

CONTRATO DE PRESTACIÓN DE SERVICIOS QUE CELEBRAN, POR UNA PARTE, EL EJECUTIVO FEDERAL, A TRAVÉS DE LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL, REPRESENTADA POR EL LIC. NICÉFORO GUERRERO REYNOSO, EN SU CARÁCTER DE OFICIAL MAYOR DEL RAMO; LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO, REPRESENTADA POR EL MTRO. LUIS RIVERA MONTES DE OCA Y EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO, REPRESENTADO POR EL LIC. GUSTAVO JÁUREGUI AGUILAR, EN SU CARÁCTER DE DIRECTOR GENERAL, A QUIENES EN LO SUCESIVO SE LES DENOMINARÁ COMO “LA SECRETARÍA”, “LA PROFEDET”, Y “CONAMPROS” RESPECTIVAMENTE Y POR LA OTRA, AXTEL, S. A. B. DE C. V. Y AVANTEL, S. DE R. L. DE C. V., REPRESENTADAS POR JORGE VICENTE MARTÍNEZ RENDÓN, EN SU CARÁCTER DE APODERADO GENERAL, A QUIENES EN LO SUCESIVO SE LES DENOMINARÁ COMO LOS “PRESTADORES DEL SERVICIO” Y LAS “PARTES” CUANDO SE REFIERA A TODAS EN SU CONJUNTO, RESPECTIVAMENTE, DE CONFORMIDAD CON LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

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

I. LA “SECRETARÍA” DECLARA QUE:

- I.1 Es una Dependencia de la Administración Pública Federal Centralizada, de conformidad con lo dispuesto en los artículos 2º, 26 y 40 de la Ley Orgánica de la Administración Pública Federal.
- I.2 El Lic. Nicéforo Guerrero Reynoso, Oficial Mayor del Ramo, cuenta con facultades para suscribir el presente contrato, de conformidad con lo dispuesto en el artículo 8 fracción XXIII del Reglamento Interior de la Secretaría del Trabajo y Previsión Social, publicado en el Diario Oficial de la Federación el 14 de noviembre del 2008.
- I.3 Requiere contratar de manera consolidada el “Servicio de Red Nacional de Servicios Integrales Administrados de voz, datos, internet y videoconferencia, para la Secretaría del Trabajo y Previsión Social (STPS), la Procuraduría Federal de la Defensa del Trabajo (PROFEDET), la Coordinación General del Servicio Nacional de Empleo (CGSNE), y el Comité Nacional Mixto de Protección al Salario (CONAMPROS)”.
- I.4 La erogación correspondiente al presente contrato se encuentra comprendida en la partida presupuestal número 31602 “Servicios de telecomunicaciones”, del Clasificador por Objeto del Gasto para la Administración Pública Federal. La “SECRETARÍA”, cuenta con los recursos presupuestales suficientes para cubrir el importe de los servicios, según se desprende del oficio número 511/01.-2013/986 de fecha 27 de agosto de 2013, emitido por el Dirección General de Programación y Presupuesto de la “SECRETARÍA”.
- I.5 La “SECRETARÍA”, cuenta con la autorización para comprometer recursos de los ejercicios 2013 a 2017, y contratar los servicios objeto del presente instrumento, de

conformidad con la autorización número 2013-14-513-154 de fecha 27 de agosto de 2013, emitida por el Módulo de Administración y Seguimiento de Contratos Plurianuales, de la Dirección General de Programación y Presupuesto de la “SECRETARÍA”.

- I.6 El presente instrumento se adjudicó mediante el procedimiento de adjudicación directa, con fundamento en la fracción VII y penúltimo párrafo del artículo 41 y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
- I.7 Su Registro Federal de Contribuyentes es STP 401231 P53, como lo acredita con la copia de su Cédula de Identificación Fiscal.
- I.8 Requiere a los “PRESTADORES DEL SERVICIO” su afiliación al “Programa de Cadenas Productivas” a que se refiere el artículo 18 del Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2013.
- I.9 Para los efectos legales de este contrato, señala como su domicilio el ubicado en Avenida Anillo Periférico Sur número 4271, colonia Fuentes del Pedregal, Delegación Tlalpan, C. P. 14140, en la Ciudad de México, Distrito Federal.

II. “LA PROFEDET” DECLARA QUE:

- II.1 Es un órgano desconcentrado de la “Secretaría”, de conformidad con lo dispuesto por los artículos 17 y 40, fracción XII de la Ley Orgánica de la Administración Pública Federal; 35, 36, fracción I y 37 del Reglamento Interior de la “SECRETARÍA” y 3 del Reglamento de la Procuraduría Federal de la Defensa del Trabajo.
- II.2 Comparece en este acto el Mtro. Luis Rivera Montes de Oca, en su carácter de Procurador General de la “PROFEDET”, quien tiene facultades para celebrar el presente contrato, con fundamento en lo dispuesto por los artículos 38, fracción VII del Reglamento Interior de la Secretaría del Trabajo y Previsión Social y 12, fracción XVI del Reglamento de la Procuraduría Federal de la Defensa del Trabajo.
- II.3 Requiere contratar de manera consolidada el “Servicio de Red Nacional de Servicios Integrales Administrados de voz, datos, internet y videoconferencia, para la Secretaría del Trabajo y Previsión Social (STPS), la Procuraduría Federal de la Defensa del Trabajo (PROFEDET), la Coordinación General del Servicio Nacional de Empleo (CGSNE), y el Comité Nacional Mixto de Protección al Salario (CONAMPROS)”.
- II.4 Cuenta con los recursos presupuestales suficientes para cubrir el importe de los servicios, según se desprende del oficio número 511/01.-2013/986 de fecha 27 de agosto de 2013, emitido por el Dirección General de Programación y Presupuesto de la “Secretaría”.

