, el Agente Integrado nGenius se ejecuta como una instancia de software sobre el módulo de servicios SRE y se encargará de monitorear el tráfico de paquetes que fluya a través del backplane del router Cisco ISR G2. Gracias a esta implementación, es posible tener visibilidad permanente del tráfico que intercambia con la WAN el Router de la oficina remota, ya que el Agente Integrado enviará las estadísticas del tráfico que genera hacia el servidor central de la solución nGenius que se encargará de presentar la información que concentra de todos los puntos de monitoreo en tiempo real e histórico permitiendo facilitar las tareas de análisis y resolución de problemas relativos a las aplicaciones o protocolos que fluyen por la red.

La herramienta genera indicadores de desempeño (KPIs Key Performance Indicators) que muestran la salud de las diferentes variables dentro de la red. Esos KPIs son enviados al servidor central de la solución llamado ngenius one y voice and video manager, quienes generan los reportes y estadísticos a fin de tener un histórico y poder llevar a cabo el análisis de capacidades de la solución.

Cuando es necesario contar con los paquetes responsables de alguna gráfica, los InfiniStreams cuentan con almacenamiento en el orden de los Terabytes, para poder regresar en el tiempo y conocer que fue lo que sucedió de manera precisa ante un evento o degradación de servicio que haya afectado la experiencia de algún usuario de la red.

Entre la información importante que la solución es capaz de generar destacan las siguientes variables:

Medición de la experiencia del usuario final
Monitoreo proactivo (la herramienta aprende del comportamiento de la red).
Tiempos de Respuesta, separado por el tiempo de aplicación y tiempo de red.
Errores en la red.
Retransmisiones.
Análisis forense a nivel de milisegundos.

Representación de Servicios a nivel protocolo aplicativo.

Monitoreo de máquinas virtuales

Utilización de ancho de banda, separado por aplicación, transacción, servidor o usuario.

Descomposición de las transacciones en la red a nivel de protocolo para ver el Three – Way Handshake.

Verificar los usuarios y sus conexiones dentro de la Red,

Validar parámetros de configuración como inscripción, QoS, VLANs, etc.

La herramienta permite asegurar la continuidad de los servicios corporativos.

Optimizar el rendimiento en la entrega del servicio.

Tiene la capacidad de integrar todas las diferentes plataformas que integran la red como pueden ser datos LAN, WAN, VoIP, Servers, aplicaciones, métricas para análisis de Performance de Red (VPN).

Incrementa el valor de la Infraestructura existente.

Ayuda en la identificación de la causa raíz de la degradación de un problema.

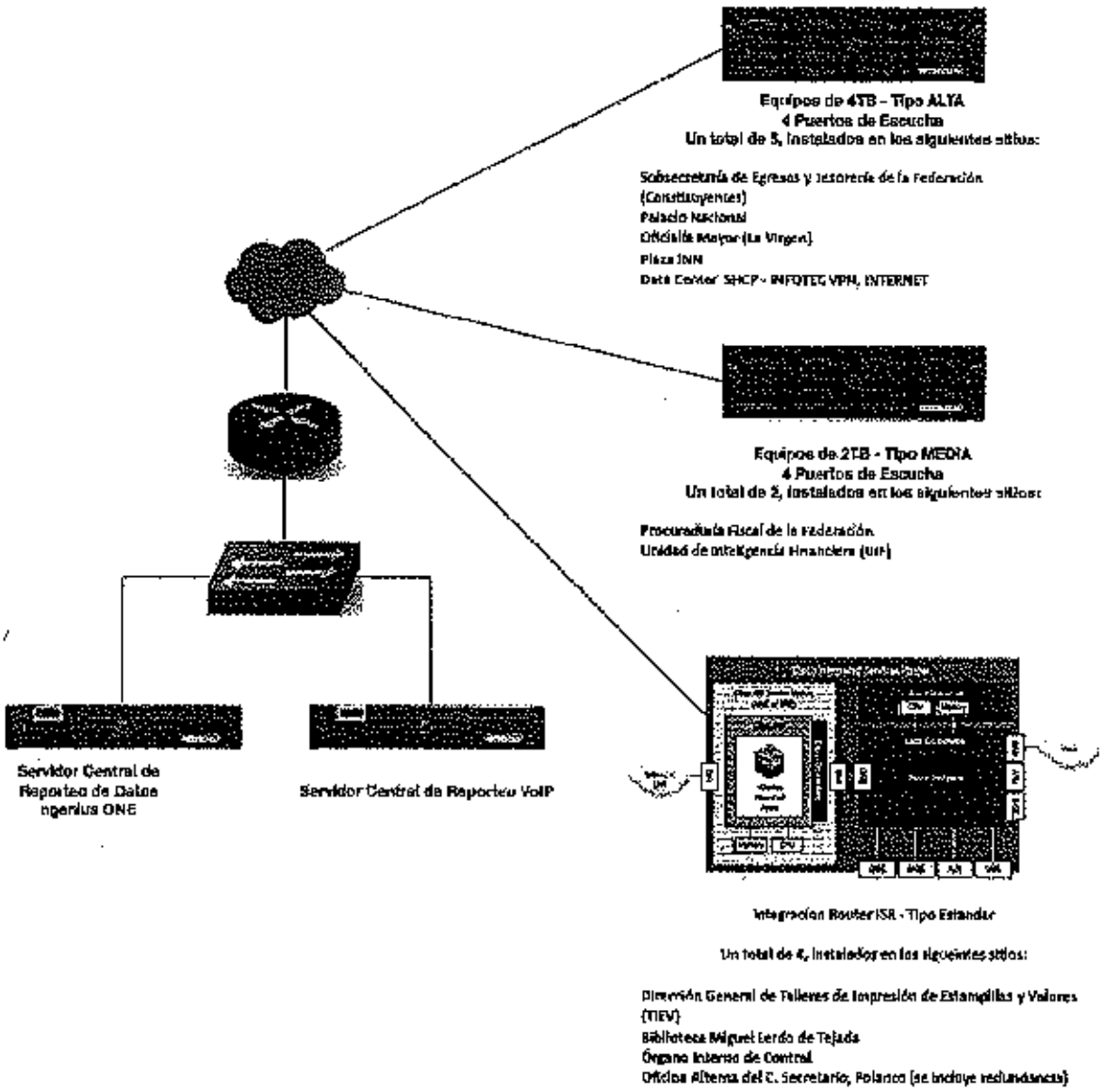
Permite disminuir los costos de impacto u operación ante la degradación de un servicio.

Es una herramienta para llevar a cabo troubleshooting de red con un análisis enfocado al servicio.

Generación de Reportes (web, PDF, CSV) y acceso a usuarios de manera ilimitada.

SOLUCION PROPUESTA

Diagrama



La solución propuesta se conforma de los siguientes elementos:
-Servidor Central de Reporteo – nGenius ONE 5608L-ENT1-4W
-Servidor Central de Reporteo de VoIP - 5510L-VDC10K-4W

-Equipos Colectores de Tráfico
- 5 Infinistreams 1G 4 TB – 4 puertos – que seran instalados en los sitios de criticidad ALTA - 6910/MS-4W
- 2 Infinistreams 1G 2 TB – 4 puertos – que seran instalados en los sitios de criticidad MEDIA - 2910/LS-4W
- 5 Sitos Estándar (criticidad monitoreo) – Integración Cisco ISR - IA1110-4W

Al cliente se le proporcionara una interfaz de usuario vía Web o la instalación de un cliente ligero, instalado en las maquinas del personal asignado para llevar a cabo las tareas de monitoreo, donde podrá consultar el rendimiento de la Red y sus Aplicaciones y servicios, en tiempo real e histórico. Esta interface web tiene la capacidad de analizar datos en línea. Cuenta con un almacenamiento histórico de los últimos 12 meses.

La propuesta de monitoreo de NetScout considera la generación de reportes históricos, estos reportes se podrán encontrar en los siguientes formatos:

-PDF
-HTML
-CSV

El monitoreo de la red, Aplicativos y servicios, se llevara a cabo en tiempo real de forma centralizada, por medio de la configuración de puertos espejo en los switches core.

Se podrán configurar aplicaciones propias del cliente bajo los siguientes parámetros:

URL

Direcciones de los servidores combinadas con los puertos

Puertos TCP o UDP

Respecto al tráfico WEB, podrá inventariarse y darse de alta aplicaciones por su URL.

Para la creación de usuarios, NetScout permite generar diversos perfiles de usuario (lectura/escritura – solo lectura).

Los usuarios tendrán acceso a tableros de control internos configurables, donde podrán visualizar entre otras cosas:

Utilización de ancho de banda

Utilización de ancho de banda de una aplicación en especifico

Bytes de entrada/salida

Top Aplicaciones que corren por la Red.

Tiempos de Respuesta de las aplicaciones que corren por la Red.

Actividad de tráfico por protocolo y por dirección IP.

Top de IP que más tráfico generan.

Top de Conversaciones que más tráfico generan.

Tabla del comportamiento de todas las aplicaciones que corren por la Red.

Tabla con cantidad de tráfico que genera cada IP.

Tiempos de respuesta Promedio y Picos.

Peores tiempos de respuesta de Aplicaciones.

Peores tiempos de respuesta de Servidores.

Tiempo de Respuesta especifico de una conversación, dividiendo tiempo de Red vs Aplicación

Cantidad de retransmisiones

Número de peticiones a un servidor en especifico

Número de peticiones satisfactorias y fallidas

OPERBES, S.A. DE C.V. considera el Anexo 1 "Matriz de Servicios" y dimensionar con base en la siguiente tabla:

Sitio Criticidad	Capacidad de Almacenamiento
ALTA	4 a 16 TB 4 puertos de escucha
MEDIA	2 TB 4 puertos de escucha
ESTANDAR	Al comunicarse los sitios estándar con sitios de mayor criticidad (alto y media), el tráfico que intercambien con estos últimos, será analizado por los equipos de monitoreo destinados para los mismos.

Tabla: 4.2.1.1

Para los nodos considerados como de criticidad MEDIA, cuyo ancho de banda especificado en el documento "Matriz de Servicios" sea igual o menor a 4.5 Mbps, la solución de monitoreo que se deberá contemplar será de tipo ESTANDAR.

El sistema de monitoreo contará al menos con las siguientes funcionalidades:

Proveer la habilidad de escuchar el tráfico de la red y descubrir elementos nuevos de infraestructura automática.

Visibilidad en toda la red (extremo a extremo), logrando identificar todos los elementos de infraestructura, conexiones y segmentos. Mostrando la distribución lógica y física de la topología de red.

Crear una CMDB de configuraciones como MAAGTIC-SI vigente o en su caso el que lo sustituya. Esta CMDB contendrá la configuración de la solución de monitoreo que proporcionará rendimiento, comportamientos y tendencias de la red así como crear, planificar, ejecutar y personalizar informes vía Web sobre la salud y rendimiento de los recursos de la red.

Este sistema tendrá la capacidad de integrar todas las diferentes plataformas que integran la red de SHF, tales como voz, datos, video, LAN, WAN, VoIP, Servidores, aplicaciones y métricas para análisis de Performance de red (LAN y WAN).

Proporcionará RCA (Root Cause Analysis) en caso de falla y en Tiempo Real, y determinar el Impacto en la Red.

La solución de monitoreo de tráfico estará basada en equipos colectores que puedan conectarse vía puerto espejo o por medio de TAP's los cuales le reportaran a un servidor central.

El servidor central estará alojado en las instalaciones de OPERBES, S.A. DE C.V..

El sistema será capaz de integrar al monitoreo aplicaciones y desarrollos propios de SHF al menos por:

Puerto

Direcciones IP de los servidores

URL´s

IP Origen y Destino

La recolección de datos de la solución de monitoreo de tráfico, no afectará el rendimiento de la red de SHF. Por lo que no será una solución basada en agentes.

La solución generará información sobre el rendimiento, comportamientos y tendencias de la red.

El sistema ofrecerá una solución de almacenamiento distribuida para datos históricos por cada sitio de SHF.

El sistema será capaz de crear reportes que permitan seleccionar el periodo (por hora, día, semana, mes, año, y personalizada es decir de fecha a fecha) y/o por grupo de nodos manteniendo en línea la información por lo menos 1 año. Esta base de datos almacenará los registros sumarizados en forma mensual, hasta la conclusión del contrato y podrán ser solicitados por SHF en cualquier momento durante la vigencia del contrato.

Respecto al tráfico HTTPS, HTTP y WEB se podrán configurar y dar de alta aplicaciones por su liga de acceso URL.

La solución será capaz de realizar desgloses sobre las gráficas para mostrar el detalle de la información (proceso conocido en inglés como Drill Down).

La resolución disponible de los datos en las gráficas podrá filtrarse, al menos, por segundos, minutos, horas, días o meses.

Se emitiran alertas cuando el desempeño y rendimiento de la red se desvíe de los patrones establecidos, mediante el análisis detallado de todas y cada una de las aplicaciones que corran en la red incluyendo voz, datos, video y las de manera nativa.

La solución incluirá mecanismos de sincronización como NTP (Network Time Protocol) o PTP (Precision Time Protocol) y así garantizar la correcta sincronización de la información.

La solución se podrá integrar con métodos de autenticación vía Directorio Activo, LDAP v3, Radius o ACS Server.

La solución facilitará la creación de reportes comparativos entre las interfaces físicas y virtuales (subnets, VLAN, QoS).

El sistema contará con un visor de alarmas que al menos de una vista retrospectiva de las mismas.

Tanto OPERBES, S.A. DE C.V. como SHF tendrá la capacidad de obtener mediciones de tráfico y monitoreo proactivo en tiempo real de todo el tráfico cursando por la red de SHF bajo las siguientes métricas:

Utilización de ancho de banda.

Pérdida de paquetes.

Latencia.

Hosts que más utilizan la red.

Enlaces que más se utilizan la red.

Aplicaciones que más consumen recursos de red

Tamaño de los paquetes (Packet Size).

Distribución de los paquetes en la red.

Utilización, errores, broadcast vs. Tiempo en los enlaces monitoreados.

Distribución de Protocolos.

Top de las Conversaciones.

Tiempo de respuesta de aplicaciones.

En los sistemas virtuales cuyo tráfico atraviese la red física monitoreada, se deberán obtener al menos las siguientes métricas: Las máquinas virtuales más utilizadas.

Las aplicaciones que más se usan.

Top de conversaciones entre las máquinas virtuales.

Tiempos de respuesta entre las máquinas virtuales.

Detectará de manera automática y proactiva la actividad de aplicaciones nuevas, como el uso de P2P no autorizado.

Será capaz de realizar análisis forense basado en el análisis de paquetes.

Garantizará el almacenamiento en cada sonda de monitoreo, de acuerdo a la Tabla: 4.2.1.1

Las capturas de paquetes que sean obtenidas por la solución, podrán exportadas en formatos .cap ó .pcap para su análisis posterior.

Permitirá generar diagramas de las conexiones TCP mostrando cómo los paquetes se mueven entre el servidor y el cliente. Esto basado en capturas de tráfico.

La solución mostrarán los grupos de conversaciones TCP/UDP.

Permitirá usar los paquetes almacenados en las sondas de monitoreo para crear gráficas de las transacciones entre 2 hosts que muestren los paquetes de una conexión y la latencia de los mismos.

La solución de análisis y tráfico graficará Tiempos de Respuesta para las aplicaciones dentro de la red, entregando resultados Top de al menos las siguientes variables:

Peores Aplicaciones
Peores Servidores
Peores Clientes
Peores Flujos
Peores Sitios

La solución de análisis de tráfico podrá calcular el tiempo de respuesta por separado de red y servidor.

Permitirá inventariar para una aplicación y/o Servidor la cantidad de respuestas fallidas o satisfactorias.

Será capaz de monitorear el uso de ancho de banda por aplicación y así mismo identificar tendencias de crecimiento para poder tomar decisiones proactivas.

Contará con mecanismos de control de acceso y autenticación para que únicamente el personal autorizado por SHF tenga acceso a la información.

Para la presentación de la información Proporcionará dashboards configurables que podrán contener diferentes paneles o gráficas de información, mostrando al menos la siguiente información:

Uso de los enlaces monitoreados en total y desglosados por:
Aplicación
IP Origen y Destino
Ancho de Banda
Conversaciones entre Hosts
Uso de una Aplicación en total y desglosado por:
Aplicación
IP Origen y Destino
Ancho de Banda
Grupos de Aplicaciones
Conversaciones entre Hosts
Permitirá visualizar para un Host:
Top aplicaciones
Top conversaciones hacia y desde el Host

Observará el estado de las aplicaciones y servicios que están corriendo en el centro de datos, como:

Indicará el número y severidad de las anomalías en indicadores clave de desempeño.

Indicará posibles problemas de desempeño de los aplicativos.

Proveerá la capacidad de hacer zoom sobre la información, conocido como drill-down hacia métricas específicas que hayan causado el problema.

El sistema será capaz de obtener datos disponibles para cada intervalo de tiempo seleccionado mostrando al menos las siguientes variables:

Los paquetes recibidos.
Tipos de errores de los paquetes recibidos.
Tráfico por dirección IP asociado con el puerto, aplicación.
Tráfico por puerto asociado con el protocolo IP y la tasa de Trasmisión en paquetes y bytes.
Conversaciones entre estaciones IP.
Mostrar estadísticas por VLAN y QoS.
Permitirá la creación de filtros personalizados.
Soportará diagnósticos en las diferentes capas del modelo OSI, las cuales deben incluir:
Red

Direcciones IP duplicadas
Frames Perdidos
Paquetes que excedieron el Tiempo de Vida (Time-to Live Expiring)
Transporte
Servidores más Lentos.
Exceso del Tamaño de Ventana en conversaciones TCP (Window Size Exceded)
Contará con filtros de post-captura, independientes de los filtros de pre - captura, al menos por:
Filtro por errores
Filtro de patrones de datos (Bytes y bits) permitiendo la configuración de cualquier patrón dentro de la trama
Filtros por conversación entre dos estaciones a través de la selección del nombre o la dirección IP/IPX
Filtro por protocolos
Tamaño de trama
Paquetes con errores
Dirección IP.
La solución de monitoreo proveerá una consola unificada de acceso a las herramientas de toda la solución de análisis de tráfico de aseguramiento del servicio desde la cual pueden ser lanzadas las interfaces de alerta, monitoreo, troubleshooting.
Gestión proactiva que permita resolver problemas de rendimiento antes de que afecten a los servicios solicitados.
Presentar la información referente a los servicios solicitados para SHF.
Soportará IPV6 y 10GIGA Ethernet.
Realizará monitoreo Ethernet, logrando identificar tecnologías como QoS, MPLS, VPNs y demás servicios encriptados.
Configuración de alarmas para netflow, sflow o similar, QoS, MPLS VLANs. Siendo capaz de generar alarmas por utilización de link.
Generación de reportes del estado actual de los elementos, su desempeño y tendencias.
Configuración de umbrales para la generación de alarmas y envío de las mismas vía correo electrónico, u otro mecanismo automatizado.
Generación de la información sobre las Clases de Servicio utilizadas en cada uno de los nodos de la RPV MPLS.
Generar reportes por Clase de Servicio.
Colectar las siguientes métricas en tiempo real:
Utilización de ancho de banda,
Pérdida de paquetes
Latencia
El sistema trabajará sobre las plataformas Windows y Linux.
Permitirá al personal que designe SHF la generación de reportes explotando todas las variables y funcionalidades de la herramienta de monitoreo, con la opción de parametrizar dichos reportes y consultarlos vía Web.
Será accedida vía WEB por todos y cada uno de los usuarios encargados del monitoreo y buen funcionamiento de la red
El monitoreo en tiempo real para la detección de alarmas y eventos de fallas se realizará al menos cada minuto, este mismo intervalo de tiempo será utilizado para la medición de los niveles de servicio.
Análisis de Voz
La herramienta de monitoreo y análisis:
Recibirá información estadística en tiempo real, de las mismas sondas de análisis de tráfico definidas en el punto anterior (Análisis de Tráfico), que permitira hacer una evaluación de la calidad de los flujos de voz, presentando resultados por medio de gráficas.
Contará con pantallas especificas para el monitoreo e identificación de posibles causas que puedan estar relacionadas con un evento de falla y que ayuden a inferir su solución, elaboración de informes, filtro de los flujos de voz analizados y un resumen de los problemas que se presentan dentro de los ambientes de voz de SHF.
La solución deberá presentar un análisis que permita ver y clasificar en un código de colores, el porcentaje del número de flujos de voz analizados dentro de niveles aceptables, degradados y críticos, basado en indicadores clave de calidad que incluyan como mínimo:
Calidad media de la voz sobre IP (puntuación MOS).

Porcentaje de los flujos de voz.

Volumen medio de las conversaciones activas medidas de los flujos de voz.

Relación señal ruido promedio de los flujos de voz.

Cada uno de estos indicadores clave coloreados, al ser seleccionado, deberá llevar a pantallas de información más profunda acerca de las localidades y los flujos de voz analizados para llegar a los valores presentados inicialmente.

Será posible crear los filtros básicos de uno o más nodos fuente de las llamadas y uno o más nodos destino de las llamadas.

Permitirá crear los siguientes filtros avanzados:

Una o más sonda de monitoreo y análisis.

Uno o varios codecs de audio, incluyendo como mínimo G.711A, G.711μ, G.723.1, G.729, G.722, G.728, GSM 06.10, AMR-NB, AMR-WB, G.722.1, G.722.1C , VMR-BM, iLBC, G.729D, G.729E, GSM-EFR, G.726 entre otros

Uno o más tipos de dispositivos incluyendo como mínimo: ATA, MCU, teléfono IP, Media Gateway, Mobile, el router NAT, Session Border Control (SBC), decodificador, Soft Phone.

También será posible construir filtros avanzados tomando en cuenta los siguientes criterios:

Voz IP MOS, Voz IP Mínimo MOS, Voz IP MOS degradado, Voz IP Máximo MOS Degradado

Número de paquetes recibidos, el porcentaje de pérdida de paquetes, promedio de pérdida de paquetes de forma consecutiva.

Jitter máximo (ms), Jitter mínimo (ms) Porcentaje de paquetes fuera de secuencia, Retardo en el transporte IP (ms)

Tasa de bits de medios (kbps).

Duración del flujo (seg), el tamaño del payload , comunicación en una vía (One-Way), VLAN ID

Calidad de Servicio (QoS), puerto de origen, puerto de destino

La solución contará con una pantalla de monitoreo que presentará una sección con los eventos más recientes coloreados e indicados por su severidad, con un link dinámico hacia pantallas de información más profunda.

La herramienta permitirá dar de alta las diferentes localidades de SHF donde se concentran los usuarios del Servicio de Telefonía IP, por rangos de direcciones IP, pudiéndose definir localidades y sublocalidades por medio de redes y subredes. Las ubicaciones se podrán visualizar ya sea por sus direcciones IP o nombres asignados en la configuración del sistema.

Existirá una pantalla de análisis de problemas, la cual será capaz de ver el número de flujos de voz afectados.

Mostrará los detalles específicos de cada paquete por punto de monitoreo, indicando el número de flujos de voz evaluados y el registro de cuántos flujos de voz.

Para calidad de escucha será presentados valores promedio, mínimo y máximo de tasa de señal en la voz.

Para calidad de conversación se debe presentar valores promedio, mínimo y máximo de Retardo de la voz.

En el caso de los problemas de red que afectan a los flujos de voz, se presentará Jitter promedio, mínimo y máximo (ms) pérdida (%) y retardo de ida y vuelta (ms) para voz.

Será capaz de acceder a la lista de los flujos de voz evaluados con los valores numéricos para cada una de las métricas clave mencionadas anteriormente.

Mostrará una pantalla con las alertas de la localidad seleccionada, así como pantallas para los flujos de voz de esa localidad.

La información de cada flujo de voz contendrá datos como la dirección IP y el puerto de origen, la dirección IP y el puerto de destino, hora de inicio y fin del flujo, duración, códec utilizado, MOS IP, IP MOS mínimo, porcentaje de pérdida de paquetes y jitter.

Para cada flujo de voz también será posible mostrar una vista lógica de la red con cada segmento evaluado, con los terminales de comunicación, las sondas colectoras y los valores de Indicadores clave obtenidos en cada punto de evaluación disponible.

Habrá una lista de los flujos de voz relacionados con la conversación seleccionada que indica la dirección de cada flujo de voz y los valores obtenidos en cada una de las métricas clave.

En los detalles del flujo de voz se presentará un resumen para las informaciones de red (VLAN, DiffServ IP, IP TTL) y métricas de paquetes (número total, porcentaje de pérdida, la pérdida consecutiva de paquetes media y máxima, Jitter mínimo y máximo, porcentaje de paquetes fuera de secuencia).

Será capaz de emitir los siguientes tipos de reportes como mínimo:

Ejecutivo, con información sobre los acontecimientos, la declaración de las métricas clave de voz.

De Negocio, que muestra diversos parámetros según la ubicación.

De Servicio, con resumen de llamadas

De Operación, con la información del dispositivo en comparación con las métricas clave, para identificar los patrones de errores y el rendimiento.

El sistema de monitoreo será capaz de generar alarmas en tiempo real respecto a la degradación de voz, basadas en los siguientes criterios; pérdida de paquetes, jitter, nivel de volumen de voz, nivel de ruido, SNR (signal-to-noise radio), distorsión de la voz, eco y retraso.

En la sección del filtro de eventos permitirá el filtrado de eventos por:

Una extensión,

Una identificación de usuario y Dirección IP.

Intervalo de tiempo y/o localidad.