II.5 Para los efectos legales del presente contrato, señala como domicilio el ubicado en la Calle de Doctor José María Vértiz número 211, Colonia Doctores, Delegación Cuauhtémoc, C.P. 06720, en la Ciudad de México, Distrito Federal.

III. “LA CONAMPROS” declara que:

III.1 Es un órgano administrativo desconcentrado de la Secretaría del Trabajo y Previsión Social de conformidad con el “DECRETO por el que se crea el Comité Nacional Mixto de Protección al Salario”, publicado en el Diario Oficial de la Federación el 31 de octubre de 2006.

III.2 El Lic. Gustavo Jáuregui Aguilar, Director General del CONAMPROS, cuenta con facultades para suscribir el presente contrato de conformidad con el Artículo Octavo del “DECRETO por el que se crea el Comité Nacional Mixto de Protección al Salario, como órgano administrativo desconcentrado de la Secretaría del Trabajo y Previsión Social”.

III.3 Requiere contratar de manera consolidada el “Servicio de Red Nacional de Servicios Integrales Administrados de voz, datos, internet y videoconferencia, para la Secretaría del Trabajo y Previsión Social (STPS), la Procuraduría Federal de la Defensa del Trabajo (PROFEDET), la Coordinación General del Servicio Nacional de Empleo (CGSNE), y el Comité Nacional Mixto de Protección al Salario (CONAMPROS)”.

III.4 Cuenta con los recursos presupuestales suficientes para cubrir el importe de los servicios, según se desprende del oficio número 511/01.-2013/986 de fecha 27 de agosto de 2013, emitido por el Dirección General de Programación y Presupuesto de la “Secretaría”.

III.5 Su Registro Federal de Contribuyentes es CNM-740403HX5, en términos de la Cédula de Identificación Fiscal.

III.6 Para los efectos legales del presente contrato señala como su domicilio el ubicado en Avenida Ricardo Flores Magón 44, Piso 3, Col. Guerrero, Delegación Cuauhtémoc, México D. F., C.P. 06300, en la Ciudad de México, Distrito Federal.

IV DECLARA “AXTEL, S. A. B. DE C. V.” QUE:

- IV.1 *Eliminado un párrafo con seis renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley.*

Eliminado un párrafo con ocho renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley.

Eliminado un párrafo con cinco renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley..

- IV.2 *Eliminado un párrafo con diez renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley..*

- IV.3 *Eliminado un párrafo con dos renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley.*

V.- DECLARA “AVANTEL, S. DE R. L. DE C. V.” QUE:

- V.1 *Eliminado un párrafo con once renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley.*

Eliminado un párrafo con cinco renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley.

Eliminado un párrafo con seis renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley.

V.2. *Eliminado un párrafo con diez renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley..*

V.3. *Eliminado un párrafo con dos renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley.*

VI. AMBAS EMPRESAS DECLARAN QUE:

VI.1 *Eliminado un párrafo con siete renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley.*

VI.2 Tienen la capacidad jurídica para contratar y reúnen las condiciones técnicas y económicas para obligarse a la prestación del servicio objeto del presente contrato; además de contar con los permisos, licencias y autorizaciones necesarias de conformidad con la legislación aplicable, para hacer uso de los bienes y técnicas de que se vale para la prestación del servicio.

VI.3 Manifiestan “bajo protesta de decir verdad” que han cumplido con sus obligaciones en materia de Registro Federal de Contribuyentes y que han presentado en tiempo y forma las declaraciones del ejercicio por impuestos federales, distintas a las del Impuesto Sobre Automóviles Nuevos (ISAN) e Impuesto Sobre Tenencia o Uso de Vehículos (ISTUV), correspondientes a sus dos últimos ejercicios fiscales y que han presentado las declaraciones de pagos mensuales, provisionales o definitivos, correspondientes a los últimos doce meses anteriores a la fecha de firma del presente contrato por los mismos impuestos. Asimismo, no tienen adeudos fiscales firmes a su cargo por impuestos federales, distintos a ISAN e ISTUV.

VI.4 Para los efectos de lo previsto por el artículo 32-D del Código Fiscal de la Federación, se compromete a entregar a la firma del presente instrumento, el acuse que comprueba el inicio del trámite alude la Regla I.2.1.15 de la Resolución Miscelánea Fiscal 2013, publicada en el Diario Oficial de la Federación el 28 de diciembre de 2012.

VI.5 Conocen plenamente el contenido y los requisitos que establecen la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento, el Código Civil Federal y los ordenamientos fiscales vigentes a la fecha de firma del presente contrato.

- VI.6 “Bajo protesta de decir verdad”, su apoderado manifiesta que sus representadas, los socios y accionistas de estos, no se encuentran en alguno de los supuestos previstos en los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
- VI.7 Mediante convenio de participación conjunta celebrado el 19 de diciembre de 2013, Axtel, S.A.B. de C.V. (participante “A”) y Avantel, S. de R.L. de C.V. (participante “B”), manifestaron su conformidad con el objeto de participar conjuntamente en el procedimiento de contratación del “Servicio de Red Nacional de Servicios Integrales Administrados de voz, datos, internet y videoconferencia, para la Secretaría del Trabajo y Previsión Social (STPS), la Procuraduría Federal de la Defensa del Trabajo (PROFEDET), la Coordinación General del Servicio Nacional de Empleo “CGSNE”, y el Comité Nacional Mixto de Protección al Salario (CONAMPROS)”, el cual se adiciona en fotocopia al presente contrato como anexo 2.
- VI.8 *Eliminado un párrafo con tres renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley.*

Expuesto lo anterior, las “PARTES” están de acuerdo en celebrar el presente contrato, sujetándose al contenido de las siguientes:

C L Á U S U L A S

PRIMERA.- OBJETO DEL CONTRATO: La “SECRETARÍA”, la “PROFEDET” y “CONAMPROS”, encomiendan a los “PRESTADORES DEL SERVICIO” y éstos se obligan a prestar el “SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, para la Secretaría del Trabajo y Previsión Social (STPS), la Procuraduría Federal de la Defensa del Trabajo (PROFEDET), la Coordinación General del Servicio Nacional de Empleo ‘CGSNE’, y el Comité Nacional Mixto de Protección al Salario (CONAMPROS)”, apegándose justa, exacta y cabalmente a las cantidades, términos y condiciones estipulados en el Anexo 1, el que debidamente firmado por las “PARTES”, forma parte integrante del presente instrumento.