En los detalles de los eventos se incluirá; Número del llamante, Número llamado, Hora de inicio de llamada, Duración de la llamada, Diagnóstico de la llamada, Dispositivo del llamante y Dispositivo del llamado.

Existirá una pantalla de resumen de los problemas actuales donde aparecerán los eventos más significativos en términos de porcentaje de los flujos afectados en todo el sistema, con la Descripción del problema / evento, Número de flujos afectados, Porcentaje de flujos afectados, Principio de la ocurrencia, si persiste su duración y si ha finalizado el horario de finalización.

Presentará una pantalla orientada al análisis de problemas donde se despliegue la matriz de todas las subredes dadas de alta en el sistema y cruzando las mismas con indicadores clave de desempeño y desde los cuales se pueda realizar un análisis profundo subsecuente (drilldown) hasta los flujos de voz correspondientes a ese evento, así como alertas relacionadas.

Reportes de Análisis de Tráfico y Monitoreo de Aplicaciones

Con el objetivo de contar con la información para controlar y monitorear el centro de datos, LAN, Internet, VPNs y servidores, el NOC Proporcionará a través de la herramienta de análisis de tráfico y aplicaciones al menos los siguientes reportes:

Estos reportes podrán ser solicitados de manera diaria, semanal, mensual e histórica y serán parametrizables con al menos las siguientes variables:

Disponibilidad del enlace.

Centro de Datos

VPN

Internet

LAN

Utilización de ancho de banda de todos y cada uno de los nodos.

Bytes de entrada/salida

Top Aplicaciones que corren por la Red.

Top de IP que más tráfico generan.

Top de Conversaciones que más tráfico generan.

Tabla del comportamiento de todas las aplicaciones que corren por la Red.

Tiempos de respuesta de cada nodo hacia MPLS, INTERNET y Centros de Datos.

Tiempos de Respuesta de las aplicaciones que corren por cada enlace.

Peores tiempos de respuesta de Aplicaciones.

Peores tiempos de respuesta de Servidores.

Cantidad de retransmisiones

Número de peticiones a un servidor en especifico

Número de peticiones satisfactorias y fallidas

Contadores TCP para las aplicaciones en donde aplique este criterio.

El sistema será capaz de generar estos reportes en formato HTML, PDF, Web y podrán ser enviados vía correo electrónico.

Requerimientos Técnicos:

Los equipos de monitoreo tendrán puertos para monitoreo y de gestión.

Conexión vía Port mirror o TAP divisor del medio.

Tecnología 10/100/1000 o 10G según aplique el tipo de monitoreo o el sitio a monitorear.

Capacidad de almacenamiento según la capacidad del nodo a monitorear.

El sistema trabajará sobre plataforma Linux.

Soportará fuente de poder redundante.

Controlador de disco duro SATA RAID.

Atención a Incidentes

OPERBES, S.A. DE C.V. contará con el servicio de soporte en sitio para el nodo desde su acometida hasta las puntas de conexión con el equipamiento de SHF.

OPERBES, S.A. DE C.V. se integrará al plan de marcación de SHF que así lo solicite, sin que esto represente un costo adicional.

El NOC contará con asistencia técnica las 24 horas del día, el cual incluirá un servicio telefónico gratuito (01800) para el interior del país y un número local para la ciudad de México, para lo cual deberá entregar en el apartado Mesa de ayuda, NOC, SOC, la documentación solicitada como parte de su propuesta técnica:

Detalle de los procedimientos para los diferentes niveles de escalación de servicio a reporte de incidentes.

Descripción del uso y manejo de las bitácoras mensuales de reportes de incidentes atendidos.

Descripción de sus servicios del centro de asistencia a través de WEB y/o correo electrónico.

Definir claramente su procedimiento de escalación para la atención de incidentes en cuatro niveles, en donde refleje a los responsables y sus cargos, así como datos para su localización, como celular, correo electrónico, teléfono de oficina.

Se especifica que el NOC de OPERBES, S.A. DE C.V. para el seguimiento de reportes de incidentes, en sus cuatro niveles con un procedimiento de escalamiento que se sujete a los siguientes tiempos:

5 min. Recepción del reporte en el centro de atención correspondiente.

1 HR primer nivel de escalamiento.

2 HR segundo nivel de escalamiento.

3 HR tercer y último nivel de escalamiento.

Teléfonos de oficina, y celulares de los responsables de cada nivel).

OPERBES, S.A. DE C.V. cumplirá con los niveles de servicio solicitados, para lo cual contará, con soporte del(los) fabricante(s) de los elementos involucrado.

SHF de así requerirlo podrá solicitar el escalamiento con el fabricante en caso de incidentes recurrentes y/o de alta criticidad y/o que impacte los niveles de servicio.

OPERBES, S.A. DE C.V. administrará la red de manera proactiva, recomendando cambios a los anchos de banda y/o calidades de servicio antes de que el desempeño de la red se vea impactado.

Servicio de Monitoreo de la Disponibilidad de Aplicaciones WEB

OPERBES, S.A. DE C.V. ofrece a SHF considerando que podrá solicitar bajo demanda una solución que permita mantener en vigilancia las páginas, sitios, portales o aplicaciones Web de la misma; publicados y visibles desde Internet, monitoreando la disponibilidad de los mismos (activos y en condiciones normales de operación). En caso de que algún sitio o URL se inhabilite, no responda o trabaje inadecuadamente, se alertará inmediatamente a los responsables asignados por SHF.

OPERBES, S.A. DE C.V. tomó en consideración que estas páginas o sistemas serán definidas por SHF y podrán estar basadas en tecnologías HTML, JAVA, JAVA SCRIPT, FLASH, entre otras; al menos soportadas por las plataformas Apache, Microsoft IIS.

Se cumplirá y operará al menos con lo siguiente:

Monitoreo de la disponibilidad de todos los servicios Web o URL's de SHF.

Monitoreo a través de una herramienta automatizada con la cual se verifique, en intervalos regulares, la disponibilidad del servicio HTTP/HTTPS para cada uno de los sitios definidos por SHF.

La herramienta de monitoreo estará en el NOC OPERBES, S.A. DE C.V., se brindará el acceso a la herramienta vía HTTPS, mediante cuentas con rol de solo lectura, tanto de forma interna a la red de SHF como de forma externa (a través de internet).

Se incluirá en la propuesta los manuales, guías, orientación, referencias o transferencia de conocimiento necesarios, sin costo adicional para SHF, para que el personal que esta designe, cuente con los conocimientos y/o habilidades para realizar consultas y generar reportes personalizados en dicha herramienta.

OPERBES, S.A. DE C.V. tomó en consideración que el intervalo de poleo será inicialmente de 120 segundos para cada sitio sin que represente ningún tipo de afectación. SHF podrán modificar el intervalo de poleo por sitio en cualquier momento durante la vigencia del contrato.

OPERBES, S.A. DE C.V. notificará al personal responsable designado por SHF, vía telefónica (en caso de que no contesten en 2 llamadas o intentos seguidos, se dejará mensaje de voz y enviar SMS al celular del personal) y correo electrónico, cualquier pérdida de disponibilidad y recuperación con base en los siguientes puntos:

Si el servicio no responde en el intervalo de poleo, se enviarán otros tres intentos dentro de los siguientes 120 segundos.

En caso de que no se haya restablecido la disponibilidad, SHF requiere que se compruebe la pérdida del servicio de forma manual a través de un enlace independiente al utilizado por la herramienta de monitoreo en 120 segundos.

En caso de comprobar la no disponibilidad del servicio, se notificará a SHF de inmediato.

En el momento de que se detecte la recuperación y estabilización del servicio por al menos 15 minutos, se notificará a SHF.

OPERBES, S.A. DE C.V. tomó en consideración que se requiere que se almacene la información registrada en la herramienta por tres meses en línea, al menos con la siguiente información:

Monitoreo de Dominios

Monitoreo de IPs

Tiempo promedio de disponibilidad.

OPERBES, S.A. DE C.V. entregará un reporte en caso de que se presenten problemas críticos de no disponibilidad.

Centro de Operaciones de Seguridad (SOC)

OPERBES, S.A. DE C.V. ofrece 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. OPERBES, S.A. DE C.V. 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 OPERBES, S.A. DE C.V. OPERBES, S.A. DE C.V. aplicará la pro actividad (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, OPERBES, S.A. DE C.V. cumplirá como mínimo las siguientes especificaciones:

SHF contará con acceso de sólo lectura en los equipos de seguridad utilizados para la prestación del servicio no obstante que sean propiedad OPERBES, S.A. DE C.V., con el fin de poder supervisar y evaluar la configuración de los mismos.

El SOC de OPERBES, S.A. DE C.V. proporcionará a SHF, la atención a sus necesidades en cuanto a solicitud de cambios, reportes y atención de incidentes, así como consultas con relación al estado de la seguridad perimetral y de la RPV MPLS en un horario de 7x24 los 365 días del año.

Para nuevas versiones de sistema operativo, parches, o de cualquier actualización en software ambiental recomendada por el fabricante, para la correcta operación de los dispositivos; la aplicación de las actualizaciones por parte de OPERBES, S.A. DE C.V. no excederá las 48 horas desde que el fabricante informa sobre la necesidad o conveniencia de aplicarla y será programada en caso de que afecten la disponibilidad del equipo. Si la aplicación es urgente se hará del conocimiento y aprobación por parte de SHF, para evitar riesgos a la operación. En ambos casos estará evaluado por OPERBES, S.A. DE C.V. y con el visto bueno por SHF.

Corrección de vulnerabilidades del software de seguridad, ya sea de forma remota o en sitio en caso de contingencia.

El Centro de Operaciones de Seguridad configurará y aplicará políticas de control de acceso a los equipos de seguridad perimetral e infraestructura de la RPV MPLS.

OPERBES, S.A. DE C.V. Contará con las herramientas para el registro, notificación, seguimiento y coordinación para la atención a fallas.

Supervisará y llevará el control, mantenimiento y actualización de inventarios de los equipos de seguridad, incluyendo por lo menos la ubicación, modelo, número de serie, software instalado y versiones tanto en software y hardware.

Realizará la administración de desempeño de los equipos de seguridad desde la herramienta de monitoreo. Los reportes de desempeño estarán disponibles para el Administrador de la Red de SHF vía web para su consulta.

OPERBES, S.A. DE C.V. llevará un proceso de control de cambios que se sujete a la aprobación de un comité conformado por los responsables de cada servicio tanto de SHF como de OPERBES, S.A. DE C.V. El control de cambios se apegará al MAAGTIC-SI vigente o en su caso el que lo sustituya.

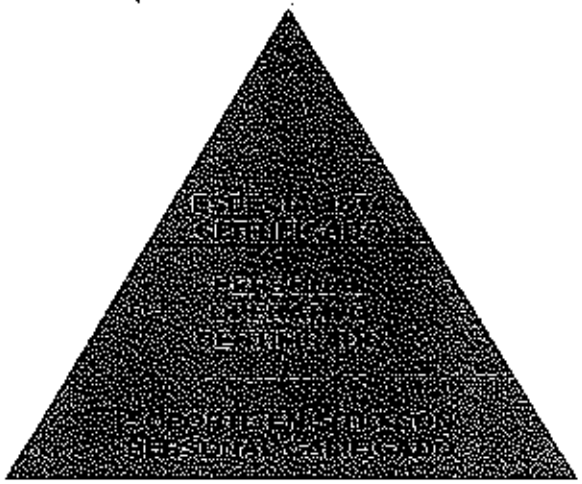
OPERBES, S.A. DE C.V. considera los siguientes tipos de control de cambios.

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	SLA del nodo.

Tipo de Cambio	Definición	Tiempo de Solución
	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.	
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 hrs. después de la solicitud de SHF

Tabla: 4.3.1

Modelo de Operación SOC Y NOC



Gráfica: 4.3.1

OPERBES, S.A. DE C.V. comprueba que cuenta 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 OPERBES, S.A. DE C.V.

Los Recursos Humanos indicados anteriormente serán responsables de garantizar que los servicios que preste OPERBES, S.A. DE C.V. 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, OPERBES, S.A. DE C.V. tomó en consideración que Además de la documentación que se consignará 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.

OPERBES, S.A. DE C.V. asegura 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 la RPV.

Asegurar el correcto funcionamiento del sistema operativo correspondiente para las soluciones del software de seguridad perimetral y de infraestructura de la RPV MPLS.

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 la RPV MPLS.

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, OPERBES, S.A. DE C.V. lleve 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 OPERBES, S.A. DE C.V. bajo la supervisión del área técnica de cada área solicitante.

En el Apartado SOC y NOC se presentan las certificaciones del personal considerado por OPERBES, S.A. DE C.V. para la prestación del servicio.

Los recursos Humanos que OPERBES, S.A. DE C.V. 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 OPERBES, S.A. DE C.V., 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.

Los Recursos Humanos indicados anteriormente ejecutarán la operación de los servicios que OPERBES, S.A. DE C.V. preste a SHF.

Como parte del servicio y dependiendo de las necesidades de SHF según las tecnologías del "Anexo VIII. Matriz de Servicios", se incluye en sitio al menos 1 Ingeniero independiente del personal que OPERBES, S.A. DE C.V. 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 OPERBES, S.A. DE C.V. cumple con:

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.

Realizar la detección pro-activa de fallas mediante la generación de alarmas.

Notificar automáticamente las alarmas de cada dispositivo de seguridad para la escalación de la falla hacia el sistema de la Mesa de Ayuda.

Notificar automáticamente vía correo electrónico y/o vía telefónica a los responsables asignados por SHF al detectarse un incidente de seguridad.

Herramienta de monitoreo con acceso vía HTTPS para al menos 3 usuarios simultáneos de SHF.

Monitoreo del desempeño de los equipos de seguridad, incluyendo utilización de CPU, memoria, errores.

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

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 asigne a OPERBES, S.A. DE C.V., indicando nombre, cargo, correo electrónico y teléfono celular.

SHF, tendrá derecho a solicitar en cualquier momento a OPERBES, S.A. DE C.V., 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 OPERBES, S.A. DE C.V. en caso de ser el licitante ganador, como parte de las reglas de operación.

Herramientas de Monitoreo

OPERBES, S.A. DE C.V. incluye 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.

Monitoreo en línea de las alarmas de seguridad generadas en los equipos de seguridad.

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 OPERBES, S.A. DE C.V. proporcionará 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, OPERBES, S.A. DE C.V. proporcionará un número local alternativo.

OPERBES, S.A. DE C.V. tomó en consideración que integrará una punta a la MPLS solo cuando el uso exceda del 5% del ancho de banda en cualquier enlace de SHF para el monitoreo, gestión y correlación de los equipos, así como la comunicación de voz IP, dicho enlace independiente no excedera del 70% del uso del ancho de banda para éste servicio durante la vigencia del contrato, quedando siempre bajo su responsabilidad.

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 zero).

OPERBES, S.A. DE C.V. contará con una matriz de severidades la cual se definirá con SHF para la identificación de incidentes de seguridad usando una plataforma para la correlación de eventos que le permitan identificar un Incidente (evitar falsos positivos) con mínimo los siguientes niveles:

Crítico: Incidente de alto impacto dado el riesgo que representa; puede, potencialmente, ocasionar afectación y/o daño en activos y/o servicios de SHF. Afectación total al servicio, pérdida total de algún dispositivo de seguridad o bien mediante la explotación de vulnerabilidades críticas en la infraestructura protegida.

Medio: Incidente serio en el que hay una degradación, más no una afectación a los servicios e infraestructura que es protegida mediante las soluciones de seguridad. Bloqueo o bajo desempeño al acceder a ciertos servicios de red que requieren el uso de los dispositivos de seguridad así como la pérdida parcial de alguna funcionalidad. Degradación en el servicio sin llegar a ocasionar caída del mismo.

Estándar: Incidente menor que no trae consecuencias de impacto a los servicios e infraestructura protegida por las soluciones de seguridad. El incidente se da mediante fallas en visualización de bitácoras o problemas para comunicación de servicios internos del cliente.

El Centro de Operaciones de Seguridad detectará y mitigará proactivamente los incidentes de seguridad catalogados como de día cero, y contará con 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 proporcionados, en tanto se determina la corrección que el propio fabricante publique.

Notificación de Incidentes de Seguridad (mecanismos: e-mail, teléfono fijo, teléfono móvil): Son las vías que OPERBES, S.A. DE C.V. empleará para comunicarse con el cliente ante cualquier incidente de seguridad.

Solución a Incidentes Críticos de Seguridad. OPERBES, S.A. DE C.V. se compromete con SHF a:

Identificar un Incidente catalogado como Crítico, con atención inmediata.
Descartar que se trate de un falso positivo
Alertar del incidente mediante los mecanismos ya descritos
Prevenir el ataque
E implementar solución de remediación (previa notificación a SHF). Siempre que no incluya equipo de cómputo de SHF.

Solución a Incidentes de tipo medio (60 minutos): Es el tiempo en el cual OPERBES, S.A. DE C.V. se compromete con SHF a:

Identificar un incidente catalogado como medio.
Descartar que se trate de un falso positivo
Alertar del incidente mediante los mecanismos ya descritos
Prevenir el ataque
E implementar solución de remediación (en caso de que aplique previa aprobación del cliente)

Solución a Incidentes de tipo estándar (24 horas naturales): Es el tiempo en el cual OPERBES, S.A. DE C.V. se compromete con SHF :

Identificar un incidente catalogado como bajo

Descartar que se trate de un falso positivo

Alertar del Incidente mediante los mecanismos ya descritos

Prevenir el ataque

E implementar solución de remediación (en caso de que aplique previa aprobación del cliente)

Una vez que la vulnerabilidad ha sido corregida por OPERBES, S.A. DE C.V. se procederá a realizar recomendaciones y tomar las medidas necesarias en los equipos de seguridad perimetral e infraestructura de RPV, para evitar que este tipo de incidencia se repita.

El tiempo de resguardo de información se determinará en conjunto con SHF, por lo menos 6 meses en línea y posterior Considerarpa de forma preventiva, la posibilidad de contar con equipos y espacio necesario para resguardar la información por la vigencia total del contrato, al término del contrato será entregada a los responsables que SHF designe.

OPERBES, S.A. DE C.V. contará con un proceso ya definido de respuesta a incidentes de seguridad, el cual será revisado por personal que SHF designe y afinado por OPERBES, S.A. DE C.V. de acuerdo a la retroalimentación recibida. Para esto, OPERBES, S.A. DE C.V. contempla las sesiones de trabajo necesarias para que el proceso quede totalmente adecuado a las necesidades de SHF.

OPERBES, S.A. DE C.V. documentará el proceso de atención a SHF para requerimientos de cambios, reporte de fallas, solución de dudas.

OPERBES, S.A. DE C.V. presentará sus reportes tipo a generar como resultado de la operación, para que SHF los pueda revisar y, de acuerdo a sus necesidades, solicitar los cambios que considere pertinentes.

Reportes Estándar: Son los reportes predefinidos a los cuales SHF,tiene acceso para validar el desempeño del servicio contratado

Reportes Personalizados: Es la capacidad para poder definir y ejecutar reportes a la medida del cliente en formato mínimo PDF.

Asistencia Técnica en Sitio y Remota

OPERBES, S.A. DE C.V. considera en su proposición los recursos técnicos y humanos necesarios con experiencia de al menos 3 años en administración 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. OPERBES, S.A. DE C.V. deberá:

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.

El personal asignado por OPERBES, S.A. DE C.V. para la administración monitoreo y soporte en sitio de la red RPV, 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) regional(es).

OPERBES, S.A. DE C.V. supervisará y en su caso corregir en forma proactiva, el estado lógico y físico de los equipos y enlaces de comunicaciones ofertados, utilizando para ello la infraestructura instalada en punto "Servicio de Operación"

OPERBES, S.A. DE C.V. será el 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.

OPERBES, S.A. DE C.V., 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 indique 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 RPV, 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.

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.

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

Ejecución de altas, bajas y cambios, en la infraestructura, considerando:

Altas, como la nueva configuración o nuevo servicio del sistema de la red RPV, Internet y solución de seguridad

Bajas, como la eliminación de un servicio integrante del sistema de la red RPV, Internet y solución de seguridad

Cambios, como cualquier modificación en la configuración de la infraestructura que permita la reubicación de equipos terminales.

OPERBES, S.A. DE C.V. contará 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.

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

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

Entrega de Servicios

Implementación de Servicios al Inicio del Proyecto

OPERBES, S.A. DE C.V. cumplirá con las fechas de instalación, de acuerdo al plan de trabajo de transferencia de servicios en el que detalla la entrega de los mismos. Dicho plan será propuesto por OPERBES, S.A. DE C.V., a SHF dentro de los 10 días hábiles a la firma del contrato y SHF realizará los comentarios pertinentes para su ajuste y aprobación final.

Se realizará una junta de inicio de proyecto con SHF, que será realizada con el Administrador del Proyecto y el personal que designe SHF. Posteriormente se deberán realizar juntas de seguimiento. La periodicidad de estas juntas será establecida durante la junta de arranque.

Con el fin de garantizar la correcta ejecución del proyecto, durante el desarrollo OPERBES, S.A. DE C.V. considera la participación de un Project Manager Professional que estará certificado por el PMI (Project Management Institute) para lo cual entrega copia de la documentación que lo acredite dentro de su proposición junto con el original para su cotejo. Las funciones que desarrollará son las siguientes, las tareas son enunciativas y no limitativas:

Plan de Trabajo de la Implementación

Desarrollo del Plan de Trabajo

Control del Plan de Trabajo

Seguimiento a las actividades y ejecución del Plan de Trabajo

Notificar a SHF sobre desviaciones en el Plan de Trabajo.

Entrega de la memoria técnica final a SHF.

El plan de trabajo de la implementación de los servicios solicitados por SHF será detallado por día y durante el desarrollo del proyecto se elaborará un reporte de avance donde se incluyan las desviaciones del proyecto.

OPERBES, S.A. DE C.V. entregará en la etapa de instalación de cada uno de los servicios solicitados, un inventario de todos y cada uno de los equipos y productos de software que formen parte de la solución propuesta el cual será validado por personal técnico de SHF.

El PMP deberá fungir como único punto de contacto entre SHF y OPERBES, S.A. DE C.V. durante la fase de implementación de la red.

OPERBES, S.A. DE C.V. asignará una Oficina de Proyectos (PMO) para ejecutar la implementación de manera efectiva para SHF.

OPERBES, S.A. DE C.V. y el Licitante de servicios actual, podrán establecer acuerdos de operación y comerciales que apoyen la transferencia de los servicios.

Los horarios de migración de los nodos se establecerán en coordinación con SHF.

Se considerará que los servicios son entregados al 100%, cuando OPERBES, S.A. DE C.V., cumpla con todos los puntos definidos en el formato de verificación de puesta en operación de los servicios solicitados por SHF y firmado de conformidad.

OPERBES, S.A. DE C.V. considera los servicios profesionales por parte del Fabricante para todas las tecnologías, para el diseño de la arquitectura, instalación, configuración, parametrización, pruebas, puesta en operación y ajuste fino de todas las soluciones integradas para el desarrollo del servicio. El diseño estará basado en mejores prácticas.

OPERBES, S.A. DE C.V. tomo en consideración al menos 3 meses de operación asistida por parte del fabricante una vez que se dé por terminada la instalación y configuración de los equipos propuestos.

OPERBES, S.A. DE C.V. tomó en consideración la asistencia por parte del fabricante hasta 2 eventos al año en caso de que algún incidente o falla no permita brindar los niveles de servicio solicitados, requerido soporte en sitio y sin costo para SHF

Entrega de Servicios Durante la Vigencia del Contrato

OPERBES, S.A. DE C.V. tomó en consideración que una vez concluido el plan de trabajo inicial de la entrega de los servicios, los tiempos de entrega máximos que se cumplirán durante la vigencia del contrato son los siguientes:

Puesta en servicio de nuevos nodos: 6 semanas.

Para cambios de domicilio de nodos existentes, SHF y OPERBES, S.A. DE C.V. determinarán de común acuerdo las fechas de baja y activación del nuevo domicilio, las cuales no excederán de 6 semanas contadas a partir de la notificación formal. Los costos por cambio de domicilio se requieren con precio unitario para SHF.

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

Modificaciones a anchos de banda, siempre y cuando no sean bajo demanda e impliquen un cambio físico en él o los enlaces de transmisión (incrementos por configuración): 5 días naturales. Si implican cambio físico aplican los tiempos de cambios de domicilio.

Modificaciones a anchos de banda para nodos bajo demanda que impliquen un cambio físico en él o los enlaces de transmisión, se requieren incrementos y decrementos, aplican los tiempos de cambio de domicilio.

Puesta en servicio de videoconferencia solicitado por SHF, será de 4 semanas.

OPERBES, S.A. DE C.V. tomó en consideración que estos tiempos comenzarán a contar a partir de que se emita la solicitud de servicios correspondientes por parte de SHF.

Las notificaciones y/o respuestas serán válidas formalmente por oficio o de forma electrónica.

OPERBES, S.A. DE C.V. contempla la integración dentro de la RPV-MPLS los Nodos que requieran los proveedores de SHF para su integración, cumpliendo con las mismas características en cuanto a niveles de disponibilidad, precio, enlaces e infraestructura. El proceso de contratación del servicio será tratado directamente entre OPERBES, S.A. DE C.V. de la RPV-MPLS y el proveedor de SHF.

Entregable Final para la Aceptación Formal y Pago de los Servicios

Las entregas se darán por concluidas mediante el formato de verificación de puesta en operación de los servicios, el contenido de dicho formato, así como las firmas reconocidas para el mismo y otros aspectos serán definidos con OPERBES, S.A. DE C.V. y SHF, previo a la puesta en operación del servicio.