SEGUNDA.- VIGENCIA: Las “PARTES” aceptan que la vigencia del presente contrato será del 23 de diciembre de 2013 y hasta el 22 de diciembre de 2017; el plazo señalado en la presente cláusula será forzoso para los “PRESTADORES DEL SERVICIO” y voluntario para la “SECRETARÍA”, la “PROFEDET” y “CONAMPROS”.

TERCERA.- MONTO DEL CONTRATO: El monto mínimo disponible para cubrir los gastos que genere el presente contrato es por la cantidad de **\$196,230,410.40 (CIENTO NOVENTA Y SEIS MILLONES DOSCIENTOS TREINTA MIL CUATROCIENTOS DIEZ PESOS 40/100 M. N.)**, y el monto máximo asciende a la cantidad de **\$490’576,026.00 (CUATROCIENTOS**

NOVENTA MILLONES QUINIENTOS SETENTA Y SEIS MIL VEINTISEIS PESOS 00/100 M. N.). Dichos montos incluyen el correspondiente Impuesto al Valor Agregado (IVA) y el 3% del Impuesto Especial sobre Productos y Servicios.

ORG	MONTO	2013	2014	2015	2016	2017	TOTAL
STPS	MÁXIMO	\$300,000.00	\$97,948,940.00	\$130,948,940.00	\$130,949,940.00	\$111,348,510.00	\$471,496,330.00
	MÍNIMO	\$120,000.00	\$39,179,576.00	\$52,379,576.00	\$52,379,976.00	\$44,539,404.00	\$188,598,532.00
PROFEDET	MÁXIMO	\$30,000.00	\$2,051,060.00	\$7,051,060.00	\$6,050,060.00	\$3,897,516.00	\$19,079,696.00
	MÍNIMO	\$12,000.00	\$820,424.00	\$2,820,424.00	\$2,420,024.00	\$1,559,006.40	\$7,631,878.40

Nota: el presupuesto para CGSNE, PROFEDET Y CONAMPROS se encuentran incluidos en la autorización plurianual de la "Secretaría".

Los compromisos que se generen para los ejercicios presupuestales de 2014, 2015, 2016 y 2017, quedarán sujetos para efectos de ejecución y pago a las disponibilidades del Presupuesto de Egresos de la Federación que apruebe la H. Cámara de Diputados y el oficio de liberación del presupuesto que emita la Secretaría de Hacienda y Crédito Público, para cada ejercicio fiscal correspondiente.

Asimismo, no habrá penalización para la "SECRETARÍA", la "PROFEDET" y "CONAMPROS", de ningún tipo, en caso de que ocurran variaciones en el presupuesto que apruebe la H. Cámara de Diputados para los ejercicios fiscales de 2014, 2015, 2016 y 2017.

La "SECRETARÍA", la "PROFEDET" y "CONAMPROS" no pagarán comisiones por ningún concepto, ni otorgará anticipo alguno a los "PRESTADORES DEL SERVICIO".

Dichos montos incluyen la remuneración o pago total a los "PRESTADORES DEL SERVICIO", por todos los gastos directos e indirectos que origine el presente contrato, la utilidad y en su caso, el costo de obligaciones adicionales.

Las "PARTES" convienen que durante la vigencia del presente contrato los costos unitarios ofertados por los "PRESTADORES DEL SERVICIO" se mantendrán fijos. Asimismo, los precios unitarios se indican en el Anexo 1 del presente instrumento.

CUARTA.- FORMA, LUGAR, TÉRMINOS Y CONDICIONES DE PRESTAR EL SERVICIO:

Los "PRESTADORES DEL SERVICIO" se obligan a prestar los servicios a que se refiere la cláusula Primera, en la forma, lugar, términos y condiciones descritos en el Anexo 1, el cual firmado por las "PARTES" forma parte integrante del presente contrato, la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" podrán realizar a través de órdenes de surtimiento, requerimientos adicionales a los "PRESTADORES DEL SERVICIO".

QUINTA.- FORMA Y LUGAR DE PAGO: La "SECRETARÍA", la "PROFEDET" y "CONAMPROS" pagarán el monto a que se refiere la cláusula Tercera, en moneda nacional, mediante la formulación de facturas debidamente requisitadas y aceptadas por la Dirección General de Programación y Presupuesto, las cuales abarcarán periodos mensuales vencidos.

Los "PRESTADORES DEL SERVICIO" deberán entregar tres (3) facturas con los requisitos fiscales que establece la legislación vigente en la materia; dichas facturas deberán presentarse conforme a lo siguiente: una factura para la "SECRETARÍA" la cual deberá incluir los servicios

prestados a la misma, y ser remitida a la Dirección General de Tecnologías de la Información ubicada en Félix Cuevas No. 301, Piso 4, Colonia del Valle, Del. Benito Juárez, Código Postal 03100, México, Distrito Federal; otra factura en la que se incluyan los servicios prestados al "CONAMPROS", misma que deberá ser remitida a la Dirección General del citado Organismo, ubicado en Avenida Ricardo Flores Magón 44, Piso 3, Col. Guerrero, Delegación Cuauhtémoc, México D. F., C.P. 06300; y la tercer factura deberá incluir los servicios prestados a la "PROFEDET" y deberá ser remitida al titular de la "PROFEDET", ubicada en Doctor José María Vertiz número 211, Colonia Doctores, Delegación Cuauhtémoc, C.P. 06720, en la Ciudad de México, Distrito Federal.

En caso de que se detecten en las facturas errores o deficiencias de forma o fondo imputables a los "PRESTADORES DEL SERVICIO" o bien se presenten sin la validación de los servicios que amparan, dentro de los tres días hábiles siguientes al de su recepción, la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" indicarán por escrito a los "PRESTADORES DEL SERVICIO" las deficiencias que deberán corregir. Para efectos de la validación en comento, los "PRESTADORES DEL SERVICIO" deberán entregar a la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" la relación de los servicios proporcionados previo a la presentación de la factura, en todos los casos en un horario de 9:00 a 14:00 horas en días hábiles.

Eliminado un párrafo con seis renglones, con fundamento legal en términos de la fracción I del artículo 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por contener datos personales protegidos para su difusión, distribución o comercialización por la citada Ley.

En caso de que los datos indicados en el párrafo anterior sean equivocados, los "PRESTADORES DEL SERVICIO" asumirán las pérdidas que se deriven de esta situación.

Los pagos que haga la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" cubren los servicios, organización, dirección, administración y técnica propia, impuestos, derechos o cualquier contraprestación a favor de los "PRESTADORES DEL SERVICIO" que se generen con motivo de la celebración o cumplimiento del presente contrato, por lo que estos últimos no podrán reclamar algún otro pago adicional.

SEXTA.- PAGOS EN EXCESO: Tratándose de pagos en exceso que reciban los "PRESTADORES DEL SERVICIO", deberán reintegrar las cantidades pagadas en exceso en términos del artículo 51 de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público, más los intereses generados a la tasa que señale la Ley de Ingresos de la Federación, para los casos de prórrogas de créditos fiscales, que se calcularán sobre el monto pagado de más, computándose por días calendario desde la fecha en que se realizó el pago en exceso de los servicios, hasta aquélla en que se pongan efectivamente las cantidades a disposición de la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" y, en su caso, podrá hacerse efectiva la garantía de cumplimiento del contrato.

SÉPTIMA.- PAGO DE IMPUESTOS: Será responsabilidad y a cargo de las "PARTES" el pago de impuestos y derechos que les corresponda a cada una de ellas, conforme a la normatividad vigente, y que se generen con motivo del presente contrato.

OCTAVA.- RELACIONES LABORALES: Los "PRESTADORES DEL SERVICIO" como patronos del personal que ocupen con motivo de la prestación del servicio materia del

presente contrato, manifiestan que cuentan con los elementos propios y suficientes para responsabilizarse de las obligaciones derivadas de las relaciones de trabajo. En consecuencia, serán los únicos responsables, en relación con sus trabajadores, de las obligaciones derivadas de las disposiciones legales y demás ordenamientos en materia de trabajo y de seguridad social, obligándose por tanto a responder de todas las reclamaciones que sus trabajadores presentaren en su contra o en contra de la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" en relación con los servicios materia del presente contrato, obligándose a sacar en paz y a salvo a éstas, en caso de que surja algún conflicto laboral. La "SECRETARÍA", la "PROFEDET" y "CONAMPROS" en ningún caso tendrá el carácter de patrón sustituto o solidario de los trabajadores de los "PRESTADORES DEL SERVICIO".

NOVENA.- CESIÓN DE DERECHOS Y OBLIGACIONES: Los "PRESTADORES DEL SERVICIO" no podrán ceder en forma parcial ni total a favor de otra persona, los derechos y obligaciones que se deriven del presente contrato, salvo los derechos de cobro que podrá ceder, previa autorización por escrito de la "SECRETARÍA", la "PROFEDET" y "CONAMPROS", en términos del artículo 46 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

DÉCIMA.- SUPERVISIÓN Y VERIFICACIÓN: La "SECRETARÍA", la "PROFEDET" o "CONAMPROS" tienen el derecho de supervisar en todo momento y cuando así lo juzguen conveniente, el desarrollo y cumplimiento de los servicios contratados con los "PRESTADORES DEL SERVICIO".

La supervisión y verificación a que se refiere el párrafo anterior la podrá hacer la "SECRETARÍA", la "PROFEDET" o "CONAMPROS" a través del servidor o servidores públicos que al efecto designe.

Los "PRESTADORES DEL SERVICIO" se obligan a dar todas las facilidades al servidor público o servidores públicos que al efecto designen la "SECRETARÍA", la "PROFEDET" o el "CONAMPROS", para que se lleve a cabo la supervisión y verificación.

Los "PRESTADORES DEL SERVICIO" se obligan a subsanar todas las deficiencias detectadas por la "SECRETARÍA", la "PROFEDET" o el "CONAMPROS", en un plazo no mayor de 3 días hábiles, contados a partir de la fecha de notificación que por escrito le hagan "SECRETARÍA", la "PROFEDET" o el "CONAMPROS" a los "PRESTADORES DEL SERVICIO", en el domicilio señalado para los efectos del presente contrato.

DÉCIMA PRIMERA.- REPOSICIÓN DE LOS SERVICIOS: La "SECRETARÍA", la "PROFEDET" y "CONAMPROS" solicitarán a los "PRESTADORES DEL SERVICIO" la reposición de los servicios objeto del presente contrato y descritos en el Anexo 1, cuando éstos no cumplan con la calidad, condiciones, términos y especificaciones solicitados en el mismo.

En dicho caso, los "PRESTADORES DEL SERVICIO" se obligan a reponer a la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" sin condición y sin costo, los servicios que no cumplan con la calidad y especificaciones originalmente convenidas, en un plazo máximo de tres días hábiles a partir de la notificación que para tal efecto realice la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" en el domicilio señalado para los efectos del presente contrato, mismo que no lo exime de la sanción por cada día de atraso en el cumplimiento.