OPERBES, S.A. DE C.V. tomó en consideración que el siguiente material será entregado a SHF, como entregable final del desarrollo del proyecto, dentro de los 15 días naturales después de la implementación del último nodo descrito en el "Anexo VIII. Matriz de Servicios":

Documento de implementación del plan de continuidad de la operación de los servicios de la RPV-MPLS.

Documento de análisis de impacto en la operación de los servicios de la RPV-MPLS.

Documento de análisis de riesgos en la operación de los servicios de la RPV-MPLS.

Documento de estrategia de reanudación y continuidad de la operación de los servicios de la RPV-MPLS.

Metodología del mantenimiento al plan de continuidad de la operación de los servicios de la RPV-MPLS.

La aceptación formal del inicio del servicio y para propósito del inicio de la facturación del mismo será en el momento en que se concluya con la instalación y puesta a punto de la totalidad de los servicios, la cual deberá ocurrir a más tardar a la fecha de fin de transición de los servicios identificados en el "Anexo1: Servicios" como "Entrega inicial mínima", los cuales incluyen en forma enunciativa enlaces de última milla, CPE's, nodos, equipos, e interconexión, sistema de administración y monitoreo, así mismo deberán cumplir con las pruebas que SHF y el Licitante definan en la fase de planeación y en forma mínima con las pruebas que a continuación se detallan tanto en la Red Privada Virtual, el Acceso a Internet y solución de seguridad.

Red Privada Virtual

Se realizarán llamadas simultaneas en función de la capacidad del nodo, las cuales no deberán presentar degradación, eco y retardo que impidan llevar una conversación continua e inteligible y al colgar cualquiera de las extensiones, se deberá liberar en forma automática el canal.

Se realizarán pruebas de transmisión de fax, sin que se presenten problemas de cortes en la transmisión y recepción de documentos.

Se realizarán pruebas simultáneas de transmisión de voz y datos sin que se tenga degradación en cualquiera de los servicios. Para ello se utilizará el máximo de canales de voz disponibles en el nodo a prueba.

Se validará que el nodo del Centro Alterno en forma alternativa al nodo central, cuente con la conectividad y comunicación con cada uno de sus nodos remotos y regionales.

Se analizara el tráfico que circula por cada enlace para corroborar que la información viaje en forma cifrada.

Se validará que la infraestructura que integra el servicio este reconocida e incorporada al sistema de administración y monitoreo propuesto por OPERBES, S.A. DE C.V., en las instalaciones de SHF.

Acceso a Internet

Se validará el esquema de direccionamiento homologado asignado para los nodos centrales y centro alterno para SHF que así lo requieran.

Se validará que desde los nodos central y centro alterno se cuente con la conectividad y acceso a Internet de acuerdo a las capacidades solicitadas en cada nodo.

Se validara la resolución de nombres de dominios internos y externos, desde cada uno de los equipos Servidores DNS proporcionados.

Se comprobara que los dominios y certificados digitales SSL listados en el punto 2.5 de este anexo hayan sido transferidos con el rol de pago, al contacto designado por el prestador de servicios.

Solución de Seguridad.

Se validará el cumplimiento de la infraestructura de seguridad propuesta (FW) en cuanto a sus capacidades y características mínimas presentadas:

Modelo

Memoria

Interfaces

Se validara la aplicación y correcta funcionalidad de las políticas y reglas configuradas en forma mínima necesarias para la sustitución del servicio.

Al cumplimiento total de las pruebas de aceptación de los servicios se firmara el acta de aceptación y a partir de ésta fecha empezará a contar la facturación.

Al cumplimiento total de las pruebas de aceptación de los servicios se firmara el acta de aceptación y a partir de ésta fecha empezará a contar la facturación.

Memoria Técnica

Al final de los trabajos de instalación, OPERBES, S.A. DE C.V. entregará una Memoria Técnica en papel y medio electrónico, reflejando los aspectos técnicos de la infraestructura auxiliar implementada para cada nodo, misma que incluirá al menos la siguiente información:

La infraestructura a instalar por parte OPERBES, S.A. DE C.V. estará debidamente etiquetada en un lugar visible para su identificación.

Índice

Descripción del Sistema Integral (solución UPS, aire acondicionado, tierra física, rack´s y acondicionamiento eléctrico)

Descripción del equipo instalado para la solución de acceso a la RPV-MPLS

Planos de la Red que incluyan ubicación del sistema de tierras y acondicionamiento eléctrico

Diagramas de conexión.

Pruebas (del sistema de cableado estructurado, validación del tiempo de respaldo de la solución UPS, del sistema de aire acondicionado, pruebas de conexión hacia la RPV-MPLS y hacia la LAN de SHF.

Una fotografía de cada uno de los siguientes sistemas: tierra física, aire acondicionado, rack de comunicaciones, acondicionamiento eléctrico y solución UPS.

Transferencia de Conocimiento

OPERBES, S.A. DE C.V. proporcionará la transferencia de conocimiento con instructores certificados, al personal de SHF, que requiera de alguna de las soluciones de seguridad para cada una de las tecnologías que proponga el Licitante, a nivel certificación. Deberá entregar a los participantes la constancia correspondiente avalada por el fabricante en los siguientes temas:

Solución del Repositorio de Información

Solución de Monitoreo (Todas las Instaladas), Informes de Gestión y Administración de Niveles de Servicio

Solución de Mesa de Ayuda

Soluciones de Seguridad (Todas)

Solución de análisis de Tráfico

Tecnología de la Red Privada Virtual MPLS

Solución de Administración de Tráfico

Solución de control de ancho de banda

Soluciones de contención de ataques perimetral y en la nube de internet.

Security Management ISO 27001

CISSP (Certified Information Systems Security Professional).

CISM (Certified Information Security Manager

CISA (Certified Information Security Auditor)

ITIL Fundamentals Versión 3

GIAC Incident Handler.

GCFA-GIAC (Certified Forensic Analyst).

Investigación forense en Intrusiones informáticas (investigación Digital)

Ethical Hacking o Hacking & Securiting

Criptografía

OPERBES, S.A. DE C.V. considera un seguro de certificación el cual cubrirá los costos de certificación para el personal que SHF designe, incluyendo una segunda vuelta de examen para aquellos participantes que no aprueben al primer intento.

El calendario de estos cursos será propuesto por OPERBES, S.A. DE C.V. y autorizado por SHF ; los tiempos para proporcionar la totalidad de los cursos no excederán de seis meses a partir del inicio de vigencia del contrato.

Con el fin de garantizar la disponibilidad de la transferencia de conocimiento en el tiempo comprometido, la programación de los mismos se cubrirá con el mínimo de 5 personas de SHF sin generar ningún costo adicional y se efectuará dentro del plazo y lugar definido en bases.

OPERBES, S.A. DE C.V. tomó en consideración que la transferencia de conocimiento se efectuará en la Ciudad de México; sin embargo, en caso de existir viáticos, transporte y hospedaje del personal de SHF para asistir a la transferencia de conocimientos, serán cubiertos por SHF. Así mismo, será responsabilidad de SHF que su personal cubra con ciertos pre-requisitos en caso de existir. Serán certificados por los fabricantes. Cuando no se proporcione la transferencia de conocimientos certificados se impartirán personalizados avalados por el fabricante y que estos permitan la certificación, previa autorización por parte de SHF.

Capacitación presencial, impartida por centro o socio de entrenamiento certificado por el fabricante que cuente con Instructores certificados para la impartición de cursos ofertados, contar con material original y certificado así como presentación visual y laboratorios requeridos. OPERBES, S.A. DE C.V. en caso de ser el licitante ganador entregará dentro de la propuesta técnica, un documento que haga constar por parte del fabricante de la tecnología propuesta, que el centro que desea entregar la transferencia de conocimientos se encuentra autorizado por éstos.

Reporte del Servicio

OPERBES, S.A. DE C.V. tomó en consideración que aplicará para todos los reportes y será condicionante para el pago de la factura.

Con el objeto de medir el desempeño de los servicios proporcionados por OPERBES, S.A. DE C.V., será necesario generar los reportes de comportamiento, desempeño y disponibilidad de la RPV-MPLS con la cual se proporcionen los servicios solicitados, de acuerdo con los niveles de servicio definidos. Estos reportes serán entregados de forma electrónica.

Los reportes serán entregados por OPERBES, S.A. DE C.V., a SHF de la siguiente forma, enunciativa más no limitativa, son:

Número de Reporte	Nombre/Descripción	Frecuencia del Reporte
1	Administración de configuraciones Cambio en la infraestructura Actualización de una memoria técnica integral de los servicios	Cada mes durante los primeros 7 días hábiles por nodo de la RPV-MPLS
2	Reporte de Atención y solución de Incidentes que contenga lo siguiente: Tipos de Incidentes Tiempo de solución (TTR) Si afectan o no la disponibilidad	Cada mes durante los primeros 7 días hábiles por nodo de la RPV-MPLS
3	Reporte por nodo de: Disponibilidad Latencia Utilización de ancho de banda QoS Calidad del Servicio Pérdida de Paquetes por nodo Degradación por Pérdida de Paquetes del acceso a Internet	Cada mes durante los primeros 7 días hábiles por nodo de la RPV-MPLS
4	Informes de gestión del NOC y/o SOC (Mesa de Ayuda)	Cada mes durante los primeros 7 días hábiles por nodo de la RPV-MPLS
5	Reportes de Análisis de Tráfico de DATOS WAN Utilización de ancho de banda por nodo Top de aplicaciones por nodo Top de IP's que más tráfico generan por nodo Top de conversaciones que más tráfico generan por nodo Tiempos de respuesta de cada nodo Peores tiempos de respuesta por nodo Reportes por QoS por nodo LAN Top de utilización de ancho de banda por IP Top de conversaciones especificas origen-destino Peores tiempos de respuesta por aplicación Distribución de los Protocolos de Red.	Cada mes durante los primeros 7 días hábiles
6	Reportes de Análisis de Tráfico de VOZ Porcentaje de llamadas con MOS por arriba del umbral establecido Top de llamadas con Jitter alto	Cada mes durante los primeros 7 días hábiles

Número de Reporte	Nombre y Descripción	Frecuencia del Reporte
	Reportes de calidad de Voz Top de pérdida de paquetes de Voz por ID Delay de voz por ID	
7	Reportes de las soluciones de seguridad con las que cuenta SHF Métricas de desempeño (%Procesador, %Memoria, %Disco Duro, donde apliquen) Puertos TCP/UDP y protocolos más utilizados Top 20 de las aplicaciones utilizadas o pasando a través de la solución Top 20 IP's más bloqueadas Top 20 de las Firmas de ataque más vistas Top de los 20 usuarios o cuentas, según tráfico y tiempo de conexión Top de las 20 páginas, según número de consultas y tiempo de conexiones Consumo de Ancho de banda por tipo de protocolo.	Cada mes durante los primeros 7 días hábiles por nodo de la RPV-MPLS
8	Reporte de actividades sospechosas e incidentes de seguridad mensuales	Cada mes durante los primeros 7 días hábiles por nodo de la RPV-MPLS

Todos los reportes se programarán y se generarán de manera sencilla y permitirán la agrupación de dispositivos y la concentración de distintas métricas en un solo reporte.

La interfaz de generación de reportes permitirá exportar de forma simple, y mínimo soportará la exportación a los siguientes formatos: PDF y CSV.

Reporte de Degradación en Servicio de Voz

Cuando exista una degradación en el servicio de Voz a través de la RPV-MPLS, incluyendo aquellas relacionadas con el manejo de la Calidad de Servicio de voz, OPERBES, S.A. DE C.V., realizará un análisis para determinar la causa raíz y realizará los ajustes necesarios en los equipos CPE, así como las recomendaciones pertinentes cuando las causas sean ajenas a él; para ello, OPERBES, S.A. DE C.V. tendrá hasta 24 horas para presentar el informe correspondiente.

La red de OPERBES, S.A. DE C.V. permitirá que se realicen mediciones de variación, en la latencia y/o el Jitter desde cualquier CPE hacia cualquier otro CPE por parte de SHF o quien ésta designe para tal fin.

Esta información, podrá ser utilizada para determinar si existen fenómenos de degradación en el servicio.

No se considerará degradación de voz, si existe en el mismo periodo del Incidente condiciones de no disponibilidad.

Optimización y Administración de Liberaciones en la RPV-MPLS

En todo momento OPERBES, S.A. DE C.V. como proveedor de la RPV-MPLS, será responsable de conducir todas las tareas relacionadas con la optimización del uso y configuración de la RPV-MPLS, con el fin de garantizar el correcto funcionamiento; así como el mejor desempeño de la misma. Esta responsabilidad, observará solicitudes y requerimientos especiales de configuración, que sean formalizados por SHF de manera expresa; a fin de satisfacer completamente las necesidades de SHF. Así mismo; OPERBES, S.A. DE C.V., acepta someter su implementación y configuración a un proceso de "Administración de Liberaciones" bajo ITIL por sus siglas en inglés, en caso de así determinarlo SHF. Para esto, OPERBES, S.A. DE C.V., proporcionará todas las facilidades,

autorizaciones, y accesos a información que le sean requeridos para conducir este proceso a satisfacción de SHF.

Repositorio de Información

SHF tendrá únicamente acceso a su repositorio correspondiente, con el fin de realizar consultas, modificaciones o aprobar documentos; a continuación se menciona parte de la información que al menos estará contenida en el repositorio, ya que durante la vigencia se podrá ampliar:

Información sobre la infraestructura de la RPV-MPLS

Direccionamiento IP

Calendario de Mantenimientos

Control de Cambios

Procesos para el Plan de Continuidad de la RPV-MPLS

Copias de las configuraciones (versión de sistema operativo, configuración lógica, configuración física) actualizadas de todos los CPE de la red MPLS

Memorias Técnicas de los nodos

Documentación de los incidentes, requerimientos y soluciones.

Planes de mejora de los servicios

Reportes de Niveles de Servicio

El acceso al repositorio de información será a través del protocolo a través de un canal seguro y cifrado con interfaz Web, al menos a 4 usuarios con sesiones simultáneas por SHF, en caso de requerir más accesos se solicitarán por escrito sin costo alguno para SHF.

Los roles de las cuentas de acceso serán de 3 tipos:

"Lector", solamente puede ver los documentos publicados.

"Autor", puede ver los documentos publicados y no publicados, añadir documentos, crear o borrar sus propias carpetas; editar, borrar y publicar cualquier documento en el sitio.

"Aprobador", puede ver las carpetas y documentos a los cuales tiene acceso, y puede revisar, aprobar o rechazar documentos.

La plataforma propuesta por OPERBES, S.A. DE C.V. tendrá las siguientes funcionalidades:

Control de versiones. La herramienta dará seguimiento de los documentos e impedirá que alguien pueda sobre escribirlos y guardará una versión de cada documento en el que se hayan introducido cambios.

Perfiles de documentos. La herramienta será capaz de agregar información a los documentos para plantear búsquedas de palabras clave, fechas de modificación o características.

Publicación de documentos. Los documentos publicados serán accesibles para los usuarios del portal en vistas privadas o públicas, el proceso de publicación de documentos será establecido de común acuerdo entre OPERBES, S.A. DE C.V. y SHF.

Al final del contrato OPERBES, S.A. DE C.V. entregará en medio electrónico el total de la información generada durante la vigencia del Contrato.

Transferencia de Servicios al Final del Proyecto

El nuevo Licitante ganador en su caso, deberá coordinar la transferencia de servicios con el OPERBES, S.A. DE C.V. (el Licitante ganador motivo del proceso de este documento), así como con futuros proveedores de servicios en el caso de un cambio, elaborando conjuntamente la logística de transición, misma que será avalada y autorizada por SHF.

El nuevo Licitante ganador y OPERBES, S.A. DE C.V., podrán establecer acuerdos de operación y comerciales que apoyen la transferencia de los servicios.

En el plan de transferencia de servicios de OPERBES, S.A. DE C.V. al nuevo Licitante ganador, este último deberá detallar la entrega de la infraestructura, instalación, configuración, puesta a punto y operación de los servicios. Este plan, incluirá un apartado de "RollBack" o regreso al punto de partida, en caso de no ser posible concluir al 100% la entrega de los servicios de acuerdo al plan de migración presentado en su proposición a cada una de SHF.

Conforme se vayan migrando los servicios a la infraestructura del nuevo Licitante ganador, el nodo de la RPV-MPLS migrado tendrá conexión a todos los nodos de SHF (Migrados y No Migrados), así como acceso al Centro de Cómputo Institucional de SHF para cursar tráfico de voz.

En caso que se requiera, el nuevo Licitante ganador, se coordinará con el proveedor actual del servicio de RPV-MPLS, a fin de cumplir con el plan de migración presentado en su proposición a SHF.

OPERBES, S.A. DE C.V. tomó en consideración que deberá desmontar los equipos de su propiedad y proporcionar las facilidades para el montaje de los equipos suministrados por el nuevo Licitante ganador.

Condiciones Técnicas para la Transmisión a un Nuevo Proveedor Posterior al Término del Contrato

La obligación de OPERBES, S.A. DE C.V. como prestador del servicio durante el periodo de transición a un nuevo contrato de servicios, se deberá realizar bajo las siguientes condiciones:

OPERBES, S.A. DE C.V. garantizará los niveles de servicios durante el procedimiento de contratación de un nuevo "proyecto".

OPERBES, S.A. DE C.V. al término de este proyecto, garantizará los niveles de servicio durante el periodo de transferencia de servicios al nuevo Licitante.

En su caso, OPERBES, S.A. DE C.V., integrará la infraestructura necesaria para conectarse al nuevo Licitante.

OPERBES, S.A. DE C.V., durante el periodo de transición que podrá durar máximo 4 meses, mantendrá la infraestructura que proporcione el servicio de la red virtual a SHF con objeto de que el nuevo Licitante integre su infraestructura total de solución y no afecte sus procesos de operación.

Adicionalmente, es importante mencionar que OPERBES, S.A. DE C.V., dará todas las facilidades que SHF considere pertinentes; para garantizar la transparencia en el proceso de transición al nuevo Licitante de servicios.

Durante la etapa de migración de los servicios, OPERBES, S.A. DE C.V., retirará todos los equipos que hubieran sido parte de la solución y que sean única y exclusivamente de su propiedad; a solicitud de SHF, dichos retiros formarán parte del acta de liberación del servicio y será requisito para la liberación de la Garantía de Cumplimiento del Contrato.

En su caso, OPERBES, S.A. DE C.V., se coordinará con el nuevo Licitante para realizar la migración progresiva del proyecto.

OPERBES, S.A. DE C.V., durante el periodo de transición hacia el Nuevo Licitante de RPV-MPLS, 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 OPERBES, S.A. DE C.V., SHF y el Nuevo Licitante sobre los servicios con objeto de no afectar la operación de la Red Virtual de SHF.

Es importante señalar que OPERBES, S.A. DE C.V., en conjunto con SHF, apoyará a la integración continua y transparente de los servicios bajo las prioridades y normas que SHF determine.

Niveles de Servicio

Descripción del Servicio

Los niveles de servicio estarán relacionados a la RPV-MPLS, Internet y otros servicios en términos de disponibilidad, desempeño del servicio, entrega de los servicios, tiempo de solución a Incidentes (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.

OPERBES, S.A. DE C.V. entregará a SHF los reportes del servicio solicitados en este documento. La evaluación se realizará tomando como base los reportes registrados en las Mesas de Ayuda de SHF, utilizando sus herramientas de medición; para la evaluación del servicio ofertado y el resultado del nivel de servicio proporcionado en el mes correspondiente.

Características Técnicas del Servicio

Disponibilidad RPV-MPLS

OPERBES, S.A. DE C.V. tomó en consideración que 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.

OPERBES, S.A. DE C.V. tomó en consideración que la disponibilidad del servicio provisto por la RPV-MPLS, se agrupa en: Disponibilidad Física del Medio, Disponibilidad Físico del Nodo y Disponibilidad Lógica.

Disponibilidad Física del Medio

OPERBES, S.A. DE C.V. mantendrá una Disponibilidad de los canales de comunicación, conforme a los niveles de servicio que se especifican en este documento. Se considera que un enlace no se encuentra disponible físicamente cuando:

El medio de transmisión o cualquiera de sus componentes (medio físico, equipo de TX/RX, terminador de red) se encuentra abajo (down), es decir, no hay ningún tipo de comunicación y/o señalización a nivel capa física.

El protocolo de transmisión (por ejemplo HDLC o PPP), se encuentra abajo (line protocol down), es decir, no hay señalización a nivel capa de enlace.

En el caso de intermitencia se considerará como no disponible.

Disponibilidad Física del Nodo

OPERBES, S.A. DE C.V. mantendrá una Disponibilidad de los elementos del nodo (equipos de comunicación, equipos de seguridad (appliance), equipos de administración de tráfico y optimización de aplicaciones), conforme a los niveles de servicio que se especifican en este documento. En el caso de no poder cumplirlos, OPERBES, S.A. DE C.V., realizará las adecuaciones necesarias en los equipos que integran el nodo.

Se considera que un elemento del nodo no está disponible físicamente cuando:

El elemento se encuentre dañado físicamente, en su conjunto o en alguno de sus componentes, de tal manera que no permita ofrecer íntegramente las funciones de la solución solicitada.

Disponibilidad Lógica

Se considerará que un enlace no está disponible lógicamente cuando:

El protocolo de enrutamiento (cuando se trate de protocolos de ruteo dinámicos en el CPE) se encuentra abajo (protocol down), es decir, no hay señalización a nivel capa de ruteo.

La transmisión y recepción de información no sea completada entre el equipo CPE fuente y destino

Cuando se realicen mantenimientos que no sean programados y que no se observen los acuerdos establecidos en el proceso de control de cambios.

La red de OPERBES, S.A. DE C.V., permitirá la medición de la Disponibilidad Lógica.

Disponibilidad del Servicio

En la siguiente tabla se presentan las disponibilidades de servicio por tipo de nodo, solicitadas por SHF para los diferentes tipos de nodo de la RPV-MPLS:

NIVELES DE SERVICIO			
	Nodo criticidad alta	Nodo criticidad media	Nodo criticidad estándar
Disponibilidad Mensual Del Servicio de RPV-MPLS	>= 99.98%	>= 99.93%	>= 99.5%
Disponibilidad Mensual Del Servicio de Internet	>= 99.98%	>= 99.93%	>= 99.5%

Tabla: 6.5.1

OPERBES, S.A. DE C.V. proveerá 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 VIII. Matriz de Servicios", de acuerdo al tipo de nodo, ubicación geográfica, condiciones físicas, y demás consideraciones que estime pertinentes.

OPERBES, S.A. DE C.V. entregará 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 OPERBES, S.A. DE C.V. debe realizar cambios en la solución para poder dar cumplimiento a la disponibilidad solicitada por SHF, estos cambios serán programados y observar los acuerdos establecidos en el proceso de control de cambios; asimismo estos cambios no causarán costos adicionales para SHF, siempre y cuando dichos cambios no sean debido a una solicitud expresa de SHF para cambiar el nivel de servicio del nodo que se trate, en cuyo caso solo se incrementará el costo mensual con base a los costos ofertados por OPERBES, S.A. DE C.V., para cada elemento del nodo en el nivel de disponibilidad solicitado.

Incidente en el Suministro Eléctrico

OPERBES, S.A. DE C.V. considera una solución UPS para los distintos nodos donde SHF no proporcionen energía eléctrica regulada ininterrumpible, y que como referencia se indica en el "Anexo VIII. Matriz de Servicios". Cumplirán los niveles de servicio solicitados indicados en el punto Infraestructura Auxiliar.

Latencia y Pérdida de Paquetes

OPERBES, S.A. DE C.V. tomó en consideración que en la siguiente tabla se presentan los niveles de servicio requeridos, para las diferentes calidades de servicio:

Calidad de Servicio	Nivel de Servicio Solicitado	
QoS	Tiempo máximo de ida y vuelta en mili segundos	Pérdida de paquetes
Voz, Datos y Video	100	< 1%

Tabla: 6.7.1

OPERBES, S.A. DE C.V. tomó en consideración que SHF le indicará el ID de referencia que se tomará como punto central para la medición de las latencias desde los demás nodos que conformen la Red RPV-MPLS de SHF ; cabe indicar que dicho ID central podrá cambiar, previo aviso, según las necesidades de SHF.

Medición de la Pérdida de Paquetes

Para la medición de la pérdida de paquetes, OPERBES, S.A. DE C.V. entregará un reporte mensual con base en la herramienta de monitoreo descrita en el punto 4.2, Centro de Operación de Red (NOC) y recibida.

OPERBES, S.A. DE C.V. tomó en consideración que no se considerará pérdida de paquetes, si existe en el mismo periodo de Incidente condiciones de no disponibilidad física o lógica.

Disponibilidad del Centro de Operaciones de Red (NOC) y Centro de Operación de Seguridad (SOC)

OPERBES, S.A. DE C.V. incluye todas las licencias, mantenimientos y actualizaciones necesarias tanto en software y hardware para mantener la operación continua con una disponibilidad solicitada por nodo. La Disponibilidad se obtendrá a partir de:

Disponibilidad de las Herramientas de Monitoreo y Análisis de Tráfico.

OPERBES, S.A. DE C.V. mantendrá una disponibilidad de las herramientas de monitoreo y análisis de tráfico en una operación 7X24. Cuando alguna de estas no se encuentren disponibles y esto ocasione la pérdida de la información utilizada para la medición de disponibilidad, latencia, ancho de banda y análisis de tráfico de uno o más nodos, el tiempo que esté relacionado con la pérdida de información y que impida el cálculo será considerado como no disponibilidad para el nodo o nodos afectados por la falta de información.