DÉCIMA SEGUNDA.- CASO FORTUITO O FUERZA MAYOR: Ninguna de las “PARTES” serán responsables del incumplimiento de este Contrato que resulte de caso fortuito o fuerza mayor, por lo que en el caso de que la “SECRETARÍA”, la “PROFEDET” y “CONAMPROS” suspendan la prestación del servicio, únicamente se pagarán aquéllos que hubiesen sido efectivamente prestados y en su caso, se reintegrarán los anticipos no amortizados, lo anterior con apoyo en lo dispuesto en el primer párrafo del artículo 55-Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en relación con el artículo 102 de su Reglamento.

DÉCIMA TERCERA.- SUSPENSIÓN TEMPORAL DEL CONTRATO: La “SECRETARÍA”, la “PROFEDET” y “CONAMPROS” podrán suspender en cualquier momento y de manera temporal, en todo o en parte, la prestación del servicio contratado, sin que ello implique su terminación definitiva. Al efecto, notificarán a los “PRESTADORES DEL SERVICIO” en el domicilio señalado para los efectos del presente contrato, un aviso por escrito, en el que indicarán las causas de suspensión. Dicho aviso surtirá sus efectos a los diez días naturales siguientes a su notificación. El presente contrato podrá continuar produciendo sus efectos legales una vez que hayan desaparecido las causas que motivaron dicha suspensión, lo que hará saber la “SECRETARÍA”, la “PROFEDET” o el “CONAMPROS” a los “PRESTADORES DEL SERVICIO” en los mismos términos que le hizo saber de la suspensión, dentro de los tres días hábiles siguientes a que haya desaparecido la causa de ésta.

DÉCIMA CUARTA.- TERMINACIÓN ANTICIPADA: La “SECRETARÍA”, la “PROFEDET” y “CONAMPROS” podrán dar por terminado anticipadamente el contrato sin responsabilidad alguna a su cargo, en términos del artículo 54 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, cuando por causas justificadas se extinga la necesidad de requerir el servicio originalmente contratado, o se determine la nulidad total o parcial de los actos que dieron origen al contrato, con motivo de la resolución de una inconformidad emitida por la Secretaría de la Función Pública, o cuando concurren razones de interés general; bastando para ello una comunicación por escrito a los “PRESTADORES DEL SERVICIO” que surtirá sus efectos a los 10 días naturales siguientes a su notificación.

DÉCIMA QUINTA.- MODIFICACIONES AL CONTRATO: Durante la vigencia del presente contrato, la “SECRETARÍA”, la “PROFEDET” y “CONAMPROS” podrán modificar el mismo o el contenido del Anexo 1, dando aviso por escrito a los “PRESTADORES DEL SERVICIO”, el cual surtirá sus efectos a los cinco días hábiles siguientes a la notificación realizada en el domicilio señalado para los efectos de este contrato; y éste se obliga a dar cumplimiento a dichas modificaciones. Cualquier modificación al contrato deberá formalizarse por escrito, en términos de lo dispuesto por el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

DÉCIMA SEXTA.- INDEMNIZACIÓN DE LOS “PRESTADORES DEL SERVICIO” A LA “SECRETARÍA”, LA “PROFEDET” Y “CONAMPROS”: Los “PRESTADORES DEL SERVICIO” durante la vigencia de este contrato, como después de su expiración, indemnizarán a la “SECRETARÍA”, la “PROFEDET” y “CONAMPROS” por cualquier daño o perjuicio que resulte o se derive de un acto ilícito, negligencia o violatorio del contrato por parte de los

“PRESTADORES DEL SERVICIO” o de su personal designado para la ejecución del objeto materia del mismo, así como de las acciones, juicios, demandas, costas y reclamaciones que se originen como resultado de dichos actos.

DÉCIMA SÉPTIMA.- GARANTÍA: Los “PRESTADORES DEL SERVICIO” se obligan a garantizar el cumplimiento de las obligaciones derivadas del presente contrato mediante fianza expedida por una institución debidamente autorizada, a favor de la Tesorería de la Federación, por un importe equivalente al 10% (diez por ciento) del monto máximo adjudicado para el ejercicio fiscal de que se trate, sin incluir el Impuesto al Valor Agregado (IVA).

La fianza en cuestión será presentada por el “PRESTADORES DEL SERVICIO” a la “SECRETARÍA” para el ejercicio fiscal 2013, en un plazo no mayor de 10 (diez) días naturales posteriores a la fecha de firma de este contrato y para los ejercicios fiscales de 2014, 2015, 2016 y 2017, dentro de los primeros 10 días naturales de enero de cada uno de dichos años, siendo causa de rescisión el no presentarla.

La garantía continuará vigente en caso de que se otorguen prórrogas al cumplimiento del contrato, así como durante la substanciación de todos los recursos legales o juicios que se interpongan hasta que se pronuncie la resolución definitiva por autoridad competente, de forma tal que su vigencia no podrá acotarse en razón del plazo de ejecución del contrato principal o fuente de las obligaciones o cualquier otra circunstancia.

La “SECRETARÍA” devolverá la fianza a los “PRESTADORES DEL SERVICIO”, una vez cumplidas las obligaciones a su cargo y a entera satisfacción de la “SECRETARÍA”, la “PROFEDET” y “CONAMPROS”, para lo cual la Dirección General de Tecnologías de la Información de la “SECRETARÍA” deberá solicitar a la “PROFEDET” y “CONAMPROS”, su manifestación por escrito en donde hagan constar que los “PRESTADORES DEL SERVICIO” cumplieron con las obligaciones pactadas en el presente contrato.