OPERBES, S.A. DE C.V. mantendrá una disponibilidad en las aplicaciones de monitoreo, seguimiento de reportes y análisis de tráfico, a través de un acceso WEB, en una operación 7X24.

Disponibilidad de la Mesa de Ayuda

OPERBES, S.A. DE C.V., mantendrá la disponibilidad de atención y recepción de llamadas que realice SHF para la recepción, registro, análisis y solución de los reportes de incidentes bajo un esquema de operación de 7X24.

La Mesa de Ayuda de OPERBES, S.A. DE C.V. responderá el 95% de los llamados dentro de un período de tiempo de 5 minutos y el máximo número de llamadas abandonadas, después de un tiempo de espera en cola de 20 segundos, no excederá de 5% mensual.

Se entregará un reporte mensual con base en la herramienta de monitoreo descrita en el punto 4.2, Centro de Operación de Red (NOC).

Disponibilidad de Internet

OPERBES, S.A. DE C.V., mantendrá una disponibilidad del servicio de Internet, considerado y medido como un nodo de la RPV-MPLS de acuerdo a lo solicitado en el "Anexo VIII. Matriz de Servicios".

Para este caso se considerará como elemento del nodo la solución seguridad en la nube de internet y de contención de ataques en el perímetro, cuando SHF la haya solicitado, aplicándose la misma regla definida en el punto: Medición de la disponibilidad del servicio.

La latencia no será mayor a 60 milisegundos de ida y vuelta al punto de acceso a la red pública más cercano en términos del número de saltos necesarios para alcanzarlo.

Se entregará un reporte mensual con base en la herramienta de monitoreo descrita en el punto 4.2, Centro de Operación de Red (NOC).

Disponibilidad de DNS

OPERBES, S.A. DE C.V. tomó en consideración que la disponibilidad del DNS se define como la medida del porcentaje de tiempo, en que sus diferentes elementos realizan la función que les es propia y se considerará como parte integrante del nodo de Internet para cálculos de disponibilidad de este último.

La disponibilidad de los equipos DNS, cumplirá con la disponibilidad solicitada en el nodo de Internet por SHF y estará basada en el protocolo ICMP. Midiendo la disponibilidad de cada uno de los componentes habilitadores del servicio DNS.

El tiempo para dar de alta un registro en el DNS será como máximo de 1 hora a partir de levantado la solicitud en la mesa de ayuda.

OPERBES, S.A. DE C.V. entregará un reporte mensual con base en la herramienta de monitoreo descrita en el punto 4.2, Centro de Operación de Red (NOC).

Niveles de Servicio Aplicables a los Elementos de Seguridad

OPERBES, S.A. DE C.V. garantizará la seguridad 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 de la RPV-MPLS en SHF. En la siguiente tabla, se presentan los niveles de servicio esperados para las tareas de administración y monitoreo de la infraestructura de seguridad:

SERVICIO	NIVEL COMPROMETIDO
Atención a requerimientos de configuraciones de seguridad	30 minutos después de acordado el cambio entre 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 proporcionado por OPERBES, S.A. DE C.V. durante todo el contrato. Entrega de la media máximo 3 días hábiles después de liberada la versión
Administración y control de accesos remotos y túneles VPN	Tiempo máximo de solución: 2 horas después de la solicitud de SHF.
Control de cambios	Por tipo Urgente - Inmediato, una vez autorizado o solicitado por SHF. Impacto Alto -24 hrs Programado Impacto Medio -48 hrs Programado Estándar -24 hrs, una vez autorizado o solicitado por SHF.
Control de accesos	Cero accesos de usuarios o equipos no autorizados en la LAN, WAN e Internet.
Dictamen de actividades sospechosas	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 servicios Medio 60 minutos Estándar 24 hrs Programado.
Servicios de remediación de vulnerabilidades	Proceso de control de cambios iniciado en máximo 2 días naturales después de ser publicados por el fabricante.
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 todo el personal solicitado durante la vigencia del contrato.

Control de accesos a páginas web o URL'S 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, OPERBES, S.A. DE C.V. 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.

Cálculo de la Disponibilidad por Nodo

OPERBES, S.A. DE C.V. tomó en consideración que la disponibilidad Lógica del nodo, se considera cuando el servicio está activo ya sea a través del enlace activo o el enlace redundante. La Disponibilidad RPV por Nodo se calculará a través de la herramienta de monitoreo del NOC descrita en el punto 4.2, Centro de Operaciones de Red NOC.

Medición de la Disponibilidad del Servicio

Betel tomó en consideración que la medición de la disponibilidad de los servicios, se realizará en forma diaria recolectando la información generada a través de la herramienta de monitoreo (definida en el Servicio de NOC), 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.

OPERBES, S.A. DE C.V. proporcionará información al menos cada minuto, la cual se almacenará en una base de datos de la misma herramienta y estará disponible en cualquier momento (dentro del plazo de 90 días en línea) para SHF por medio de las herramientas del NOC mediante su vista WEB. Posteriormente a los 90 días naturales se podrán compactar los datos para la revisión requerida por SHF.

Betel tomó en consideración para determinar la disponibilidad mensual del nodo, se realizará una sumatoria de la disponibilidad mensual de cada uno de los elementos del nodo que se trate y será visualizada por las herramientas del NOC.

Betel tomó en consideración en caso de que ocurra algún incidente y no se vea comprometida la disponibilidad en las herramientas de monitoreo pero si algún servicio o aplicación específica catalogada como crítica para SHF, se calculará la deductiva con base al tiempo de afectación a dicho servicio o aplicación.

En todos los casos, al reporte mensual que presente OPERBES, S.A. DE C.V., se le podrán hacer los ajustes correspondientes a los tiempos de indisponibilidad justificados por SHF, en el entendido que estos tiempos justificados serán previamente acordados entre OPERBES, S.A. DE C.V. y SHF, de acuerdo a las necesidades de soporte, mantenimiento, etc.; teniendo OPERBES, S.A. DE C.V. que recabar la autorización expresa de SHF que se vea afectada por estas actividades.

En casos en los que sea necesario acceder al sitio, el personal OPERBES, S.A. DE C.V. notificará con anticipación de acuerdo con el procedimiento de SHF. En caso de que no se permita el acceso al personal, se detendrá el conteo del tiempo de no disponibilidad justo cuando personal OPERBES, S.A. DE C.V. informe esta eventualidad a 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 SHF. Los procedimientos de acceso y los acuerdos operativos para el reinicio del conteo de la no disponibilidad serán definidos con OPERBES, S.A. DE C.V.. Esto será aplicable en general, para todos los niveles de servicio siempre y cuando el diagnóstico del problema, acordado con SHF, identifique que la solución del mismo depende del acceso al sitio en cuestión.

Betel tomó en consideración que SHF requiere de la gestión de niveles de servicio, de acuerdo a las disponibilidades mencionadas anteriormente, con la capacidad de monitorear, medir y dar seguimiento sobre la calidad de los servicios requeridos por SHF. La interfaz de generación de niveles de servicio permitirá exportar de forma simple y mínimo soportará la exportación a los siguientes formatos: PDF y CSV.

Servicios Complementarios

Borrado Certificado de la Información

Betel tomó en consideración que para los discos duros de los elementos de infraestructura y otros dispositivos de almacenamiento que a criterio de SHF y que formen parte del presente documento que durante la vida del contrato lleguen a tener alguna falla y que requiera la ejecución de un cambio físico y/o retiro de Infraestructura al término del contrato, OPERBES, S.A. DE C.V. realizará el borrado seguro de la información de la totalidad de los discos y en su caso dispositivos de almacenamiento de cada uno de los elementos de infraestructura mediante una herramienta y procedimiento que cumplan con el estándar DoD5220.22-M, entregando a SHF el certificado del borrado seguro de los disco duros y en su caso dispositivos para sustentar la actividad realizada.

La herramienta de destrucción digital de datos cumplirá con al menos tres de los estándares que se describen a continuación.

DOD 5220.22-M
NAVSO P-5239-26
NCSC-TG-025
NSA 130-1
Bruce Schneier´s algorithm
Peter Gutmann's algorithm
Opnavinst5239.1A
HMG Infosec Standard 5, Lower Standard
HMG Infosec Standard 5, Higher Standard
NIST 800-88 / ATA Secure Erase (+ assurance)

La herramienta de destrucción digital de datos tendrá al menos 3 de las siguientes certificaciones:

NSTL
OTAN

COMMON CRITERIA

La herramienta de destrucción digital de datos:

Contará con soporte técnico local en el país, en español y preferentemente en la Ciudad de México.

Borrar el 100% (todas las particiones y sectores) de la información contenida en el disco de todos los equipos de OPERBES, S.A. DE C.V. anterior que serán retirados una vez concluido el contrato.

Certificado de borrado de datos, reporte con características del proceso de borrado.

La herramienta utilizada por OPERBES, S.A. DE C.V. para el borrado de datos, generará por cada uno de los equipos borrados, un reporte que certifique el proceso de borrado, conteniendo al menos la siguiente información y características:

Reporte protegido digitalmente
Firma Digital
Fecha del reporte
Número del reporte
Información de disco
Información del equipo
Estatus de terminación del proceso de borrado
Duración del borrado
Campos de impresión para firmas de quien ejecuta el borrado y quien recibe el reporte.
En el Apartado Borrado de disco seguro se describe la solución propuesta
Infraestructura Auxiliar

Todos los materiales y equipos que formen parte de la solución de OPERBES, S.A. DE C.V., serán nuevos en su totalidad.

OPERBES, S.A. DE C.V. tomó en consideración las siguientes condiciones en las que se entregarán los servicios de infraestructura auxiliar:

Cableado estructurado

Las tareas de acondicionamiento incluyen el cableado estructurado (patch cord) que será al menos de categoría 6 para la interconexión de los equipos suministrados por OPERBES, S.A. DE C.V., los cuales estarán etiquetados para identificar los elementos que interconecta, y los cables de interconexión estarán organizados debidamente en el rack de comunicaciones.

Racks, gabinete, mini gabinete

OPERBES, S.A. DE C.V. suministrará en cada sitio de acuerdo al "Anexo VIII. Matriz de Servicios", los siguientes Racks o Gabinetes, cumpliendo con el estándar EIA310D.

Rack 7 pies. De aluminio natural de 7 pies de altura x 19" de ancho para la colocación del equipo activo y UPS en los casos necesarios.

Rack 4 pies. De aluminio natural de 4 pies de altura x 19" de ancho para la colocación del equipo activo y UPS en los casos necesarios.

Gabinete piso 40 UR. Profundidad Externa: 27 diseñado para el montaje y protección de equipos para toda su red puerta frontal con vidrio inastillable y puerta trasera de acero sólido con ventilación y cerradura de seguridad panel laterales desmontables el techo cuenta con ventilación para 4 extractores de aire.

Gabinete piso 20 UR. Gabinete Cerrado Metálico de 20 UR equipado con barra de contactos, kit para aterrizaje, kit de extractores de calor.

Gabinete con ventilador. Profundidad Externa: 27 diseñado para el montaje y protección de equipos para toda su red puerta frontal con vidrio inastillable y puerta trasera de acero sólido y cerradura de seguridad panel laterales desmontables el techo cuenta con sistema de enfriamiento con ventilador para garantizar una temperatura optima que proporcione un mejor rendimiento en equipos.

Los racks o gabinetes solicitados serán aterrizados a la barra de tierra que se instalará o que ya se encuentre instalada, dentro del mismo cuarto de telecomunicaciones y contará con los aditamentos necesarios para el montaje de los equipos propuestos.

UPS

Donde SHF no brinde una solución de energía eléctrica regulada ininterrumpible (UPS) indicado en el "Anexo VIII. Matriz de Servicios", Bstel instalará una solución que proporcione este servicio con la capacidad de respaldo de energía necesaria para mantener un tiempo de suministro eléctrico regulado de al menos para sitios de criticidad Alta de 4 horas y sitios de criticidad Media de 2 horas a plena carga para los equipos del nodo proporcionados por OPERBES, S.A. DE C.V..

Es importante indicar, que debido a que la disponibilidad del nodo en cuanto a suministro de energía regulada es soportada por los equipos UPS. Asimismo, OPERBES, S.A. DE C.V. integrará la

solución UPS a la herramienta de monitoreo del NOC con el fin de censar su estado y validar su correcta operación.

Infraestructura eléctrica

OPERBES, S.A. DE C.V. considera la instalación de los contactos necesarios para alimentar a la solución UPS y de aire acondicionado en los nodos que así lo requieran, considerando el cableado necesario desde el tablero más cercano, así como la canalización y todos los accesorios necesarios para su correcta instalación, sin llegar a afectar las funcionalidades actuales de dicho tablero e identificando el circuito asociado a través de una etiqueta.

OPERBES, S.A. DE C.V. tomó en consideración que en caso de requerirse más contactos, estos serán por cuenta de OPERBES, S.A. DE C.V., sin costo para SHF.

Sistema de tierra física independiente para equipamiento.

OPERBES, S.A. DE C.V. considerará la implementación de un sistema de tierra física independiente para la protección adecuada de todos los equipos propuestos, con el fin de mantener los niveles de servicio solicitados.

OPERBES, S.A. DE C.V. incluirá todos los accesorios para su conexión al rack donde se ubicará el equipo propuesto del nodo, incluyendo el material, consumibles, mano de obra, obra civil, conectores, ductería y todo lo necesario para implementar el sistema de tierra física.

OPERBES, S.A. DE C.V. tomó en consideración que no obstante SHF indiquen en su "Anexo VIII, Matriz de Servicios" la necesidad de tierra física, SHF evaluará junto con el Licitante dónde efectivamente las tierras físicas existentes no puedan ser utilizadas.

Mantenimiento de infraestructura auxiliar

OPERBES, S.A. DE C.V. consideró el realizar el mantenimiento preventivo y correctivo incluyendo la mano de obra, refacciones, viáticos que se generen, sustitución de partes y componentes de la infraestructura auxiliar durante el tiempo que dure el contrato, con el fin de mantenerla en las condiciones operativas óptimas para cumplir con los niveles de servicio solicitados.

Servicio de Supervisión y Monitoreo en Sitio

Con la finalidad de que SHF valide la administración, gestión, niveles de servicio y mantenga un monitoreo constante de todos los servicios solicitados en el presente documento; OPERBES, S.A. DE C.V. en caso de ser el Licitante ganador considera en su propuesta lo siguiente para tal efecto:

Contará al menos con un sistema que permita desplegar señales de alta definición, cómputo y video según las necesidades de SHF. Para dicho sistema se deberán incluir al menos 4 pantallas LCD de 50", integrando un sistema de colaboración con software especializado que logre enviar y recibir datos, video y audio entre diferentes pantallas, programar el contenido y las aplicaciones de manera fácil y rápida a través de una interfaz remota e intuitiva

Se considera al menos un Servidor con las capacidades para soportar la recepción de los traps SNMP, según parámetros establecidos por SHF, así como el acceso a las consolas de Monitoreo vía WEB o cliente servidor, que permitan tener visibilidad en las diferentes pantallas sobre variables importantes de la RPV-MPLS.

OPERBES, S.A. DE C.V. configurará al menos una comunidad SNMP con derechos de lectura, independiente a la comunidad que OPERBES, S.A. DE C.V. utilice para el monitoreo de los diferentes componentes habilitadores que formen parte del contrato.

OPERBES, S.A. DE C.V. tomó en consideración que en todo momento, desde el inicio del servicio, SHF podrá recibir de todo componente habilitador instalado, comunidades de SNMP con acceso Sólo-Lectura. OPERBES, S.A. DE C.V. realizará los trabajos necesarios, a fin de soportar y permitir el monitoreo de los componentes habilitadores, usando SNMP, sin costo adicional para SHF.

OPERBES, S.A. DE C.V. será responsable de la instalación y puesta a punto del servidor, pantallas e infraestructura necesaria para la correcta operación de la sala de Monitoreo. Al solicitar SHF dicho servicio, OPERBES, S.A. DE C.V. entregará un plan de trabajo a los 10 hábiles de solicitado el servicio. La instalación y puesta en punto no pasará de 15 días hábiles después de la entrega del plan de trabajo.

El servicio de Supervisión y Monitoreo en sitio estará disponible y funcionando durante la vigencia del contrato con una disponibilidad del 99.85% mensual.

Glosario

CPE: Customer Premises Equipment, por sus siglas en inglés, el Equipo Local del Cliente es un equipo de telecomunicaciones usado tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación. El equipo puede proveer una combinación de servicios incluyendo datos, voz, video y un host de aplicaciones multimedia interactivos.

Encripción: es un proceso para convertir la información a un formato más seguro. En otras palabras, los datos que están en un formato claro, o sea entendible, se convierten mediante un proceso

matemático a un formato encriptado o codificado, o sea ininteligible. Una vez que llegan a su destino, se decodifican para poder ser legibles de nuevo, se desencriptan. La criptografía se define como la técnica de ocultación de información mediante la codificación de contenidos; el término proviene del griego 'kruptos' que significa 'oculto'. La encripción consiste en aplicar una serie de operaciones matemáticas (algoritmo) a un texto legible, para convertirlo en algo totalmente inteligible.

IPS: Un Sistema de Prevención de Intrusos o por sus siglas en inglés Intrusion Prevention Systems (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos .

MPLS: (siglas de Multiprotocol Label Switching, Conmutación de Etiquetas Multiprotocolo) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

Topología de red: se define como una familia de comunicación usada por los computadores que conforman una red para intercambiar datos. El concepto de red puede definirse como "conjunto de nodos interconectados". Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente, depende del tipo de redes a que nos refiramos. Ejemplos de topología de red son: de bus, estrella, anillo o circular, malla, árbol o híbrida.

VRF: Virtual Routing Forwarding, por sus siglas en inglés, se define como una tecnología que permite tener múltiples instancias de una tabla de enrutamiento en un mismo router y éste es el mecanismo para hacer posible las VPN MPLS. Cada VRF contiene únicamente las rutas que conecta a cada sede de la misma VPN.

OPERBES, S.A. DE C.V. tomó en consideración que para las deductivas aplicará lo siguiente:

IV.- DEDUCTIVAS.

De conformidad con el artículo 53 BIS de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento vigente, en caso de que la prestación del servicio presenten fallas derivadas del incumplimiento parcial o prestación deficiente, la Dirección General de Tecnologías y Seguridad de la Información aplicará al proveedor una deducción a la facturación mensual de acuerdo a lo especificado en cada uno de los conceptos considerados en la siguiente tabla:

CONCEPTO	NIVEL DE SERVICIO	DEDUCTIVA	MÁXIMO PERMITIDO
Procesamiento y memoria de equipos	Si el uso del procesador y memoria se encuentra entre el 70% y el 85% promedio de su capacidad, durante 10 días hábiles consecutivos en el horario de operación de las 10:00 a las 19:00 horas, el Licitante deberá ampliar la capacidad en un plazo no mayor a tres días hábiles	2 al millar por cada día de atraso del monto total de la facturación mensual de los servicios correspondientes al nodo(s) afectado(s)	Con un máximo de 2 eventos al mes por nodo.
Procesamiento y memoria de equipos	Si el uso del procesador en los equipos es mayor del 85% promedio de su capacidad, durante 3 días hábiles consecutivos de operación normal en el horario de las 10:00 a las 19:00 horas, el Licitante deberá reemplazar el equipo, por la siguiente categoría, en un plazo no mayor a tres días hábiles	6 al millar por cada día de atraso del monto total de la facturación mensual de los servicios correspondientes al nodo(s) afectado(s)	Con un máximo de 2 evento al mes por nodo.
Disponibilidad nodos	Cuando no se cumplan con los objetivos	6 al millar, por cada minuto de	Con un máximo de 3 eventos al mes por nodo.

CONCEPTO	NIVEL DE SERVICIO	DEDUCTIVA	MÁXIMO PERMITIDO
de criticidad Alta	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.	indisponibilidad sobre el nivel de servicio establecido y con base al importe de la factura del mes de incidencia mensual por nodo de la RPV-MPLS; para él o los nodos afectados.	
Disponibilidad nodos de criticidad Media	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.	6 al millar, por cada minuto de indisponibilidad sobre el nivel de servicio establecido y con base al importe de la factura del mes de incidencia mensual por nodo de la RPV-MPLS; para él o los nodos afectados.	Con un máximo de 4 eventos al mes por nodo.
Disponibilidad nodos de criticidad estándar.	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.	6 al millar, por cada minuto de indisponibilidad sobre el nivel de servicio establecido y con base al importe de la factura del mes de incidencia mensual por nodo de la RPV-MPLS; para él o los nodos afectados.	Con un máximo de 4 eventos al mes por nodo.
Disponibilidad del servicio de UPS	Cuando no se cumplan con los objetivos de las disponibilidades del servicio por criticidad del nodo, para los diferentes niveles de disponibilidad, del servicio del UPS	2 al millar por cada hora sobre el nivel de servicio establecido y con base al importe mensual por nodo de la RPV-MPLS para él o los nodos afectados.	Con un máximo de 4 eventos al mes por nodo.
Latencia	Máximo 100 ms, para cada calidad de servicio establecida	2 al millar por cada milisegundo que el promedio exceda el límite establecido por cada calidad de servicio, sobre el importe de la factura mensual por nodo de la RPV-MPLS, 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	Tiempo de reparación para falla o incidente o	6 al millar por cada hora sobre el nivel de servicio establecido y con	Con máximo de 10 eventos al mes.

CONCEPTO	NIVEL DE SERVICIO	DEDUCTIVA	MÁXIMO PERMITIDO
	reconfiguración lógica de un nodo de la RPV-MPLS e internet, mayor al solicitado conforme al nivel de criticidad del nodo.	base al importe mensual por nodo de la RPV-MPLS para él o los nodos afectados.	
Internet Nodo Crítico	Cuando no se cumplan con los niveles mínimos de disponibilidad del servicio.	6 al millar por cada minuto de indisponibilidad sobre el nivel de servicio establecido y con base al importe de la facturación mensual del servicio de Internet de SHF correspondiente.	Con máximo 3 eventos al mes.
MCU Hosteado	Cuando no se cumplan con los niveles mínimos de disponibilidad del servicio.	6 al millar por cada minuto de indisponibilidad sobre el nivel de servicio establecido y con base al importe de la facturación mensual del servicio de videoconferencia.	Con máximo 5 eventos al mes.
DNS Externo	Cuando no se cumplan con los niveles mínimos de disponibilidad del servicio.	6 al millar por cada minuto de indisponibilidad sobre el nivel de servicio establecido y con base al importe de la facturación mensual del servicio de Internet de SHF correspondiente.	Con máximo 3 eventos al mes.
Degradación por perdida de paquetes	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 de la RPV-MPLS para el o los nodos afectados.	En caso de reincidencia durante dos meses consecutivos, la deducción será del 5 al millar por décima porcentual hasta el cuarto mes en que no presente incumplimiento.
Monitoreo del NOC y/o SOC	Cuando no se cumplan con los niveles mínimos solicitados requeridos.	2 al millar por hora de indisponibilidad sobre el nivel de servicio establecido y con base al importe de la factura total mensual de la RPV-MPLS.	Con un máximo de 3 eventos mensuales.
Monitoreo de la Disponibilidad de Aplicaciones Web	Cuando no se cumplan con los tiempos mínimos solicitados	2 al millar por minuto de atraso en la notificación con base al importe del servicio.	Con un máximo de 3 eventos mensuales.
Optimizador y acelerador de trafico Control de ancho de banda	Cuando no se cumplan con los niveles mínimos solicitados requeridos.	6 al millar por hora de indisponibilidad sobre el nivel de servicio establecido y con base al importe de la factura total mensual de la RPV-MPLS.	Con un máximo de 3 eventos mensuales.