DÉCIMA OCTAVA.- POLIZA DE RESPONSABILIDAD CIVIL: Los “PRESTADORES DEL SERVICIO” se obligan a presentar a la “SECRETARÍA” una Póliza de Responsabilidad Civil equivalente al 5% del monto máximo total del contrato, misma que deba de estar vigente durante la prestación de los servicios.

La Póliza en cuestión será presentada por el “PRESTADORES DEL SERVICIO” a la “SECRETARÍA”, en un plazo no mayor de 10 (diez) días naturales posteriores a la fecha de firma de este.

DÉCIMA NOVENA.- PENA CONVENCIONAL: La “SECRETARÍA”, la “PROFEDET” o “CONAMPROS” aplicarán a los “PRESTADORES DEL SERVICIO” una pena convencional conforme a lo estipulado en el anexo 1, sin que las penas excedan del 10% (diez por ciento) del monto máximo del contrato, en cuyo caso procederá la rescisión del mismo.

El procedimiento para la aplicación de la pena por atraso será el siguiente: la “SECRETARÍA”, la “PROFEDET” o el “CONAMPROS” notificaran a los “PRESTADORES DEL SERVICIO” por escrito en el domicilio señalado para los efectos del presente contrato, que incurrieron en atraso en la prestación del servicio materia del presente contrato, para que éste en un plazo de tres días hábiles contados a partir de la notificación del escrito, manifieste lo que a su derecho convenga y ofrezca las pruebas que considere pertinentes. La “SECRETARÍA”, la “PROFEDET”

o el "CONAMPROS", valorando, en su caso, el escrito presentado por los "PRESTADORES DEL SERVICIO", determinarán la aplicación o no de la pena convencional. En caso de determinar la aplicación de dicha pena se lo notificará a los "PRESTADORES DEL SERVICIO", quienes en consecuencia deberán efectuar el entero correspondiente en alguna sucursal bancaria a través del formato e-cinco del SAT, debiendo acompañar copia del mismo, previo al trámite de pago.

VIGÉSIMA.- CAUSAS DE RESCISIÓN: Serán causas de rescisión del presente contrato sin ninguna responsabilidad para la "SECRETARÍA", la "PROFEDET" y "CONAMPROS", las que se señalan en forma enunciativa más no limitativa, si los "PRESTADORES DEL SERVICIO":

- a) No inician la prestación de los servicios objeto de este contrato en la fecha pactada, sin perjuicio de lo establecido en la cláusula Décima Novena;
- b) No prestan el servicio de conformidad con lo establecido en el presente contrato y en el Anexo 1, o sin motivo justificado, no acata las indicaciones de la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" para que el servicio sea prestado debida y oportunamente, sin perjuicio de lo establecido en las cláusulas Décima Primera y Décima Novena;
- c) Cancelan o suspenden injustificadamente los servicios objeto del presente contrato;
- d) Por cualquier causa dejan de tener la capacidad técnica y los elementos necesarios para proporcionar el servicio objeto de este contrato;
- e) Ceden a terceras personas los derechos y obligaciones del presente contrato, en forma total o parcial;
- f) Ceden a terceras personas los derechos de cobro derivados del presente contrato, en forma total o parcial, sin el consentimiento previo y por escrito de la "SECRETARÍA", la "PROFEDET" y "CONAMPROS";
- g) No dan a la SECRETARÍA, la "PROFEDET" y "CONAMPROS" las facilidades y datos necesarios para la supervisión y verificación de los servicios objeto de este contrato;
- h) No otorgan a la "SECRETARÍA", la garantía de cumplimiento del contrato, dentro del plazo establecido en la cláusula Décima Séptima de este instrumento;
- i) No presentan a la "SECRETARÍA", la póliza de responsabilidad civil en la forma, términos y plazo establecido en cláusula Décima Octava de este instrumento;
- j) Son declarados en huelga o sujetos a concurso mercantil, en términos de la Ley Federal del Trabajo o de la Ley de Concursos Mercantiles, respectivamente o por cualquier otra causa análoga quedan impedidos para continuar con la prestación del servicio;
- k) Cuando la suma de las penas convencionales excedan el 10% del monto total del contrato; y
- l) En general, por cualquier otro incumplimiento a las obligaciones pactadas en el presente contrato.

VIGÉSIMA PRIMERA.- PROCEDIMIENTO DE RESCISIÓN: La "SECRETARÍA", la "PROFEDET" y "CONAMPROS" podrán rescindir el presente contrato sin necesidad de declaración judicial previa, o bien, exigir su cumplimiento forzoso, en caso de que los "PRESTADORES DEL SERVICIO" incumplan con cualesquiera de las obligaciones estipuladas y/o inherentes a la naturaleza del mismo. Si los "PRESTADORES DEL SERVICIO"

incurren en cualquiera de las causas a que se refiere la cláusula anterior la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" rescindirán el presente contrato. En caso de optar por la rescisión del contrato, se procederá conforme a lo establecido en el artículo 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

VIGÉSIMA SEGUNDA.- CONFIDENCIALIDAD: Los "PRESTADORES DEL SERVICIO" se comprometen a guardar reserva respecto de la información y actividades realizadas para el cumplimiento objeto del presente instrumento jurídico, por lo que detentará toda la información recibida como reservada, por lo que no podrá realizar ningún acto que pudiera afectar los intereses de la "SECRETARÍA", la "PROFEDET" y "CONAMPROS". Sin embargo, la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" se sujetarán en este aspecto a lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

VIGÉSIMA TERCERA.- PATENTES, MARCAS Y DERECHOS DE AUTOR: Los "PRESTADORES DEL SERVICIO" se obligan a asumir la responsabilidad total para el caso de que al prestar el servicio a la "SECRETARÍA", la "PROFEDET" y "CONAMPROS" infrinjan derechos de terceros sobre patentes, marcas y derechos de autor.

VIGÉSIMA CUARTA.- VICIOS DEL CONSENTIMIENTO: La "SECRETARÍA", la "PROFEDET" y "CONAMPROS" y los "PRESTADORES DEL SERVICIO" reconocen que en la celebración del presente contrato, no ha mediado error, dolo, lesión, violencia, ni vicio alguno del consentimiento que pudiera invalidarlo o nulificarlo.

VIGESIMA QUINTA.- LEGISLACIÓN Y JURISDICCIÓN: Todo lo no expresamente previsto en el presente contrato, se regirá por las disposiciones establecidas en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento, el Código Civil Federal, la Ley Federal de Procedimiento Administrativo y el Código Federal de Procedimientos Civiles. En caso de controversia, para la interpretación y cumplimiento del presente contrato, las "PARTES" se someten a la jurisdicción de los Tribunales Civiles de Orden Federal con residencia en la Ciudad de México, Distrito Federal, y por lo tanto, los "PRESTADORES DEL SERVICIO" renuncian expresamente al fuero que pudiera corresponderle en razón de su domicilio presente, futuro o por cualquier otra causa que tenga o que pudiera llegar a tener.

Leído que fue el presente instrumento por las "PARTES" y enteradas de su contenido y alcance legal, lo firman en nueve tantos al margen y al calce en todas sus fojas útiles, en la Ciudad de México, el día 23 de diciembre de dos mil trece.

Por la "SECRETARÍA"

**Por los "PRESTADORES DEL
SERVICIO"**

Lic. Nicéforo Guerrero Reynoso
Oficial Mayor del Ramo

Jorge Vicente Martínez Rendón
Apoderado General de Axtel, S.A.B. de
C.V. y Avantel, S. de R.L. de C..V.

L.C. María Brenda Estrada de Paz
Directora General de Recursos Materiales
y Servicios Generales

Ing. Héctor Martínez Cordero
Director General de Tecnologías
de la Información

Lic. José Luis Guzmán Martínez
Director de Adquisiciones y Almacenes

Por "LA PROFEDET"

Mtro. Luis Rivera Montes de Oca
Procurador Federal de la Defensa del
Trabajo

Por "CONAMPROS"

Lic. Gustavo Jáuregui Aguilar
Director General del Comité Nacional
Mixto de Protección al Salario

**ÁREAS ENCARGADAS DE ADMINISTRAR, VALIDAR Y VIGILAR
EL CUMPLIMIENTO DE LOS SERVICIOS**

POR “LA SECRETARÍA”

Ing. Carlos Abraham Quijas Luna
Encargado del Despacho de la Dirección de Comunicaciones
y Seguridad de la Información

Por “LA PROFEDET”

Por “CONAMPROS”

Lic. Francisco José Martínez García
Coordinador de Planeación
de Proyectos Estratégico

Celerino Pérez Escobar
Jefe de Departamento de Informática

ANEXO 1

El presente Anexo se encuentra conformado por la Propuesta Técnica presentada por los Prestadores del Servicio y forma parte integrante del contrato RF-138-2013



AXTEL, S.A.S. DE C.V./AVANTEL, S. DE R.L. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGSNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

México, D.F., a 19 de Diciembre de 2013

ANEXO TECNICO

AXTEL, S.A.S. DE C.V. , en participación conjunta con AVANTEL, S. de R.L. de C.V. en adelante AXTEL, anexa la propuesta técnica describiendo de manera clara y precisa y detallando las características técnicas y físicas mínimas de operación de los servicios requeridos en el Anexo Técnico, para la prestación DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGSNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT), de conformidad con las características, especificaciones y cantidades requeridas que se indican en el Anexo Técnico, mismas que AXTEL considero estrictamente para la presentación de su proposición.

ANEXO TÉCNICO

PROPUESTA INDIVIDUAL () PROPUESTA CONJUNTA (X)

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGSNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

1. ANTECEDENTES

AXTEL considera que la Convocante actualmente cuenta con contratos mediante los cuales se brindan los servicios de voz, datos y video a través de una red multiservicios basada en la tecnología MPLS (Multiprotocol Label Switching por sus siglas en inglés), en 195 sitios distribuidos en la República Mexicana, los cuales se encuentran en un esquema de conexión donde todos puedan comunicarse entre sí.

AXTEL considera que por la MPLS también se ofrece el servicio de Internet, para lo cual existe una salida única por donde todos los sitios tienen este servicio a excepción de los nodos con alta criticidad cuyo servicio de Internet es directo.

Las capacidades de tráfico (ancho de banda) y disponibilidad dependen de cada sitio que son establecidas por su criticidad.

AXTEL considera que en este servicio de MPLS se encuentran sitios integrados además de la SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), la Coordinación General del Servicio Nacional de Empleo (CGSNE), la Procuraduría Federal de la Defensa del Trabajo (PROFEDET), la Comisión Nacional de los Salarios Mínimos (CONASAMI), así como el Instituto del Fondo Nacional para el Consumo de los Trabajadores (INSTITUTO FONACOT).

Atentamente

Bajo protesta de decir verdad
Jorge Vicente Martínez Rendón
Representante Común

0002

México, D.F., a 19 de Diciembre de 2013

ANEXO TECNICO

AXTEL, S.A.B. DE C.V., en participación conjunta con AVANTEL, S. de R.L. de C.V. en adelante AXTEL, anexa la propuesta técnica describiendo de manera clara y precisa y detallando las características técnicas y físicas mínimas de operación de los servicios requeridos en el Anexo Técnico, para la prestación DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGSNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT), de conformidad con las características, especificaciones y cantidades requeridas que se indican en el Anexo Técnico, mismas que AXTEL considero estrictamente para la presentación de su proposición.