CONCEPTO	NIVEL DE SERVICIO	DEDUCTIVA	MÁXIMO PERMITIDO
Atención a requerimientos de configuraciones de seguridad	Cuando no se cumpla con el tiempo máximo establecido en los niveles de servicio	6 al millar por cada hora natural de atraso del monto total de la facturación mensual de los servicios correspondientes al nodo(s) afectado(s)	Con un máximo de 5 eventos mensuales por nodo.
Tiempo de solución a incidentes de seguridad	Cuando no se cumpla con los tiempos establecidos por prioridad	6 al millar por cada minuto de afectación a los servicios y/o aplicaciones y/o por atraso para la solución del mismo, sobre el monto total de la facturación mensual de los servicios correspondientes al nodo(s) afectado(s)	Con un máximo de 1 eventos mensual por nodo
Licenciamiento y entrega de actualizaciones	Cuando no se cumpla con lo establecido en los niveles de servicio	6 al millar por cada día hábil de atraso con base al monto total de la facturación mensual de la solución involucrada	Para todos los dispositivos de la RPV MULTISERVICIO MPL cuando el fabricante emita una nueva licencia del software
Control de accesos a páginas web, URL's o aplicaciones.	Cuando no se cumpla con el tiempo máximo establecido en los niveles de servicio	6 al millar sobre el total de la facturación mensual de la solución involucrada, por cada día de atraso para la categorización, re categorización, bloqueo o acceso a los sitios o categorías web,	Con un máximo de 3 eventos mensuales por nodo
Accesos de usuarios o equipos no autorizados en el mes.	Cuando no se cumpla con lo establecido en los niveles de servicio	5 al millar por cada acceso de usuarios no autorizados con base al monto total de la facturación mensual de la solución involucrada.	Para la solución de seguridad nodos críticos 5 accesos no autorizados máximo, durante 3 meses consecutivos Para la solución de seguridad nodos medio y estándar 10 accesos no autorizados máximo, durante 3 meses consecutivos
Administración de VPN	Cuando no se cumpla con lo establecido en los niveles de servicio	2 al millar por cada hora natural de atraso con base al monto total de la facturación mensual de la solución involucrada	Para la solución de seguridad tipo firewall
Control de cambios de las soluciones de seguridad	Cuando no se cumpla con lo establecido en los niveles de servicio	2 al millar por cada hora natural de atraso con base al monto total de la facturación mensual de la solución involucrada.	Aplica para: Cualquier dispositivo de seguridad Cuando se solicite un control de cambios en algún componente de las soluciones antes mencionadas

CONCEPTO	NIVEL DE SERVICIO	DEDUCTIVA	MÁXIMO PERMITIDO
Control de acceso	Cuando no se cumpla con lo establecido en los niveles de servicio	2 al millar por cada acceso no autorizado con base al monto total de la facturación mensual de la solución involucrada.	Aplica para: Cualquier dispositivo de seguridad Cuando se detecte algún acceso no autorizado por SHF
Servicios de remediación de vulnerabilidades	Cuando no se cumpla con lo establecido en los niveles de servicio	6 al millar por cada día natural de atraso con base al monto total de la facturación mensual de la solución involucrada	Aplica para: Cualquier dispositivo de seguridad Cuando el fabricante publique la remediación
Dictamen de actividades sospechosas	Cuando no se cumpla con lo establecido en los niveles de servicio	6 al millar por cada hora hábil de atraso con base al monto total de la facturación mensual de la solución involucrada	Aplica para: Cualquier dispositivo de seguridad cuando se detecte alguna actividad sospechosa.
Manejo de incidentes de día cero.	Cuando no se cumpla con lo establecido en los niveles de servicio	6 al millar por cada día de atraso del monto total de la facturación mensual de los servicios correspondientes al nodo(s) afectado(s)	Aplica para: Cualquier dispositivo de seguridad cuando se detecte algún incidente de día cero.
Personal Certificado para soportar los servicios.	Cuando no se notifique del cambio de los Recursos Humanos solicitados (Gestión del Personal Técnico)	2 al millar por cada día de indisponibilidad sobre el monto total de la facturación mensual de los servicios correspondientes al nodo(s) afectado(s)	Aplica para: NOC, SOC y personal en sitio
Servicios de Supervisión y Monitoreo	Cuando no se cumplan con los niveles de servicio establecidos	2 al millar por cada día de indisponibilidad sobre el monto total del servicio	Con un máximo de 5 eventos por año

OPERBES, S.A. DE C.V. tomó en consideración que para las penas convencionales aplicará lo siguiente:

V.- PENAS CONVENCIONALES.

Con fundamento a lo dispuesto en los Artículos 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 95 y 96 de su Reglamento, se aplicará al Licitante Ganador una pena convencional de 2 al millar por cada día natural de atraso en la entrega de los servicios, en el entendido que el monto máximo de las penas convencionales por atraso no excederá del monto de la garantía de cumplimiento del contrato.

La pena convencional se aplicara en el siguiente caso: Por cada día natural de atraso en las fechas pactadas para la prestación del servicio.

Las penas convencionales serán calculadas y notificadas al proveedor por la Dirección General de Tecnologías y Seguridad de la Información, el proveedor cubrirá a la misma la pena convencional, mediante entero a la Tesorería de la Federación, en cualquiera de las instituciones bancarias y el proveedor queda obligado a remitir al siguiente día hábil de realizado el entero de referencia un ejemplar original del mismo a la Dirección General de Tecnologías y Seguridad de la Información.

En ningún caso las penas convencionales podrán negociarse en especie.

Independientemente de la aplicación de las penas mencionadas, SHF podrá optar por la rescisión de su Contrato.

CONCEPTO	PLAZOS ESTABLECIDOS	REQUERIMIENTO	PENALIZACIONES
Adicionar e incrementar	30 días naturales a partir de la	Adicionar e incrementar equipos en los	2 al millar por cada día de atraso del

equipos en los nodos	recepción de la solicitud formal	nodos	monto total de la facturación mensual de los servicios correspondientes al nodo(s) afectado(s).
Adicionar e incrementar soluciones en los nodos	10 días hábiles a partir de la recepción de la solicitud formal	Adicionar e incrementar soluciones en los nodos	2 al millar por cada día de atraso del monto total de la facturación mensual de los servicios correspondientes al nodo(s) afectado(s).
Adicionar e incrementar soluciones IPV6 en los nodos	60 días naturales a partir de la recepción de la solicitud formal	Adicionar e incrementar equipos en los nodos	2 al millar por cada día de atraso del monto total de la facturación mensual de los servicios correspondientes al nodo(s) afectado(s).
Incrementar o disminuir anchos de banda por configuración	72 horas naturales a partir de la solicitud formal	Incrementos o decrementos de ancho de banda en nodos sin cambio en medio de transmisión de acuerdo al "Anexo VIII. Matriz de Servicios Anexo VIII. Matriz de Servicios"	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 Plan de Trabajo de Implementación de Servicios	10 días hábiles posteriores al inicio de la vigencia del contrato	Plan de Trabajo de Implementación de Servicios	2 al millar por cada 48 horas de atraso del monto total del contrato
Entrega final del desarrollo del proyecto	15 días naturales después de la implementación del último nodo	Entregable final del desarrollo del proyecto	2 al millar por cada día hábil de atraso
Entrega de nuevos servicios	45 días naturales a partir de la solicitud formal	Puesta en servicio de nuevos nodos	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 inicial de servicios	De acuerdo a las fechas del Plan de Trabajo de Implementación de Servicios propuesto para SHF	Puesta en servicio inicial de nodos	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	45 días naturales a partir de la solicitud formal	Cambio de domicilio de un nodo ya instalado	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 servicio de	20 días hábiles a partir de la solicitud	Puesta en servicio	2 al millar por cada día hábil de atraso

videoconferencia	formal.		del monto del servicio
Entrega de nuevos servicios: Clientes nuevos VPN	2 horas hábiles a partir de la recepción de la solicitud formal	Solicitud de nuevas cuentas de clientes VPN	2 al millar por cada día de atraso en el alta de cuentas nuevas para clientes VPN sobre el importe de la facturación mensual del servicio.
Entrega de reportes:	Cada mes durante los primeros 7 días hábiles por nodo de la RPV-MPLS	De administración de configuraciones y cambios en la infraestructura, así como la actualización de la memoria técnica integral de los 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 7 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 7 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 entregarán dentro de los primeros 7 días hábiles de cada mes.	Disponibilidad, latencia y degradación por pérdida de paquetes del acceso a internet, por sitio. La información contenida será real sin sumarización o compactación. 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 nuevos dominios y/o certificados digitales SSL de 128 Bits	5 días hábiles a partir de la recepción de la solicitud formal	Solicitud de nuevos dominios y certificados digitales SSL de 128 Bits	2 al millar por cada día de atraso en el alta de nuevos dominios y certificados digitales SSL de 128 bits, sobre el importe de la facturación mensual del servicio.
Entrega de plan de trabajo para la Instalación y puesta a punto del Servicio de Supervisión y Monitoreo	10 días hábiles a partir de la recepción de la solicitud formal	Plan de trabajo del Servicio de Supervisión y Monitoreo	2 al millar por cada día de atraso sobre el costo del servicio
Instalación y puesta a punto del Servicio de Supervisión y	15 días hábiles a partir de la entrega del plan de trabajo	Implementación del Servicio de Supervisión y Monitoreo	2 al millar por cada día de atraso sobre el costo del servicio

Monitoreo			

OPERBES, S.A. DE C.V. tomó en consideración que los lugares en donde se prestará el servicio son los siguientes:

X.- LUGAR Y HORARIO DONDE SE PRESTARÁ EL SERVICIO.

El horario de la prestación de los servicios será los siete días de la semana, las veinticuatro horas del día en:

Sitio	Dirección
EJERCITO NACIONAL	Ejército Nacional 180, Col. Anzures Piso PB, entre Halley y Flamarion, C.P. 11590, Ciudad de México
EJERCITO NACIONAL PISO 12	Ejército Nacional 180, Col. Anzures Piso 12, entre Halley y Flamarion, C.P. 11590, Ciudad de México
METEPEC	Adolfo López Mateos No. 1956 ORIENTE COL. BELLAVISTA, C. P. 52172 METEPEC, ESTADO DE MÉXICO
PERULA	Bahía de Perula No. 12, Col. Verónica Anzures, Ciudad de México C.P. 11300
CECOBAN	Epigmenio González No. 2, Claustros del Parque, Querétaro, Qro. CP 76168
BURÓ DE CRÉDITO	Pico de Verapaz 435 piso 5 Col. Jardines de la Montaña C.P. 14210

EN REFERENCIA A LAS PATENTES.

OPERBES, S.A. DE C.V., ASUME LA RESPONSABILIDAD POR EL USO DE PATENTES, LICENCIAS Y DERECHOS QUE PUDIERAN CORRESPONDER A TERCEROS, SOBRE LOS SISTEMAS TÉCNICOS, PROCEDIMIENTOS, DISPOSITIVOS, PARTES, EQUIPOS, ACCESORIOS Y HERRAMIENTAS QUE UTILICE Y/O PROPORCIONE PARA CUMPLIR CON EL "SERVICIO ADMINISTRADO DE TELECOMUNICACIONES" (RPV MPLS) PARA SHF, Y DADO EL CASO DE PRESENTARSE ALGUNA VIOLACIÓN, EL PROVEEDOR ASUMIRÁ TODA LA RESPONSABILIDAD POR DICHAS VIOLACIONES QUE SE CAUSEN EN LA MATERIA, RESPONDIENDO ANTE LAS RECLAMACIONES QUE PUDIERA TENER O QUE LE HICIERAN A POR DICHOS CONCEPTOS, RELEVÁNDOLA DE CUALQUIER RESPONSABILIDAD, Y QUEDANDO OBLIGADO EL PROVEEDOR A RESARCIRLA DE CUALQUIER GASTO O COSTO COMPROBABLE QUE SE EROGUE POR DICHA SITUACIÓN.

ANEXO VIII.- MATRIZ DE SERVICIOS

		Servicios de Comunicaciones								Servicios de Seguridad Perimetral						
Inmueble	Domicilio	Servicio	FUO	Ancho de Banda piso	Ancho de Banda todos	Nivel de Criticidad del nodo	Análisis de tráfico			Contención de ataques en perímetro	FW	IPS	WAF	MF	PCMW	Correlacionador
			EN DEMANDA				MPLS	LAN	INTERNET							
SOCIEDAD HIPOTECARIA FEDERAL NODO CENTRAL	Ejercito Nacional 180, Col. Anzures Piso PB, entre Halley y Flamarion, C.P. 11590, México D.F.	Internet	EN DEMANDA	50 Mbps	100 Mbps	ALTA				TIPO I ESTANDAR	TIPO I ALTA	TIPO I ESTANDAR	TIPO III ESTANDAR	TIPO I ALTA	TIPO II ESTANDAR	TIPO I ESTANDAR
SOCIEDAD HIPOTECARIA FEDERAL PISO 12	Ejercito Nacional 180, Col. Anzures Piso PB, entre Halley y Flamarion, C.P. 11590, México D.F.	Internet	EN DEMANDA	20 Mbps	50 Mbps	ALTA										
METEPEC	ADOLFO LÓPEZ MATEOS No. 1955 ORIENTE COL. BELLAVISTA, C. P. 52172 METEPEC, ESTADO DE MÉXICO	Internet	EN DEMANDA	10 Mbps	50 Mbps	ESTANDAR								TIPO I ESTANDAR		
PERULA	Bahía de Perula No. 12, Col. Verónica Anzures, México, D.F. C.P. 11300	Internet	EN DEMANDA	20 Mbps	50 Mbps	ESTANDAR										
Entre Sociedad Hipotecaria Federal y Metepec	Ver domicilios de los ID's 1 y 2 de esta tabla	LAN to LAN	FIJO	50 Mbps	0	ESTANDAR										
SOCIEDAD HIPOTECARIA FEDERAL NODO CENTRAL	Ejercito Nacional 180, Col. Anzures Piso PB, entre Halley y Flamarion, C.P. 11590, México D.F.	MPLS	FIJO	2 Mbps	0	ESTANDAR										
METEPEC	ADOLFO LÓPEZ MATEOS No. 1955 ORIENTE COL. BELLAVISTA, C. P. 52172 METEPEC, ESTADO DE MÉXICO	MPLS	FIJO	2 Mbps	0	ESTANDAR										
PERULA	Bahía de Perula No. 12, Col. Verónica Anzures, México, D.F. C.P. 11300	MPLS	FIJO	2 Mbps	0	ESTANDAR										
OCOBAN	Ignacio González No. 2, Cimatros del Parque, Querétaro, Qro. CP 76158	MPLS	FIJO	256 Kbps	0	ESTANDAR										
BURÓ DE CRÉDITO	Pico de Verapaz 435 piso 5 Col. Jardines de la Montaña C.P. 14210	MPLS	FIJO	256 Kbps	0	ESTANDAR										

OPERBES, S.A DE C.V. integra en su propuesta técnica los siguientes Anexos en formato pdf y word, donde hace las características técnicas mínimas solicitadas por SHF para las tecnologías propuestas.

ANEXO 1.1- REFERENCIAS TECNICAS SOLUCIONES DE SEGURIDAD

TIPO	MARCA	MODELO	NOMBRE DEL DOCUMENTO DE REFERENCIA	FOLIO

CARACTERISTICAS MINIMAS SOLICITADAS	NOMBRE DEL DOCUMENTO DE REFERENCIA	FOLIO

ANEXO 1.2- REFERENCIAS TECNICAS VPN

MARCA	MODELO

CARACTERISTICAS MINIMAS SOLICITADAS	NOMBRE DEL DOCUMENTO DE REFERENCIA	FOLIO	PARRAFO

Apartado Descripción de los Equipos

CPE Routers para MPLS
Los equipos propuestos son de la marca Cisco

	Router para sitios hasta a 8 MB. MPLS
CISCO2911-HSEC+/K9	VPN ISM module HSEC bundles for 2911 ISR platform

MEM-2900-512U1GB	512MB to 1GB DRAM Upgrade (512MB+512MB) for Cisco 2901-2921
RPS-ADPTR-2911	Cisco 2911 RPS Adapter for use with External RPS
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m
S29UK9-15302T	Cisco 2901-2921 IOS UNIVERSAL
PWR-2911-AC	Cisco 2911 AC Power Supply
FL-29-HSEC-K9	U.S. Export Restriction Compliance license for 2921/2951
ISM-VPN-29	3DES/AES/SUITE-B VPN Encryption module
ISR-CCP-EXP	Cisco Config Pro Express on Router Flash
MEM-CF-256MB	256MB Compact Flash for Cisco 1900, 2900, 3900 ISR
SL-29-IPB-K9	IP Base License for Cisco 2901-2951
SL-29-SEC-K9	Security License for Cisco 2901-2951
CON-SNTP-2911HSEC	SMARTNET 24X7X4 AIM VPN module HSEC bundles for 2911 ISR
SL-29-DATA-K9	Data License for Cisco 2901-2951

R MPLS 8MB-15MB	Router para sitios Mayores a 8 MB. (MPLS)(Alta Criticidad (2)
CISCO2921-HSEC+/K9	VPN ISM module HSEC bundles for 2921 ISR platform
SL-29-DATA-K9	Data License for Cisco 2901-2951
SL-29-UC-K9	Unified Communication License for Cisco 2901-2951
RPS-ADPTR-2921-51	Cisco 2921/2951 RPS Adapter for use with External RPS
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m
S29UK9-15302T	Cisco 2901-2921 IOS UNIVERSAL
PWR-2921-51-AC	Cisco 2921/2951 AC Power Supply
FL-29-HSEC-K9	U.S. Export Restriction Compliance license for 2921/2951
ISM-VPN-29	3DES/AES/SUITE-B VPN Encryption module
ISR-CCP-EXP	Cisco Config Pro Express on Router Flash
MEM-2900-512MB-DEF	512MB DRAM for Cisco 2901-2921 ISR (Default)
MEM-CF-256MB	256MB Compact Flash for Cisco 1900, 2900, 3900 ISR
PI-MSE-PRMO-INSRT	Insert, Packout - PI-MSE
SL-29-IPB-K9	IP Base License for Cisco 2901-2951
SL-29-SEC-K9	Security License for Cisco 2901-2951
CON-SNTP-2921HSEC	SMARTNET 24X7X4 AIM VPN module HSEC bundles for 2921 ISR

R INTERNET	Router INTERNET REDUNDANTE (2) hasta 20 Mbps
CISCO2911/K9	Cisco 2911 w/3 GE 4 EHWIC 2 DSP 1 SM 256MB CF 512MB DRAM IPB
CON-SNTP-2911	SMARTNET 24X7X4 Cisco 2911 w/3 GE4
S29UK9-15302T	Cisco 2901-2921 IOS UNIVERSAL

PWR-2911-AC	Cisco 2911 AC Power Supply
SL-29-IPB-K9	IP Base License for Cisco 2901-2951
HWIC-BLANK	Blank faceplate for HWIC slot on Cisco ISR
ISR-CCP-EXP	Cisco Config Pro Express on Router Flash
MEM-2900-512MB-DEF	512MB DRAM for Cisco 2901-2921 ISR (Default)
CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m
PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE
MEM-CF-256MB	256MB Compact Flash for Cisco 1900 2900 3900 ISR
SM-S-BLANK	Removable faceplate for SM slot on Cisco 290039004400 ISR

R INTERNET	Router INTERNET REDUNDANTE (2) hasta 60 Mbps
CISCO3925/K9	Cisco 3925 w/SPE100(3GE,4EHWIC,4DSP,2SM,256MBCF,1GBDRAM,IPB)
3900-FANASSY	Cisco 3925/3945 Fan Assembly (Bezel included)
C3900-SPE100/K9	Cisco Services Performance Engine 100 for Cisco 3925 ISR
ISR-CCP-EXP	Cisco Config Pro Express on Router Flash
MEM-CF-256MB	256MB Compact Flash for Cisco 1900, 2900, 3900 ISR
PWR-3900-AC	Cisco 3925/3945 AC Power Supply
S39UK9-15104M	Cisco 3925-3945 IOS UNIVERSAL
SL-39-IPB-K9	IP Base License for Cisco 3925/3945
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m
CAB-CONSOLE-USB	Console Cable 6 ft with USB Type A and mini-B
MEM-3900-1GU2GB	1GB to 2GB DRAM Upgrade (1GB+1GB) for Cisco 3925/3945 ISR
PWR-3900-AC/2	Cisco 3925/3945 AC Power Supply (Secondary PS)
CON-SNTP-3925	SMARTNET 24X7X4 Cisco 3925 w/SPE100

R INTERNET	Router INTERNET REDUNDANTE hasta 100 Mbps

CISCO3945/K9	Cisco 3945 w/SPE150(3GE,4EHWIC,4DSP,4SM,256MBCF,1GBDRAM,IPB)
3900-FANASSY	Cisco 3925/3945 Fan Assembly (Bezel included)
C3900-SPE150/K9	Cisco Services Performance Engine 150 for Cisco 3945 ISR
ISR-CCP-EXP	Cisco Config Pro Express on Router Flash
MEM-CF-256MB	256MB Compact Flash for Cisco 1900, 2900, 3900 ISR
PWR-3900-AC	Cisco 3925/3945 AC Power Supply
S39UK9-15104M	Cisco 3925-3945 IOS UNIVERSAL
SL-39-IPB-K9	IP Base License for Cisco 3925/3945
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m
CAB-CONSOLE-USB	Console Cable 6 ft with USB Type A and mini-B

MEM-3900-1GU2GB	1GB to 2GB DRAM Upgrade (1GB+1GB) for Cisco 3925/3945 ISR
PWR-3900-AC/2	Cisco 3925/3945 AC Power Supply (Secondary PS)
CON-SNTP-3945	SMARTNET 24X7X4 Cisco 3945 w/SPE150

R KEY SERVER	ROUTER COMO SERVIDOR DE LLAVES DE ENCRIPCION (2)
CISCO2911-HSEC+/K9	VPN ISM module HSEC bundles for 2911 ISR platform
CON-SNTP-2911HSEC	SMARTNET 24X7X4 AIM VPN module HSEC bundles for 2911 ISR
S29UK9-15302T	Cisco 2901-2921 IOS UNIVERSAL
FL-29-HSEC-K9	U.S. Export Restriction Compliance license for 2921/2951
PWR-2911-AC	Cisco 2911 AC Power Supply
CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m
ISM-VPN-29	3DES/AES/SUITE-B VPN Encryption module
PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE
SL-29-IPB-K9	IP Base License for Cisco 2901-2951
HWIC-BLANK	Blank faceplate for HWIC slot on Cisco ISR
ISR-CCP-EXP	Cisco Config Pro Express on Router Flash
MEM-2900-512MB-DEF	512MB DRAM for Cisco 2901-2921 ISR (Default)
MEM-CF-256MB	256MB Compact Flash for Cisco 1900 2900 3900 ISR
SL-29-SEC-K9	Security License for Cisco 2901-2951
SM-S-BLANK	Removable faceplate for SM slot on Cisco 290039004400 ISR

Switches LAN

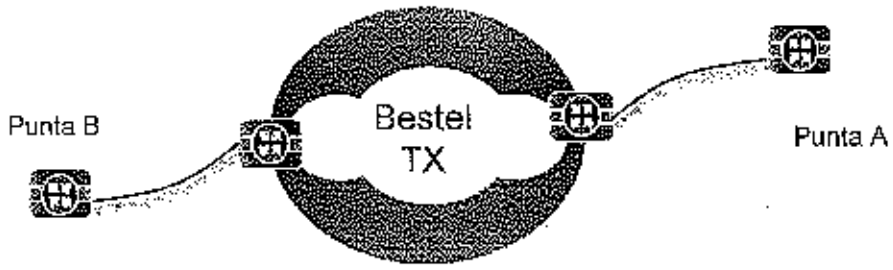
Los equipos propuestos son de la marca Cisco

SW-24	Switch Lan L2 (24 puertos),
WS-C2960S-24TS-S	Catalyst 2960S 24 GigE 2 x SFP LAN Lite
CON-SNTP-2960S2SS	SMARTNET 24X7X4 Cat 2960S 24 GigE2 x SFP LAN Lite
CAB-16AWG-AC	AC Power cord 16AWG
PI-MSE-PRMO-INSRT	Insert Packout - PI-MSE

Apartado Enlace Lan to Lan

OPERBES, S.A. en caso de que SHF lo requiera suministrará el servicio de enlace Lan to Lan para interconexión de dos sitios por medio de tecnología Ethernet.

A continuación se presenta la arquitectura considerada para el servicio.


Punta B
Bestel
TX
Punta A

Apartado Videoconferencia

Los equipos propuestos son de la marca Cisco

	SOLUCION VIDEOCONFERENCIA DE ESCRITORIO
CTS-EX90-K9	EX90 - NPP Touch UI
CON-NE4N-CTS-EX90	SNTC ESS 24X7X4 EX90 base system including NPP option
SW-S52000-TC6.XK9	Software Image TC6.x Encryption
PWR-CORD-US-A	Pwr Cord US 1.8m Black YP-12 To YC-12
CTS-CTRL-DV8	Touch Control for EX Series with cradle and handset
LIC-ECXX-NPP	EX NPP option
LIC-EX90	EX90 Product License Key
LIC-S52000-TCX.XK9	License Key Software Encrypted

	SOLUCION VIDEOCONFERENCIA DE SALA
CTS-SX20-12XK9-PRM	SX20 Quick Set HD NPP 12xPHDCam 1 mic remote cntrl
CON-NE4N-SX2012XK	SNTC ESS 24X7X4 SX20 QuickSetHDNPP12xPHDCammicremote
LIC-SX20-NPP	SX20 Natural Presenter Package (NPP) Option
SW-S52010-TC6-K9	SW Image Encrypted SX Series
PWR-CORD-US-A	Pwr Cord US 1.8m Black YP-12 To YC-12
CTS-QSC20-MIC	Performance Microphone 20
LIC-SX20-PR	Premium Resolution Option for SX20
BRKT-PHD-MONITOR	Bracket mounting for 12x PHDCAM to monitor
CAB-2HDMI-3M	HDMI to HDMI cable
CAB-HDMI-PHD12XS	Custom 12xcamera cable; HDMI Cont. and Power (3m)
CTS-PHD1080P12XS2+	PrecisionHD Camera 1080p 12x Gen 2 for use in auto expand
CTS-QSC20-MIC+	Performance Mic - for auto expand only
CTS-RMT-TRC5	Remote Control TRC 5
CTS-SX20CODEC-K9	SX20 Codec – encrypted
LIC-S52010-TC-K9	License Key Software Encrypted
LIC-SX20	SX20 License Key
LIC-SX20-DD	Dual Display Option for SX20
LIC-SX20-HD	High Definition Feature for SX20
LIC-SX20-MS	MultiSite Option for SX20

	MCU PARA 10 TERMINALES
CTI-5320-MCU-K9	Cisco TelePresence MCU 5320 up to 40 SD ports
CON-NE4N-	SNTC ESS 24X7X4 Telepresence MCU 5320 up to 40 SD ports

CTI5320M	
PWR-CORD-US-C	US power cord
LIC-AESMCU53-K9	AES and HTTPS option for MCU 5300 Series
CTI-5300-CAB2MCU	Cisco TelePresence MCU 5300 Series Stacking Cable
CON-NE4N-CTI53CAB	SNTC ESS 24X7X4 MCU 5300 Series Stacking Cable
LIC-5300-4PL	1 Full HD / 2 HD / 4 SD ports on MCU 5300 Series
CON-NE4N-LIC5304P	SNTC ESS 24X7X4 1 Full HD/2 HD/4 SD ports on MCU5300
LIC-5320-MCU-K9	License Key For MCU 5320 Software Image
SW-5300-MCU-K9	Software Image For MCU 5300 Series Latest Version

	MCU PARA 20 TERMINALES
CTI-5320-MCU-K9	Cisco TelePresence MCU 5320 up to 40 SD ports
CON-NE4N-CTI5320M	SNTC ESS 24X7X4 Telepresence MCU 5320 up to 40 SD ports
PWR-CORD-US-C	US power cord
LIC-AESMCU53-K9	AES and HTTPS option for MCU 5300 Series
LIC-5300-4PL	1 Full HD / 2 HD / 4 SD ports on MCU 5300 Series
CON-NE4N-LIC5304P	SNTC ESS 24X7X4 1 Full HD/2 HD/4 SD ports on MCU5300
CTI-5300-CAB2MCU	Cisco TelePresence MCU 5300 Series Stacking Cable
CON-NE4N-CTI53CAB	SNTC ESS 24X7X4 MCU 5300 Series Stacking Cable
LIC-5320-MCU-K9	License Key For MCU 5320 Software Image
SW-5300-MCU-K9	Software Image For MCU 5300 Series Latest Version

	MCU PARA 30 TERMINALES
CTI-5320-MCU-K9	Cisco TelePresence MCU 5320 up to 40 SD ports
CON-NE4N-CTI5320M	SNTC ESS 24X7X4 Telepresence MCU 5320 up to 40 SD ports
LIC-5300-4PL	1 Full HD / 2 HD / 4 SD ports on MCU 5300 Series
CON-NE4N-LIC5304P	SNTC ESS 24X7X4 1 Full HD/2 HD/4 SD ports on MCU5300
PWR-CORD-US-C	US power cord
LIC-AESMCU53-K9	AES and HTTPS option for MCU 5300 Series
CTI-5300-CAB2MCU	Cisco TelePresence MCU 5300 Series Stacking Cable
CON-NE4N-CTI53CAB	SNTC ESS 24X7X4 MCU 5300 Series Stacking Cable
LIC-5320-MCU-K9	License Key For MCU 5320 Software Image
SW-5300-MCU-K9	Software Image For MCU 5300 Series Latest Version
CTI-5320-MCU-K9	Cisco TelePresence MCU 5320 up to 40 SD ports
CON-NE4N-CTI5320M	SNTC ESS 24X7X4 Telepresence MCU 5320 up to 40 SD ports
CTI-5300-	Cisco TelePresence MCU 5300 Series Stacking Cable

CAB2MCU	
CON-NE4N-CTI53CAB	SNTC ESS 24X7X4 MCU 5300 Series Stacking Cable
LIC-5320-MCU-K9	License Key For MCU 5320 Software Image
SW-5300-MCU-K9	Software Image For MCU 5300 Series Latest Version
PWR-CORD-US-C	US power cord
LIC-AESMCU53-K9	AES and HTTPS option for MCU 5300 Series
LIC-5300-4PL	1 Full HD / 2 HD / 4 SD ports on MCU 5300 Series
CON-NE4N-LIC5304P	SNTC ESS 24X7X4 1 Full HD/2 HD/4 SD ports on MCU5300

	PLATAFORMA DE CONTROL DE VIDEO (HW Y SW, TIENE PRECIOS UNITARIOS POR CADA UNIDAD QUE SERÁ CONTROLADA)
CTI-VCS-CONTRL-K9	VCS Control
CON-NE4N-SCNTRLK9	SNTC ESS 24X7X4 VCS Cntrl
LIC-VCS-GW	Enable GW Feature (H323-SIP)
LIC-VCSE-100	Video Communication Server - 100 Traversal Calls
LIC-VCS-BASE-K9	License Key - VCS Encrypted Software Image
SW-VCS-7.X-K9	Software Image for VCS with Encryption Version 7.X
PWR-CORD-US-A	Pwr Cord US 1.8m Black YP-12 To YC-12
LIC-VCS-10	Video Comm Server 10 Add Non-traversal Network Calls
CON-NE4N-LICVCS10	SNTC ESS 24X7X4 VCS 10 Add Non-traversal Ntwk Calls

Apartado Administración de Tráfico y Optimización de Aplicaciones se describe la solución propuesta

Los equipos propuestos son de la marca Riverbed
De los siguientes modelos

CXA 7055-L
CXA 5055-M
CXA 1555-M
CXA 755-H
CXA 555-H
CXA 255-H

Apartado Continuidad de la Operación.

METODOLOGÍA Y PLAN PARA CONTINGENCIAS QUE SE TIENEN PARA CUBRIR LAS EVENTUALIDADES OCASIONADAS POR DESASTRES

Planes y Contingencias.

OPERBES S.A. DE C.V. cuenta desde Enero del 2007 con políticas internas de Continuidad del Negocio las cuales le permiten a OPERBES S.A. DE C.V. tener un Plan de Continuidad y Recuperación en caso de desastre, incendio o cualquier suceso que atente con la continuidad del negocio de OPERBES S.A. DE C.V.

A continuación OPERBES S.A. DE C.V. describe las principales políticas que ha desarrollado para hacer frente a amenazas potenciales.

Políticas de Continuidad del Negocio en caso de contingencia.

Las políticas de Continuidad del Negocio, tienen como objetivo proteger los procesos críticos del negocio de OPERBES S.A. DE C.V., contra desastres o fallas mayores, junto con las posibles consecuencias que se puedan derivar de ellas, como pérdidas operacionales, infraestructura y otras de tipo financiero, productividad y comerciales, esto originado a la no disponibilidad de los recursos de la organización. Las políticas de Continuidad del Negocio buscan mitigar el riesgo a dichas fallas o desastres, mediante diferentes acciones que permita la pronta recuperación de la operación, en caso de presentarse algún evento que afecte el flujo normal de las actividades de OPERBES S.A. DE C.V.

Políticas Generales de Continuidad del Negocio:

Políticas documentadas con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto a la operación del negocio de OPERBES S.A. DE C.V.

Políticas de Contingencia:

Es un subconjunto de las Políticas de Continuidad del Negocio, que contempla cómo reaccionar ante una contingencia que pueda afectar la disponibilidad o los servicios ofrecidos por los enlaces y equipos de OPERBES S.A. DE C.V. Una contingencia puede ser un problema de un doble corte de fibra óptica, pérdida de la comunicación de un punto de presencia de OPERBES S.A. DE C.V., corrupción de las bases de datos de las centrales telefónicas de OPERBES S.A. DE C.V., pérdida mayor de los equipos de OPERBES S.A. DE C.V., el suministro eléctrico, un problema de software o hardware, errores humanos, sabotaje, intrusiones y cualquier otro que atente con la operación de OPERBES S.A. DE C.V.

Políticas de Recuperación Frente a Desastres:

Es aquella parte de las políticas de contingencia y de las políticas de continuidad de negocio que aborda aquellas contingencias que por su gravedad no permiten continuar prestando los servicios de OPERBES S.A. DE C.V. en cualquiera de sus edificios y debe continuarse los servicios desde un nuevo edificio. Este plan debe contemplar la vuelta atrás cuando, tras arreglar las consecuencias del desastre, los servicios puedan ser reanudados en el centro local.

Políticas de Impacto al Negocio:

La Política de Impacto al Negocio es mantener un documento que ayude a entender el impacto que un desastre pueda tener sobre un negocio en particular. Contempla dos objetivos fundamentales:

Proporciona la Prioridad a los Procesos Críticos del Negocio.

Se establece el tiempo máximo sin servicio que OPERBES S.A. DE C.V. puede soportar y seguir siendo una compañía que cumpla con sus objetivos de negocio.

Plan de Continuidad, Contingencia, Protección y Restablecimiento Rutas de Servicios y Protección en Anillo

Objetivo

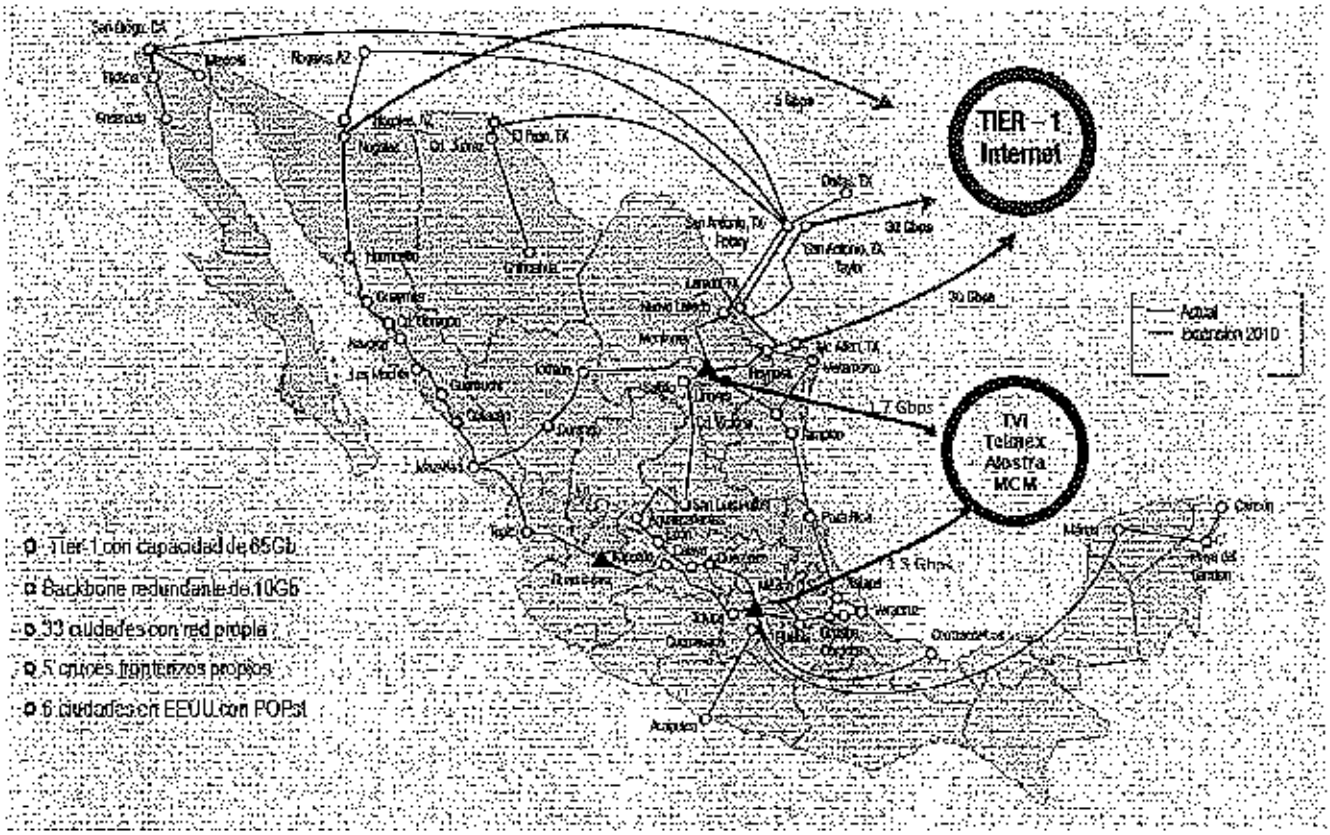
El presente documento establece las generalidades sobre las cuales se basó el diseño del Plan de Desastres para Protección y Restablecimiento de Servicios en la Red de OPERBES S.A. DE C.V. y que abarca diversos aspectos como son topología de la red de transporte, tanto en planta externa, como en equipos DWDM y SDH.

Generalidades

La Red de Terrestre de OPERBES S.A. DE C.V. consta de una infraestructura principal o "Backbone" de Fibra Óptica con capacidad de 60 fibras ópticas corriendo en el Derecho de Vía del FFCC y 72 fibras en el Derecho de Vía de la red eléctrica de la CFE, a través de las cuales OPERBES S.A. DE C.V. brinda su servicio.

La red contempla nodos de acceso y regeneración los cuales integran dos anillos (uno Norte y otro Sur). Por medio de estos se cuenta con acceso a ciudades principales tales como: México, Toluca, Irapuato, Guadalajara, Tepic, Mazatlán, Durango, Torreón, Monterrey, Saltillo, San Luis Potosí, Aguascalientes, León, Celaya, Querétaro, e inclusive en los EE.UU., en Laredo, San Antonio y Mc Allen, entre otros.

El esquemático de físico y geográfico de la red es la siguiente:



Red de Fibra Óptica de Transmisión de BackBone OPERBES S.A. DE C.V.

Descripción

La protección de las rutas del BackBone de OPERBES S.A. DE C.V. se ha diseñado en varios niveles, sin embargo se centran principalmente en una configuración de anillo, en donde los niveles antes mencionados son:

Redundancia de ruta (fibra óptica).
Redundancia en vías lógicas equipo de transporte DWDM
Protección de anillo en equipo de transporte SDH
Protección de tarjetas críticas en equipo SDH.

Redundancia de Ruta de Fibra.

La redundancia de ruta se realiza para tener una trayectoria alterna para ser utilizada en la protección del tráfico en caso de una afectación o desastre debido a causas naturales o provocadas.

Generalmente las rutas son independientes, sin embargo en el caso de la ruta Laredo a San Antonio se aplica un criterio distinto.

Para el BackBone de OPERBES S.A. DE C.V. se han formado 2 anillos: el Anillo Norte y el Anillo Sur.

El anillo Norte consta de:

Monterrey, Candela, Nuevo Laredo, Laredo, Artesia, Moore, San Antonio Rotary, San Antonio Taylor, Mirando, San Isidro, Hidalgo, Mc Allen, Reynosa y General Bravo.

El Anillo Sur consta de:

Monterrey, Saltillo, Salado, Laguna Seca, San Luis Potosí, Salinas, Aguascalientes, León, Celaya, Querétaro, Nopala, México, Toluca, Salvatierra, Irapuato, Yurecuaro, Guadalajara, San José de Gracia, Tepic, Ruiz, Escuinapa, Mazatlán, Las Adjuntas, Durango, Yerbaniz, Torreón, Talia, Sauceda.

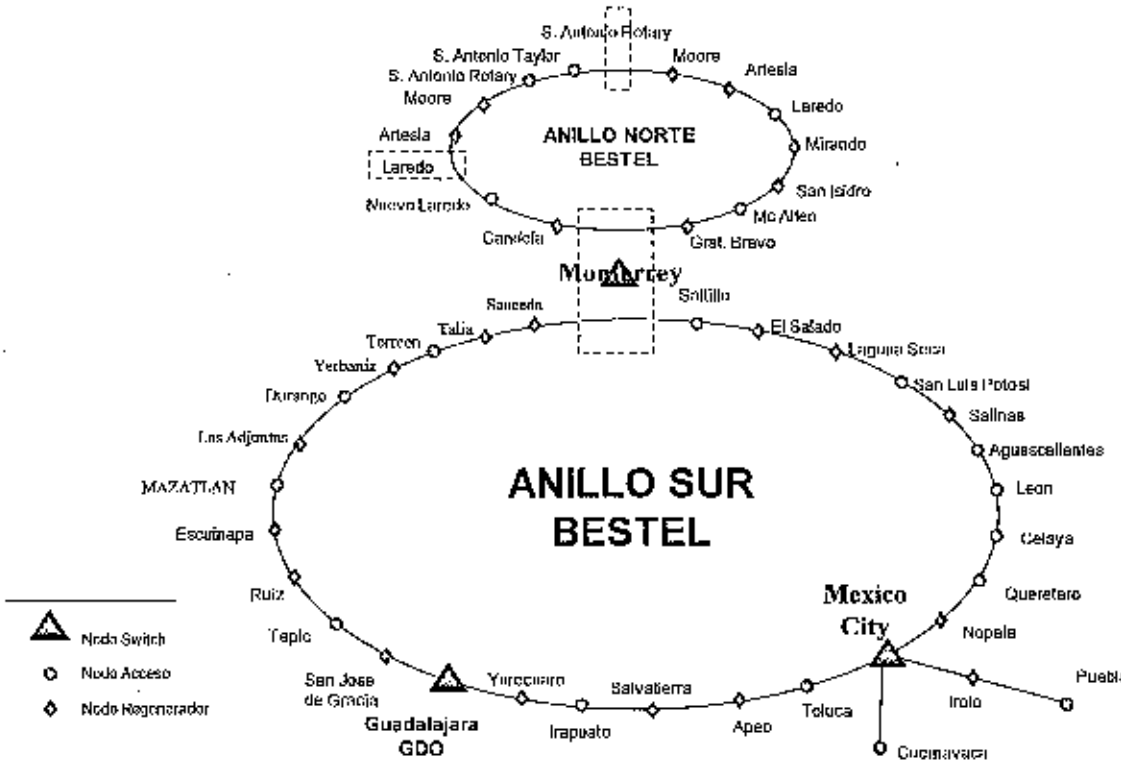
A continuación se presentan esquemas lógicos para facilitar la comprensión de la protección ya que sobre una misma ruta física se pueden utilizar diferentes fibras para formar el anillo.

En la figura de abajo se presenta el esquemático de rutas lógicas de los anillos del BackBone.

Cabe mencionar que la ruta marcada entre nodos se refiere a que existe un par de fibras conectando dichos nodos. En el caso del anillo Norte se presenta el nodo de Laredo, Artesia, Moore y Rotary duplicados ya que se utilizan fibras independientes en una misma ruta física para conectar a los nodos.

Por otra parte en Artesia y Moore se tienen fibras y equipo independientes para cada trayecto, mientras en Laredo y Rotary en un caso la fibra independiente pasa el nodo sin tocar ningún equipo (by-pass) y en el otro, las fibras pasan el nodo tocando equipos.

RUTAS LOGICAS BACKBONE BESTEL



Anillos OPERBES S.A. DE C.V. (Esquemático lógico)

Redundancia en vías lógicas DWDM

Sobre la Red de fibra óptica de transmisión de OPERBES S.A. DE C.V. se ha instalado equipo DWDM, el cual, permite con un par de fibras establecer hasta 96 vías o canales lógicos que pueden ser usados para transportar y/o proteger el tráfico. Este equipo se ha configurado para disponer de vías lógicas a lo largo del anillo y así, asegurar la redundancia de ruta.

La protección de tráfico no se realiza en el DWDM, ya que la funcionalidad de la protección la soporta y es una función natural del equipo SDH.

El equipo DWDM soporta, como ya se mencionó, hasta 96 canales (vías) o más dependiendo de su equipamiento.

La configuración instalada en el BackBone contempla la operación de una cantidad importante de canales o lambdas en ambos anillos lo cual facilita la construcción de la redundancia en ambas direcciones.

Dos ventajas adicionales del DWDM son:

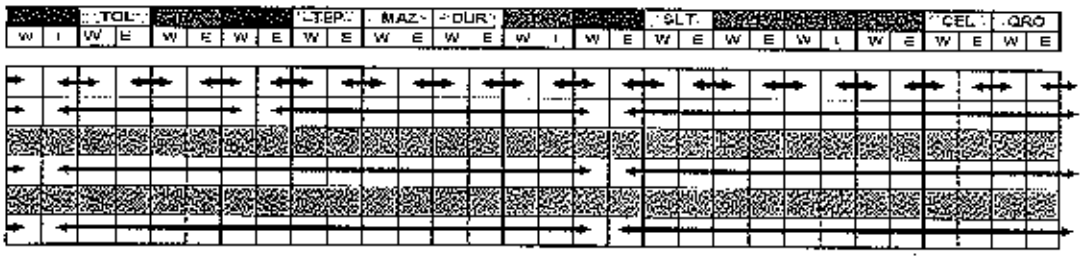
La eliminación de equipos regeneradores SDH, ya que el DWDM tiene la capacidad de incorporar tarjetas regeneradoras en su plataforma.

La eliminación del cálculo de presupuesto óptico en los equipos SDH, dando en consecuencia la utilización de tarjetas de Agregados de Línea de menor potencia.

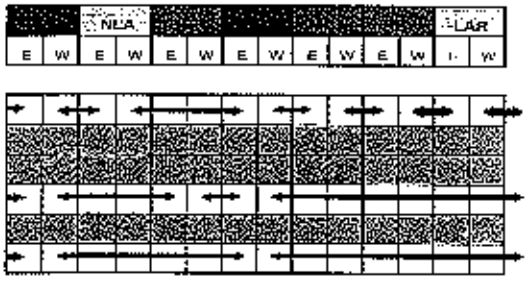
La Configuración de canales en DWDM se ha diseñado como sigue:

ENLACES DE CANALES 2.5Gbps DWDM

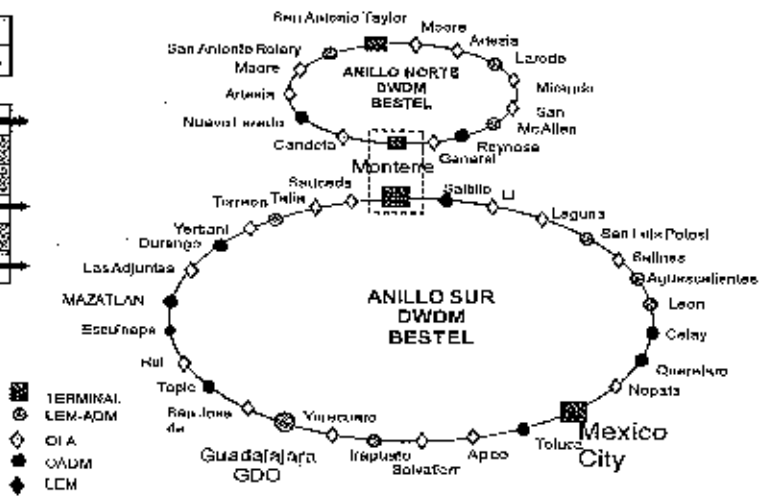
ANILLO SUR



ANILLO NORTE

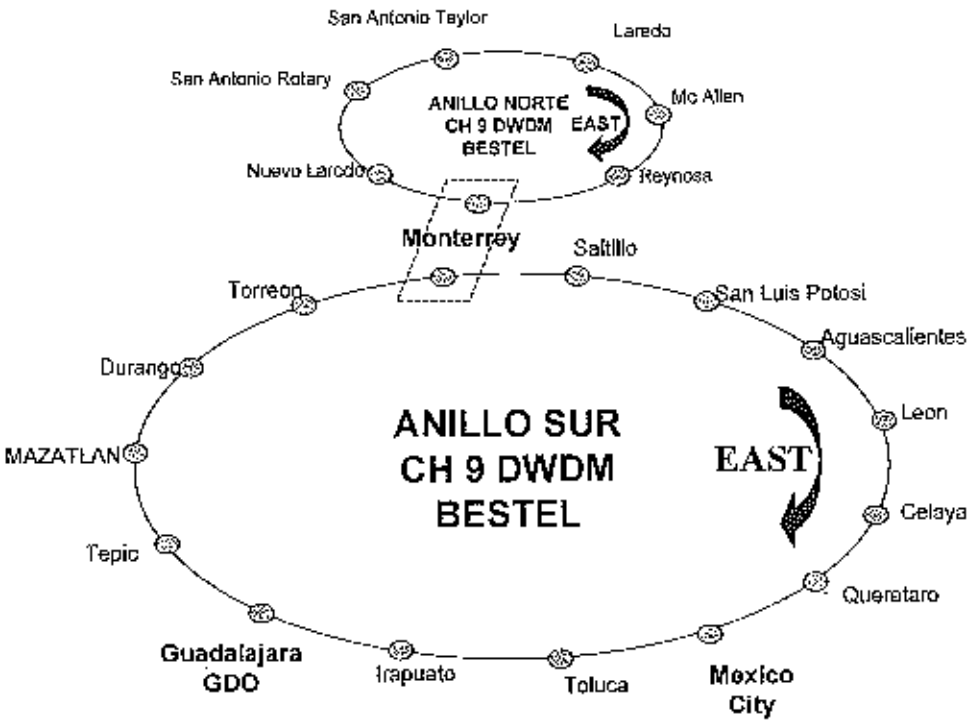


Configuración de Canales DWDM

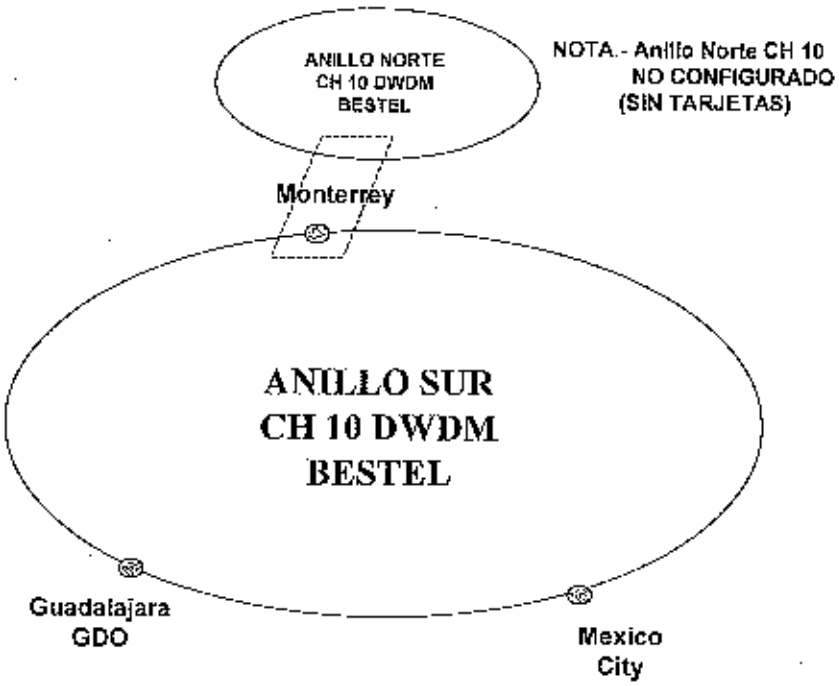


Gráficamente y a manera de ejemplo los nodos del Anillo Norte y Sur, se presentan en la siguiente figura:

NODOS ANILLOS CH 9 DWDM BESTEL



NODOS ANILLOS CH 10 DWDM BESTEL



Cabe mencionar que para cada Nodo de los anillos se dispone de una capacidad a nivel STM-16, la cual será provista con un equipo SDH.

Protección de Anillo en Equipo SDH.

La funcionalidad de protección de anillo proporciona la utilización de la redundancia lógica y física de la red, con una rapidez de protección en MS-SPRING de 50 a 300ms, y en SNCP de 50ms.

La diferencia entre la protección MS-SPRING a SNCP se centra principalmente en el ancho de banda utilizable en el anillo y en el tiempo de protección real del trafico.

Protección SNC (Sub Network Connection)

Un anillo protegido SNCP solo permite utilizar, en equipos STM-16, hasta un máximo de 16 STM-1 protegidos, ya que él tráfico utiliza el trayecto físico y lógico de trabajo y de redundancia al mismo tiempo.

Su tiempo de protección es el tiempo de conmutación del equipo, típicamente 50ms.

Los equipos terminales de los servicios son los que conmutan, ya que los demás de antemano están configurados para manejar la infonnación en ambas vías.

La topología del anillo se llama Unidireccional (aunque los enlaces sean bidireccionales).

Protección MS-SPRING (Mutiplex Section Share Protection RING)

En un anillo protegido MS-SPRING el ancho de banda es mayor, ya que como no se manda la señal en ambas direcciones del anillo, se puede utilizar la ruta de protección para trabajo.

La protección entonces es compartida a nivel STM-1, de los 16, 8 son de trabajo y 8 son de protección. Esto al contrario de disminuir la capacidad del anillo, permite, en equipos STM-16, hasta un máximo de 8 STM-1 X No de Nodos en el anillo, considerando que todo él tráfico va entre nodos contiguos.

El precio de ésta protección es el tiempo de protección de los enlaces, ya que el trayecto de redundancia física y lógica no se utiliza hasta que llegue un criterio de protección. Es hasta entonces que los equipos automáticamente se configuran para proteger el tráfico afectado.

El tiempo de conmutación de un equipo es de 50 ms, sin embargo, cada uno de los equipos en el anillo debe autoconfigurarse para permitir la protección.

El comando para indicar la autoconfiguración es insertado en el encabezado de la siguiente trama SDH (125ms por trama) a ser transmitida al siguiente nodo, mas el tiempo de propagación.

La topología del anillo se llama Bidireccional.

Las fallas que cubren ambas protecciones son:

Fibra

Corte de fibra en un punto, todo él tráfico se protege.

Corte de fibra en dos puntos, el tráfico que cruza los puntos de corte se pierde, sin embargo, el que no lo cruza queda trabajando.

Se protegen la Tarjeta de Agregado de Línea, debido a que el daño de una tarjeta de este tipo representa en gran parte una similitud al corte de fibra o degradación de señal, la protección de anillo cubre esta falla.

Para la implementación del equipo SDH se ha definido la tecnología de equipo SDH, sobre los nodos de los anillos Norte y Sur del equipo DWDM.

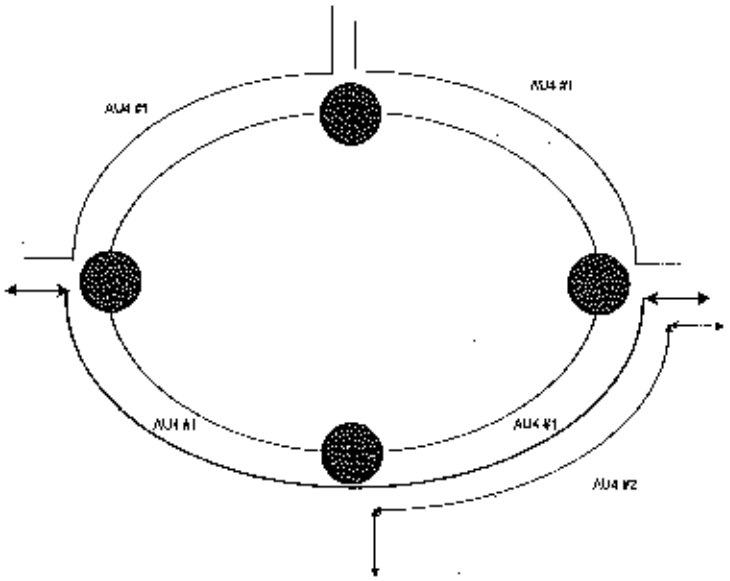
La red de OPERBES S.A. DE C.V. se ha implementado utilizando la protección MS-SPRING.

El funcionamiento de la protección MS-SPRING es el siguiente:

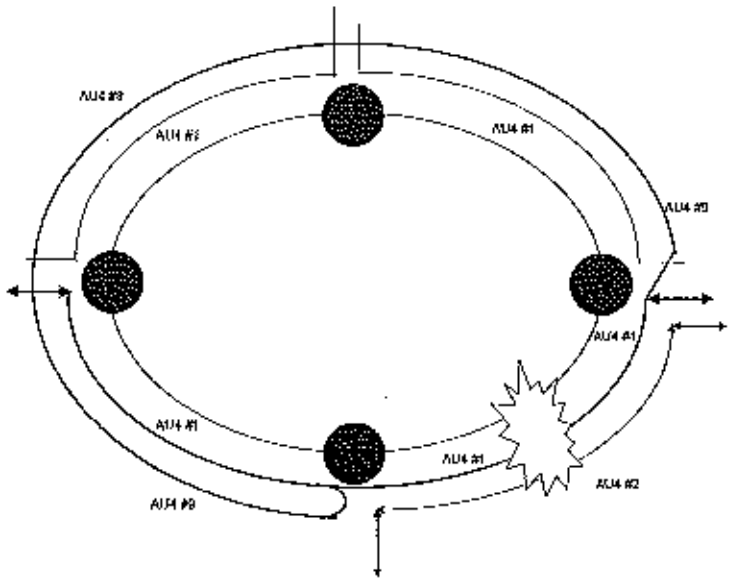
Considere un anillo con 4 nodos.

Considere que se tienen servicios entre nodos 2-3, 3-4, 1-2 y 2-4.

Debido a que la topología del anillo es bidireccional y que se usan 8 AU4 de trabajo y 8 de protección, en cada una de las tarjetas agregados de línea considere que los servicios 2-3, 3-4 y 2-4 van en el AU4#1, mientras el 1-2 va por el AU4#2.



Supongamos un corte de fibra entre el nodo 1 y 4. Los servicios que no atraviesan la ruta abierta no se ven afectados, sin embargo los servicios que sí, se conmutan a su respectivo AU4 del 9 al 16. La conmutación se realiza en los equipos inmediatamente involucrados en el corte, mas no en los que suben y bajan él tráfico. En éste caso, el servicio que va del nodo 2-4 sobre el AU4#1 conmuta al AU4#9 en equipos de los nodos 1 y 4 y, retorna por todo el anillo para llegar al equipo del nodo 4.



El servicio del nodo 1-4 que va sobre el AU4#2 conmuta al AU4#10. Los servicios protegidos dan la vuelta a todo el anillo, en este caso del nodo 1 se retornan pasando a través de los nodos 2 y 3, usando el AU4#10 hasta llegar al nodo 4, que lo conmuta al AU4 #2 y de ahí baja él tráfico.

Cabe mencionar que en la protección, aparte de la conmutación del tráfico en los nodos directamente afectados por el corte, todos los equipos de los nodos del anillo se autoconfiguran para dar

paso al tráfico protegido (pass frought). La distancia que debe de recorrer la señal protegida puede ser igual o mayor que la longitud del anillo.

Protección de Tarjetas Críticas en Equipo SDH.

Los equipos SDH adicionalmente tienen protección de tarjetas (protección en hardware). La cual puede ser 1 + 1 o 1 + N, en el caso de la configuración instalada en OPERBES S.A. DE C.V. se cuenta con la siguiente protección.

Configuración 1+1:

Tarjeta Fuente de Poder
Reloj de Sincronía
Tarjeta Crosconectora

Configuración 1 + N

Tarjeta 63XE1. En un solo enlace el equipo de Lucent conmuta los servicios a la tarjeta de respaldo, esto en el caso que la de trabajo se haya dañado.

Conclusión.

La red de OPERBES S.A. DE C.V. ha sido diseñada para garantizar los más altos requerimientos de seguridad y confiabilidad de la red, garantizando la continuidad de los servicios de sus clientes con base a tecnología altamente probada y confiable.

El manejo de la protección mediante equipo SDH y utilizando una topología de Anillo Bidireccional confiabilidad a un costo de unos milisegundos de conmutación.

El equipo DWDM incrementa la protección física y además la capacidad en una plataforma de anillos virtuales sobre un par de fibras.

Todo esto crea una base sólida para la protección del tráfico y los servicios de OPERBES S.A. DE C.V. y garantizan un nivel de servicio "CARRIER-CLASS", que respalda las aplicaciones, facilidades e inversión de nuestros clientes aún bajo condiciones de riesgo y afectación en caso de un desastre.

Apartado contención de ataques en el perimetro de Internet
Los equipos propuestos son de la marca Arbor modelos

Tipo 1
Pravail APS 2105
Pravail APS 2100---Series Spare.
Tipo 2
Pravail APS 2104
Pravail APS 2100
Tipo 3
Pravail APS 2003
Pravail APS 2000
Tipo 4
Pravail APS 2002
Pravail APS 2000---

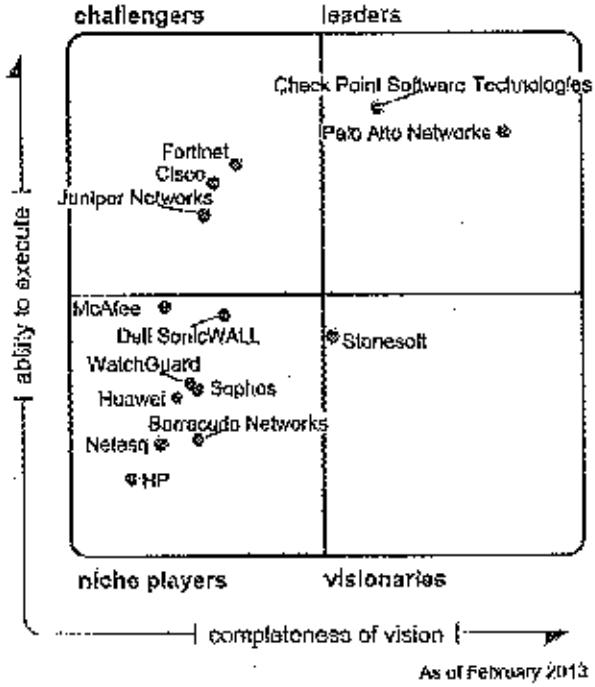
Apartado Administrador de Ancho de Banda

Se proponen equipos de la marca Exinda modelos

EX-6762-1G
EX-6762-500
EX-4761-100
EX-4710-50
EX-4710-20
EX-2861-6
EX-2861-1

Apartado Firewall

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (February 2013)

Los equipos Propuestos son de la marca Fortinet de los siguientes modelos:

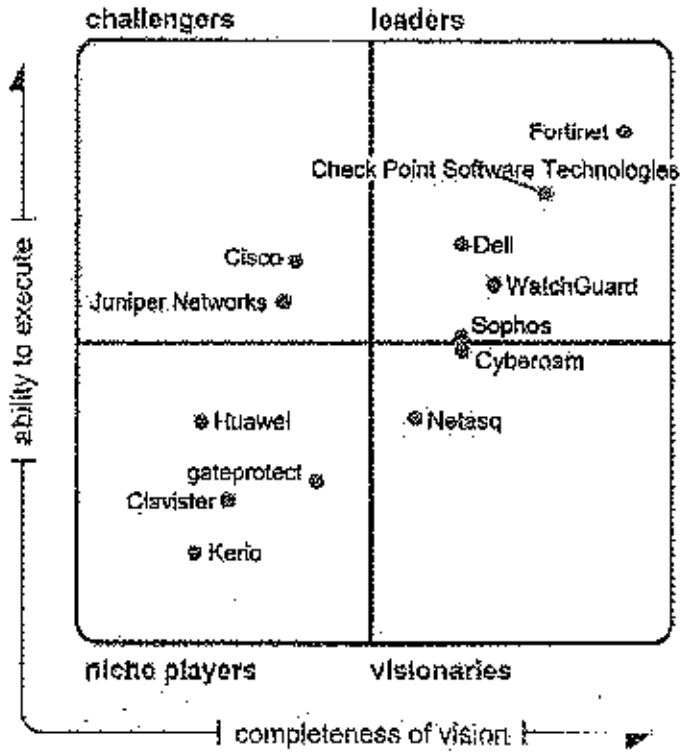
Tipo 1
FortiGate 3040B

Tipo 2
FortiGate 3040B
Tipo 3
FortiGate 600C
Tipo 4
FortiGate 200D
Tipo 5

Apartado WAF
Los equipos propuestos son de la marca Fortinet de los modelos:
Tipo 1
FWB-4000D-BDL
Tipo 2
FWB-3000D-BDL
Tipo 3
FWB-1000D-BDL

Apartado UTM
Se proponen equipos de la marca fortinet.

Figure 1. Magic Quadrant for Unified Threat Management



Source: Gartner (July 2013)

Los equipos propuestos son

Tipo 1
FG-800C-BDL-950-36

Tipo 2
FG-800C-BDL-950-36

Tipo 3
FG-300C-BDL-950-36

Tipo 4
FG-200D-BDL-950-36

Tipo 5
FG-200D-BDL-950-36

Apartado PCMW

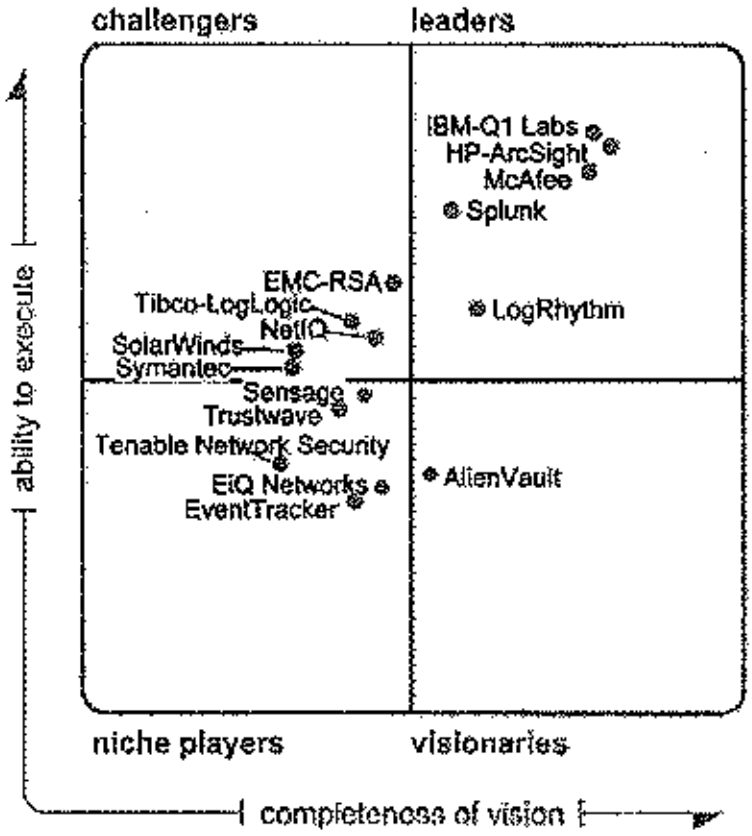
Los equipos propuestos son de la marca FireEye de los modelos

Tipo 1
4400NX-HW

Tipo 2
4400NX-HW
Tipo 3
4400NX-HW

Apartado Correlacionador

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (May 2013)

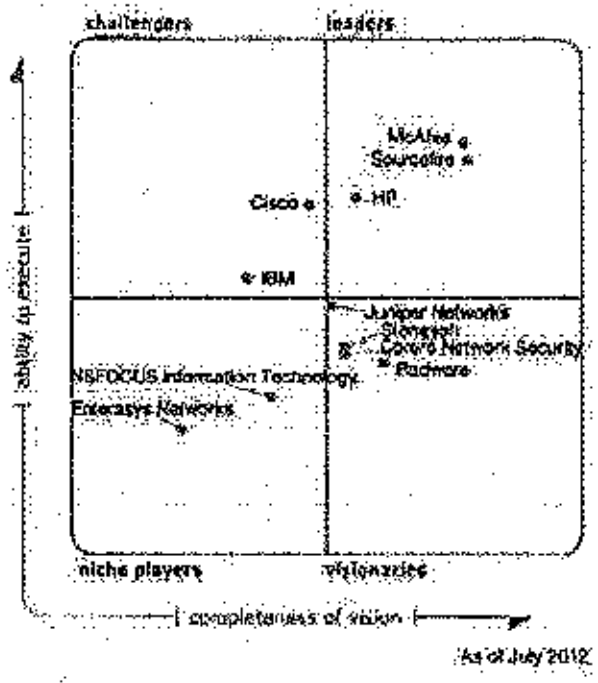
Los equipos propuestos son de la marca Mcafee de los modelos:

Correlacionador Tipo 1
ETM5600
Correlacionador Tipo 2
ETM5600
Correlacionador Tipo 3
ETM5600
Colector Tipo 1
ERC1250
Colector Tipo 2
ERC1250
Colector Tipo 3
ERC1250

Apartado IPS

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Intrusion Prevention Systems



Source: Gartner (July 2012)

Los equipos propuestos son de la marca SourceFire de los modelos:
Tipo 1
3D8140-IPS-000-CHAS
Tipo 2
3D8130-IPS-000-CHAS
Tipo 3
3D7120-IPS-C08-000
Tipo 4
3D7110-IPS-C08-000
Tipo 5
3D7030-IPS-C08-000

Apartado Borrado de discos seguro

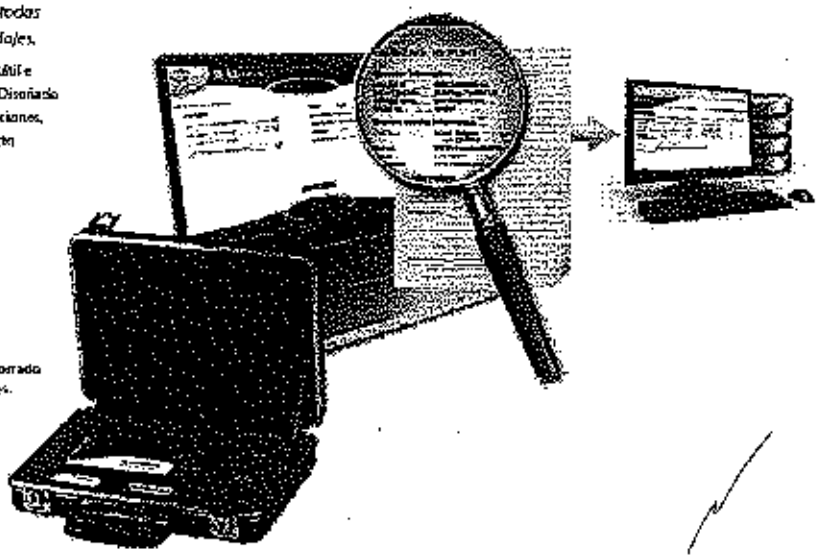
Se propone la Herramienta Blancco Toolkit 2.0. de la cual se describen a continuación las principales características:

Blancco Toolkit 2.0

Una solución fácil, ligera y portátil para satisfacer todas sus necesidades de borrado de datos durante los viajes.

Blancco Toolkit 2.0 es la solución perfecta de borrado, portátil e independiente, que no precisa red ni conexión a Internet. Diseñado para realizar borrado de datos dentro y fuera de las instalaciones, su funda de fibra de carbono le otorga un aspecto y un tacto elegante y profesional.

- Productividad mejorada mediante un borrado de datos rápido y simple.
- Tranquilidad con un borrado 100 % seguro.
- Fácil de usar como herramienta portátil para el borrado durante viajes y dentro y fuera de las instalaciones.
- Comodidad para almacenar una cantidad ilimitada de licencias.



ESPECIFICACIONES TÉCNICAS

ADMINISTRACIÓN DE USUARIOS & PORTABILIDAD:

- Se instala con facilidad y es extremadamente fácil de usar
- Funciona como una herramienta de borrado totalmente independiente, sin necesidad de Internet ni conexión a la red
- Software personalizado para su organización
- Su pequeño tamaño exige el mínimo espacio (300 mm x 200 mm x 75 mm; peso 1,2 kg)
- Su atractiva funda de fibra de carbono es compacta y ligera

BORRADO:

- Cada kit realiza entre 75 y 100 borrados al día
- Crea un proceso de destrucción de datos en solo 5 minutos
- Cumple con reconocidos estándares de borrado internacionales
- Perfecto para el borrado en uno o múltiples emplazamientos

INFORMES & AUDITORÍA:

- Tras realizar el proceso de borrado, genera automáticamente informes detallados y certificados
- Ofrece informes exhaustivos como prueba del proceso de borrado para protegerse de riesgos por incumplimiento de responsabilidades.
- Los informes proporcionan datos de los activos tales como etiquetas del servicio, etiquetas de los activos y números de serie

CONTENIDO:

- Funda exterior de fibra de carbono (300 mm x 200 mm x 75 mm, peso 1,2 kg)
- CD del software de sistema
- Clave HASP para el almacenamiento de licencias
- USB de 4 GB con aplicación de arranque USB de serie
- Linterna de LED súper brillante
- Herramienta múltiple 12 en 1

www.blancco.com

Apartado SOC y NOC

METODOLOGÍA Y PLAN PARA CONTINGENCIAS QUE SE TIENEN PARA CUBRIR LAS EVENTUALIDADES OCASIONADAS POR DESASTRES

Planes y Contingencias.

OPERBES S.A. DE C.V. cuenta desde Enero del 2007 con políticas internas de Continuidad del Negocio las cuales le permiten a OPERBES S.A. DE C.V. tener un Plan de Continuidad y Recuperación en caso de desastre, incendio o cualquier suceso que atente con la continuidad del negocio de OPERBES S.A. DE C.V.

A continuación OPERBES S.A. DE C.V. describe las principales políticas que ha desarrollado para hacer frente a amenazas potenciales.

Políticas de Continuidad del Negocio en caso de contingencia.

Las políticas de Continuidad del Negocio, tienen como objetivo proteger los procesos críticos del negocio de OPERBES S.A. DE C.V., contra desastres o fallas mayores, junto con las posibles consecuencias que se puedan derivar de ellas, como pérdidas operacionales, infraestructura y otras de tipo financiero, productividad y comerciales, esto originado a la no disponibilidad de los recursos de la organización. Las políticas de Continuidad del Negocio buscan mitigar el riesgo a dichas fallas o desastres, mediante diferentes acciones que permita la pronta recuperación de la operación, en caso de presentarse algún evento que afecte el flujo normal de las actividades de OPERBES S.A. DE C.V.

Políticas Generales de Continuidad del Negocio:

Políticas documentadas con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto a la operación del negocio de OPERBES S.A. DE C.V.

Políticas de Contingencia:

Es un subconjunto de las Políticas de Continuidad del Negocio, que contempla cómo reaccionar ante una contingencia que pueda afectar la disponibilidad o los servicios ofrecidos por los enlaces y equipos de OPERBES S.A. DE C.V. Una contingencia puede ser un problema de un doble corte de fibra óptica, pérdida de la comunicación de un punto de presencia de OPERBES S.A. DE C.V., corrupción de las bases de datos de las centrales telefónicas de OPERBES S.A. DE C.V., pérdida mayor de los equipos de OPERBES S.A. DE C.V., el suministro eléctrico, un problema de software o hardware, errores humanos, sabotaje, intrusiones y cualquier otro que atente con la operación de OPERBES S.A. DE C.V.

Políticas de Recuperación Frente a Desastres:

Es aquella parte de las políticas de contingencia y de las políticas de continuidad de negocio que aborda aquellas contingencias que por su gravedad no permiten continuar prestando los servicios de OPERBES S.A. DE C.V. en cualquiera de sus edificios y debe continuarse los servicios desde un nuevo edificio. Este plan debe contemplar la vuelta atrás cuando, tras arreglar las consecuencias del desastre, los servicios puedan ser reanudados en el centro local.

Políticas de Impacto al Negocio:

La Política de Impacto al Negocio es mantener un documento que ayude a entender el impacto que un desastre pueda tener sobre un negocio en particular. Contempla dos objetivos fundamentales:

Proporciona la Prioridad a los Procesos Críticos del Negocio.

Se establece el tiempo máximo sin servicio que OPERBES S.A. DE C.V. puede soportar y seguir siendo una compañía que cumpla con sus objetivos de negocio.

Plan de Continuidad, Contingencia, Protección y Restablecimiento Rutas de Servicios y Protección en Anillo

Objetivo

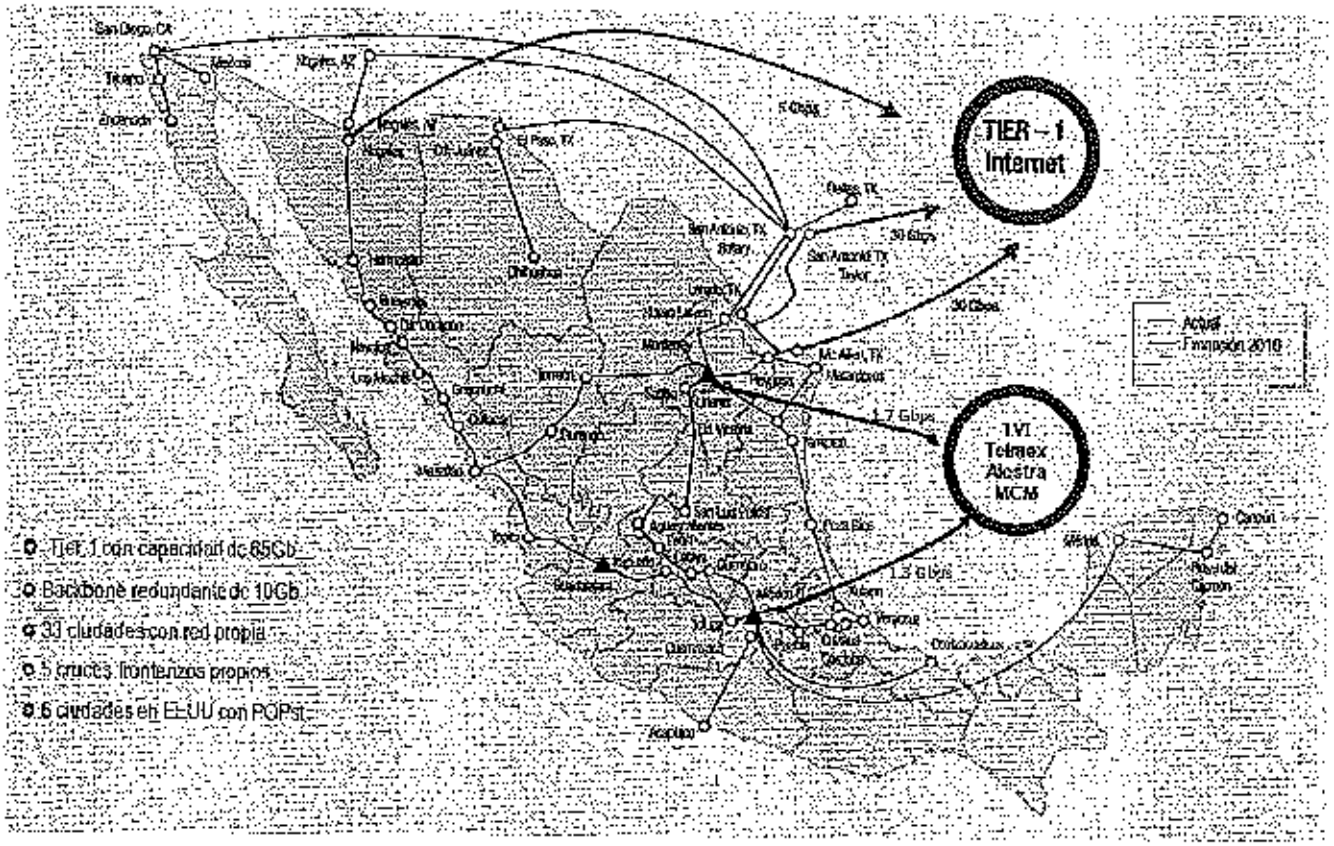
El presente documento establece las generalidades sobre las cuales se basó el diseño del Plan de Desastres para Protección y Restablecimiento de Servicios en la Red de OPERBES S.A. DE C.V. y que abarca diversos aspectos como son topología de la red de transporte, tanto en planta externa, como en equipos DWDM y SDH.

Generalidades

La Red de Terrestre de OPERBES S.A. DE C.V. consta de una infraestructura principal o "Backbone" de Fibra Óptica con capacidad de 60 fibras ópticas corriendo en el Derecho de Vía del FFCC y 72 fibras en el Derecho de Vía de la red eléctrica de la CFE, a través de las cuales OPERBES S.A. DE C.V. brinda su servicio.

La red contempla nodos de acceso y regeneración los cuales integran dos anillos (uno Norte y otro Sur). Por medio de estos se cuenta con acceso a ciudades principales tales como: México, Toluca, Irapuato, Guadalajara, Tepic, Mazatlán, Durango, Torreón, Monterrey, Saltillo, San Luis Potosí, Aguascalientes, León, Celaya, Querétaro, e inclusive en los EE.UU., en Laredo, San Antonio y Mc Allen, entre otros.

El esquemático de físico y geográfico de la red es la siguiente:



Red de Fibra Óptica de Transmisión de BackBone OPERBES S.A. DE C.V.

Descripción

La protección de las rutas del BackBone de OPERBES S.A. DE C.V. se ha diseñado en varios niveles, sin embargo se centran principalmente en una configuración de anillo, en donde los niveles antes mencionados son:

Redundancia de ruta (fibra óptica).
Redundancia en vías lógicas equipo de transporte DWDM
Protección de anillo en equipo de transporte SDH
Protección de tarjetas críticas en equipo SDH.

Redundancia de Ruta de Fibra.

La redundancia de ruta se realiza para tener una trayectoria alterna para ser utilizada en la protección del tráfico en caso de una afectación o desastre debido a causas naturales o provocadas.

Generalmente las rutas son independientes, sin embargo en el caso de la ruta Laredo a San Antonio se aplica un criterio distinto.

Para el BackBone de OPERBES S.A. DE C.V. se han formado 2 anillos: el Anillo Norte y el Anillo Sur.

El anillo Norte consta de:

Monterrey, Candela, Nuevo Laredo, Laredo, Artesia, Moore, San Antonio Rotary, San Antonio Taylor, Mirando, San Isidro, Hidalgo, Mc Allen, Reynosa y General Bravo.

El Anillo Sur consta de:

Monterrey, Saltillo, Salado, Laguna Seca, San Luis Potosí, Salinas, Aguascalientes, León, Celaya, Querétaro, Nopala, México, Toluca, Salvatierra, Irapuato, Yurecuaro, Guadalajara, San José de Gracia, Tepic, Ruiz, Escuinapa, Mazatlán, Las Adjuntas, Durango, Yerbaniz, Torreón, Talia, Sauceda.

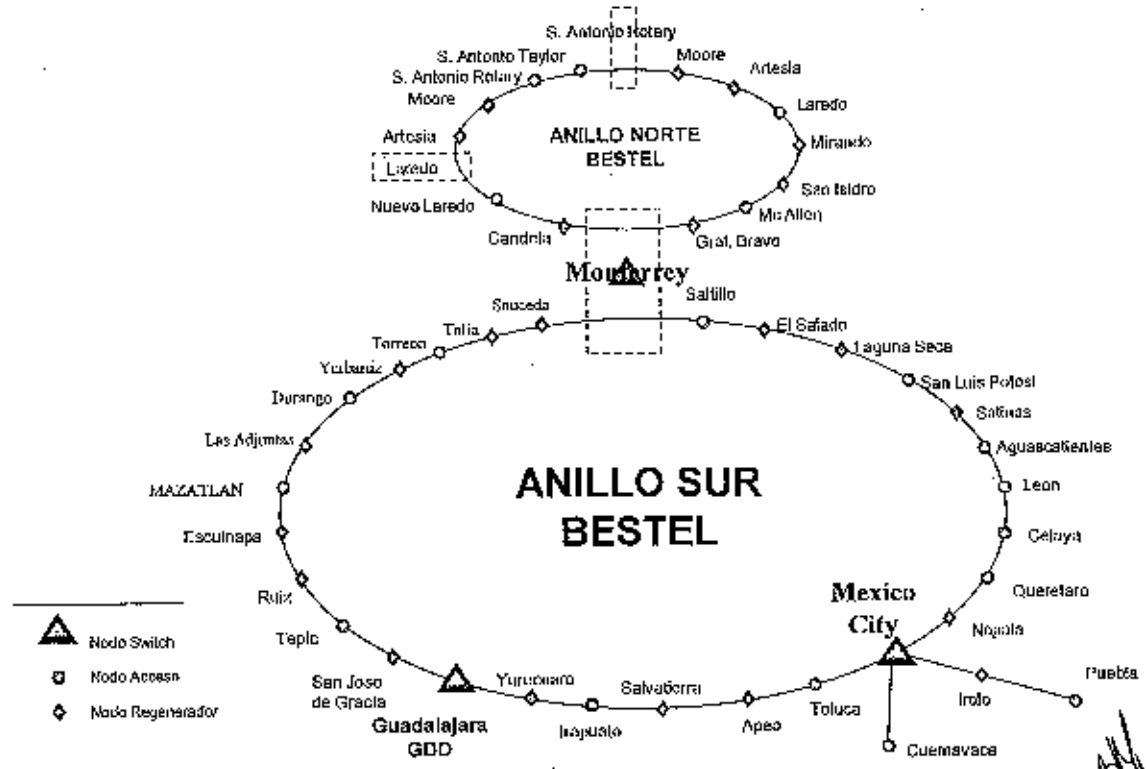
A continuación se presentan esquemas lógicos para facilitar la comprensión de la protección ya que sobre una misma ruta física se pueden utilizar diferentes fibras para formar el anillo.

En la figura de abajo se presenta el esquemático de rutas lógicas de los anillos del BackBone.

Cabe mencionar que la ruta marcada entre nodos se refiere a que existe un par de fibras conectando dichos nodos. En el caso del anillo Norte se presenta el nodo de Laredo, Artesia, Moore y Rotary duplicados ya que se utilizan fibras independientes en una misma ruta física para conectar a los nodos.

Por otra parte en Artesia y Moore se tienen fibras y equipo independientes para cada trayecto, mientras en Laredo y Rotary en un caso la fibra independiente pasa el nodo sin tocar ningún equipo (by-pass) y en el otro, las fibras pasan el nodo tocando equipos.

RUTAS LOGICAS BACKBONE BESTEL



Anillos OPERBES S.A. DE C.V. (Esquemático lógico)

Redundancia en vías lógicas DWDM

Sobre la Red de fibra óptica de transmisión de OPERBES S.A. DE C.V. se ha instalado equipo DWDM, el cual, permite con un par de fibras establecer hasta 96 vías o canales lógicos que pueden ser usados para transportar y/o proteger el tráfico. Este equipo se ha configurado para disponer de vías lógicas a lo largo del anillo y así, asegurar la redundancia de ruta.

La protección de tráfico no se realiza en el DWDM, ya que la funcionalidad de la protección la soporta y es una función natural del equipo SDH.

El equipo DWDM soporta, como ya se mencionó, hasta 96 canales (vías) o mas dependiendo de su equipamiento.

La configuración instalada en el BackBone contempla la operación de una cantidad importante de canales o lambdas en ambos anillos lo cual facilita la construcción de la redundancia en ambas direcciones.

Dos ventajas adicionales del DWDM son:

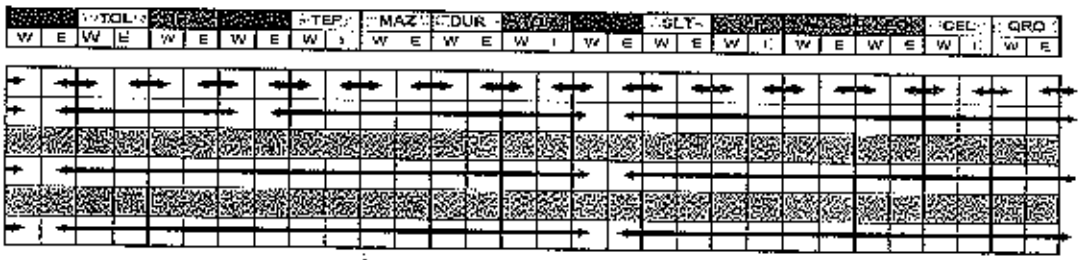
La eliminación de equipos regeneradores SDH, ya que el DWDM tiene la capacidad de incorporar tarjetas regeneradoras en su plataforma.

La eliminación del cálculo de presupuesto óptico en los equipos SDH, dando en consecuencia la utilización de tarjetas de Agregados de Línea de menor potencia.

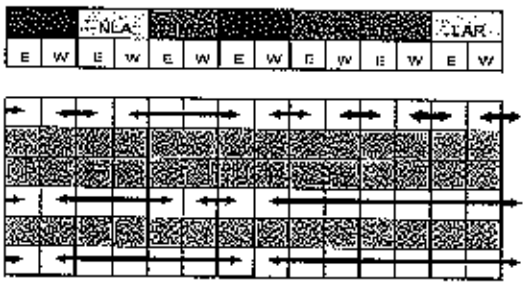
La Configuración de canales en DWDM se ha diseñado como sigue:

ENLACES DE CANALES 2.5Gbps DWDM

ANILLO SUR



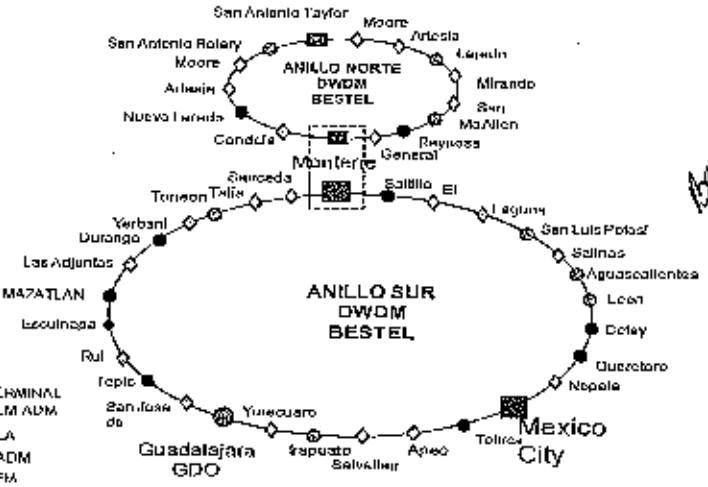
ANILLO NORTE



TERMINAL
LEM AD
OADM

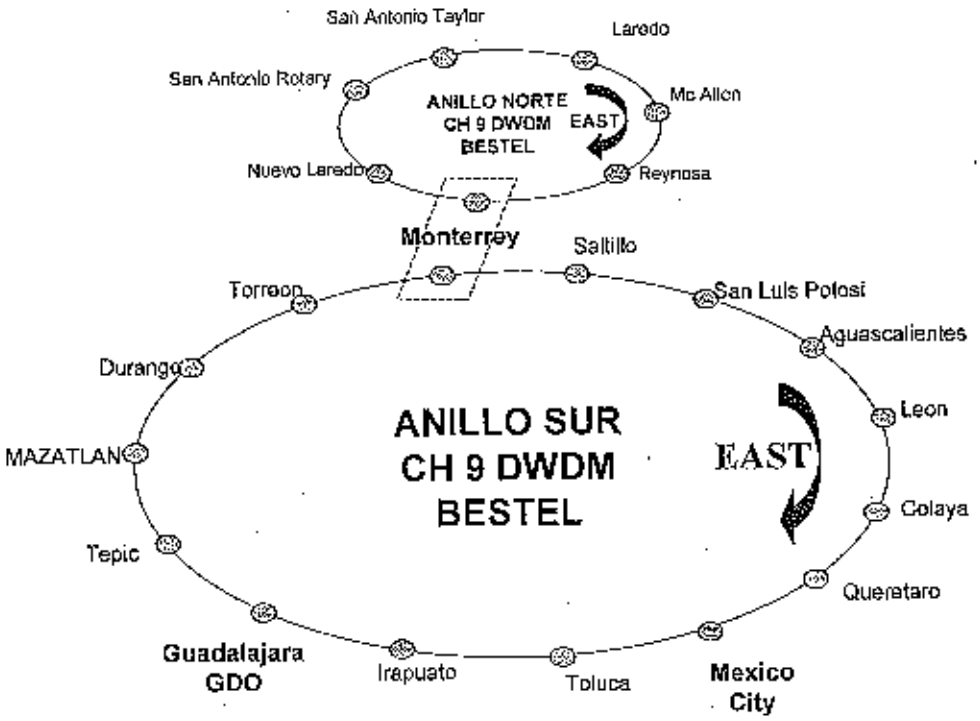
Configuración de Canales DWDM

ANILLOS DWDM BESTEL

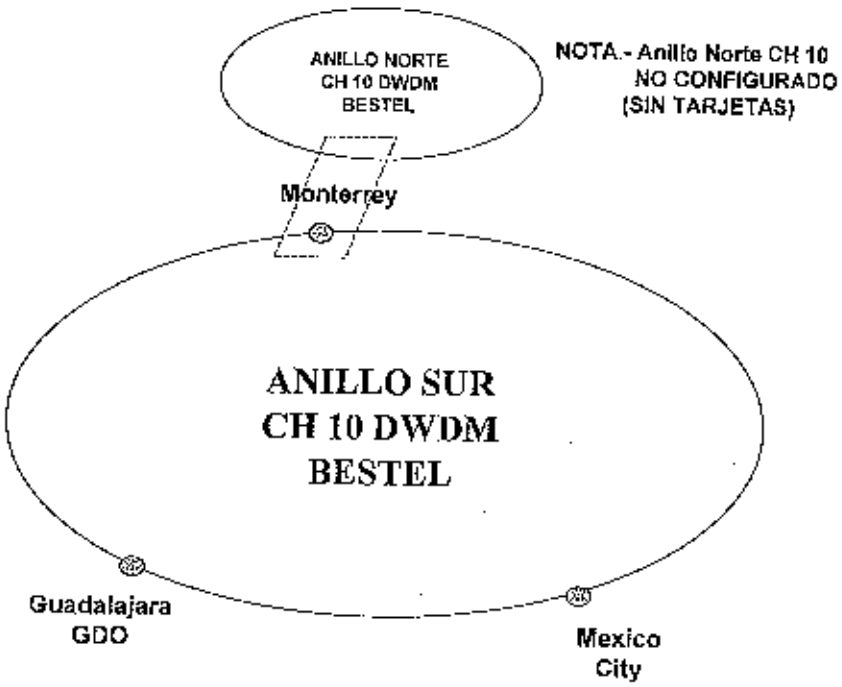


Gráficamente y a manera de ejemplo los nodos del Anillo Norte y Sur, se presentan en la siguiente figura:

NODOS ANILLOS CH 9 DWDM BESTEL



NODOS ANILLOS CH 10 DWDM BESTEL



Cabe mencionar que para cada Nodo de los anillos se dispone de una capacidad a nivel STM-16, la cual será provista con un equipo SDH.

Protección de Anillo en Equipo SDH.

La funcionalidad de protección de anillo proporciona la utilización de la redundancia lógica y física de la red, con una rapidez de protección en MS-SPRING de 50 a 300ms, y en SNCP de 50ms.

La diferencia entre la protección MS-SPRING a SNCP se centra principalmente en el ancho de banda utilizable en el anillo y en el tiempo de protección real del tráfico.

Protección SNC (Sub Network Connection)

Un anillo protegido SNCP solo permite utilizar, en equipos STM-16, hasta un máximo de 16 STM-1 protegidos, ya que él tráfico utiliza el trayecto físico y lógico de trabajo y de redundancia al mismo tiempo.

Su tiempo de protección es el tiempo de conmutación del equipo, típicamente 50ms.

Los equipos terminales de los servicios son los que conmutan, ya que los demás de antemano están configurados para manejar la información en ambas vías.

La topología del anillo se llama Unidireccional (aunque los enlaces sean bidireccionales).

Protección MS-SPRING (Multiplex Section Share Protection RING)

En un anillo protegido MS-SPRING el ancho de banda es mayor, ya que como no se manda la señal en ambas direcciones del anillo, se puede utilizar la ruta de protección para trabajo.

La protección entonces es compartida a nivel STM-1, de los 16, 8 son de trabajo y 8 son de protección. Esto al contrario de disminuir la capacidad del anillo, permite, en equipos STM-16, hasta un máximo de 8 STM-1 X No de Nodos en el anillo, considerando que todo el tráfico va entre nodos contiguos.

El precio de ésta protección es el tiempo de protección de los enlaces, ya que el trayecto de redundancia física y lógica no se utiliza hasta que llegue un criterio de protección. Es hasta entonces que los equipos automáticamente se configuran para proteger el tráfico afectado.

El tiempo de conmutación de un equipo es de 50 ms, sin embargo, cada uno de los equipos en el anillo debe autoconfigurarse para permitir la protección.

El comando para indicar la autoconfiguración es insertado en el encabezado de la siguiente trama SDH (125ms por trama) a ser transmitida al siguiente nodo, más el tiempo de propagación.

La topología del anillo se llama Bidireccional.

Las fallas que cubren ambas protecciones son:

Fibra

Corte de fibra en un punto, todo él tráfico se protege.

Corte de fibra en dos puntos, el tráfico que cruza los puntos de corte se pierde, sin embargo, el que no lo cruza queda trabajando.

Se protegen la Tarjeta de Agregado de Línea, debido a que el daño de una tarjeta de este tipo representa en gran parte una similitud al corte de fibra o degradación de señal, la protección de anillo cubre esta falla.

Para la implementación del equipo SDH se ha definido la tecnología de equipo SDH, sobre los nodos de los anillos Norte y Sur del equipo DWDM.

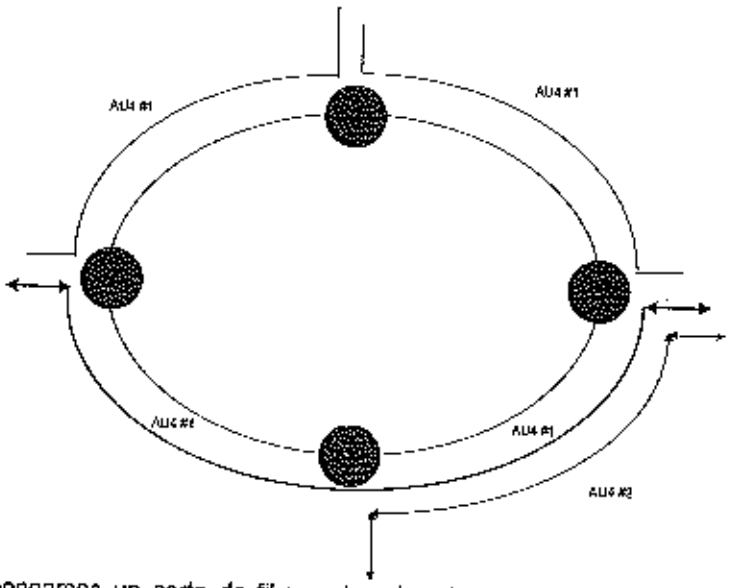
La red de OPERBES S.A. DE C.V. se ha implementado utilizando la protección MS-SPRING.

El funcionamiento de la protección MS-SPRING es el siguiente:

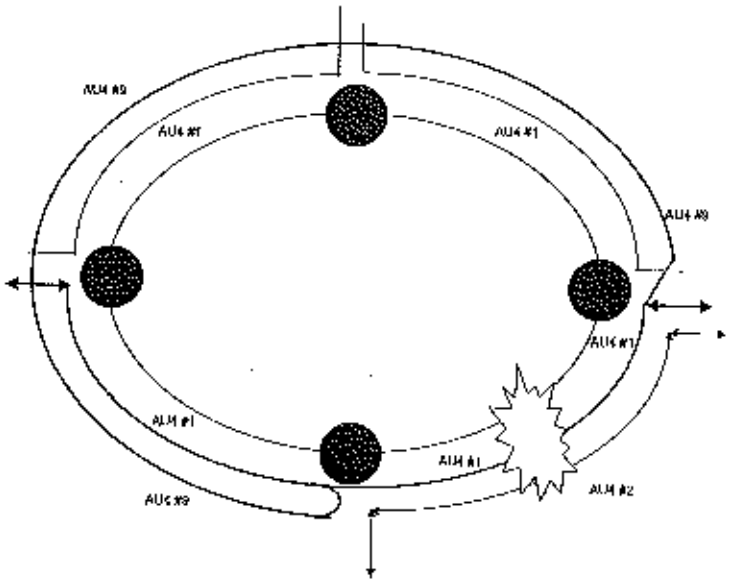
Considere un anillo con 4 nodos.

Considere que se tienen servicios entre nodos 2-3, 3-4, 1-2 y 2-4.

Debido a que la topología del anillo es bidireccional y que se usan 8 AU4 de trabajo y 8 de protección, en cada una de las tarjetas agregados de línea considere que los servicios 2-3, 3-4 y 2-4 van en el AU4#1, mientras el 1-2 va por el AU4#2.



Supongamos un corte de fibra entre el nodo 1 y 4. Los servicios que no atraviesan la ruta abierta no se ven afectados, sin embargo los servicios que si, se conmutan a su respectivo AU4 del 9 al 16. La conmutación se realiza en los equipos inmediatamente involucrados en el corte, mas no en los que suben y bajan el tráfico. En éste caso, el servicio que va del nodo 2-4 sobre el AU4#1 conmuta al AU4#9 en equipos de los nodos 1 y 4 y, retorna por todo el anillo para llegar al equipo del nodo 4.



El servicio del nodo 1-4 que va sobre el AU4#2 conmuta al AU4#10. Los servicios protegidos dan la vuelta a todo el anillo, en este caso del nodo 1 se retornan pasando a través de los nodos 2 y 3, usando el AU4#10 hasta llegar al nodo 4, que lo conmuta al AU4 #2 y de ahí baja el tráfico.

Cabe mencionar que en la protección, aparte de la conmutación del tráfico en los nodos directamente afectados por el corte, todos los equipos de los nodos del anillo se autoconfiguran para dar