2. OBJETIVOS

AXTEL considera que la Convocante busca establecer una red de voz, datos y video de cobertura nacional entre sus oficinas que se ubican en el interior del país. Los objetivos fundamentales para conformar la red y a los que AXTEL se compromete a proveer son los siguientes:

- a) Establecer una Red Privada Virtual (VPN) MPLS administrada por AXTEL de cobertura nacional de la Convocante para cursar los servicios de voz, datos y video, según corresponda.
- b) Habilitar el servicio de Internet Dedicado en nodos estratégicos de la Convocante y mediante un nodo concentrador distribuir el servicio a través de la Red Privada Virtual de telecomunicaciones nacional, según corresponda.
- c) Proteger la información de la Convocante de los servicios de Internet a través de soluciones de Seguridad Perimetral, según corresponda.
- d) Instalar cableado con fibra óptica para completar soluciones de cableado estructurado convergente en las oficinas principales de la Convocante que así lo demanden, para contar con la infraestructura mínima y eficiente de conectividad en la red local, según corresponda.
- e) Dotar a las oficinas principales de la Convocante que requieran de equipo de conmutación o switches para interconectar dispositivos de cómputo, impresoras, teléfonos IP



AXTEL, S.A.B. DE C.V./AVANTE!, S. DE R.L. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRADOS ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFDEF), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "COSME", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MEXICO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

entre otros; a fin de conformar así redes de área local o LAN que operen de manera eficiente servicios de voz, datos y video, según corresponda.

- f) Conformar en oficinas estratégicas de la Convocante redes inalámbricas o WLAN para extender la capacidad de las redes LAN, facilitando la movilidad y agilizar la operación de algunos servicios a usuarios internos y externos, según corresponda.
- g) Contar con equipo de telefonía IP en oficinas específicas de la Convocante que así lo demanden para integrarlos en una red de voz nacional, según corresponda.
- h) Habilitar un servicio de mensajería instantánea tipo Chat que permita comunicación en tiempo real con el personal de diversas oficinas, según corresponda.
- i) En nodos estratégicos de la Convocante contar con servicios de videoconferencia que permitan interactuar con personal de diversas regiones del país, según corresponda.
- j) Contar con un servicio integral administrado y alineado a procedimientos estandarizados internacionales para la continuidad de los servicios, según corresponda.

2.1 VIGENCIA DEL CONTRATO

AXTEL considera que la vigencia del contrato será a partir del día hábil siguiente a la notificación del fallo y hasta por 48 meses.

2.2 VISITA A LAS INSTALACIONES DE LA CONVOCANTE

Los días 19 y 20 de noviembre del año en curso, se realizará la visita a las instalaciones de la convocante en la Ciudad de México con los contactos que se presentan a continuación.

CONTACTO	DÍA DE VISITA	LUGAR DE VISITA	CITA
"La SECRETARIA" Ing. Juan Manuel Enriquez Roca.	19	LUGAR DE VISITA FELIX GUEVAS No. 301 PISO 4, COLONIA DEL VALLE, DELEGACIÓN BENITO JUÁREZ, C.P. 03100, PARA DESPUES DIRIGIRSE A LOS SIGUIENTES INMUEBLES:	LA CITA SERÁ EN LA PUERTA PRINCIPAL DEL INMUEBLE LA JUNTA FEDERAL DE CONCILIACIÓN Y ARBITRAJE UBICADA EN AV. AZCAPOTZALCO LA VILLA 311, COL. BARRIO SANTO TOMÁS PARA DESPUES DIRIGIRSE A LOS SIGUIENTES INMUEBLES:
"LA PROFEDET" Lic. Elías Jaime Pott León.	20	- ETIOPIA - PERIFERICO SUR	- REFORMA - CONASAMI - PROFEDET - INSTITUTO FONACOT
"CONASAMI" Lic. Adriana Elguera Almazán.		- AJUSCO	
"CONAMPROS" Lic. Colorino Pérez Escobar.			
"INSTITUTO FONACOT" Lic. Raúl Adén Alvarado Corrales.			

Al finalizar la visita se entregará constancia de asistencia a los licitantes participantes.

AXTEL considerará La visita de manera opcional.

2.3 VISITA A LAS INSTALACIONES DE LOS LICITANTES

Para más información sobre el proceso de licitación, los interesados deben acudir a la oficina de atención al cliente de AXTEL en la Ciudad de México.

20/11/20



AXTEL S.A.B. DE C.V./AVANTEI, S. DE R.L. DE C.V.
EN PARTICIPACION COMUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONSEP), LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL MIXTO DE PROTECCION AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

No aplica.

2.4 FORMA DE PAGO

AXTEL considera que los costos de todos los servicios deberán ser facturados por separado para cada uno de los organismos o Unidades Administrativas de "LA CONVOCANTE", conforme el desglose establecido en el anexo.

AXTEL considera que el servicio se pagará a mes vencido, de conformidad con lo estipulado en el punto VIII Inicio del Servicio de este Anexo Técnico.

AXTEL considera que LA CONVOCANTE no realizará pago alguno por servicios no incluidos en la presente convocatoria, por lo que se recomienda a los licitantes que resulten adjudicados prever lo conducente a efectos de que no existan servicios disponibles no contratados.

2.5 INICIO DEL SERVICIO

AXTEL considera que será su responsabilidad en caso de resultar el licitante adjudicado realizar todas las actividades necesarias para que los servicios relacionados con el INSTITUTO FONACOT, se encuentren operando al 100% el primer minuto del primero de abril del 2014.

Será responsabilidad de AXTEL en caso de resultar el licitante adjudicado realizar todas las actividades necesarias para que los servicios relacionados con el STPS/CONASAMI/CONAMPROS/PROFEDET, se encuentren operando al 100% el primer minuto del primero de abril del 2014, exceptuando lo señalado en el párrafo que precede.

AXTEL considera que para el Servicio de Cableado Estructurado Convergente: Este servicio debe iniciar el 15 de diciembre de 2013, y concluir al menos los servicios integrados en el Anexo "d" nodos para los sitios indicados con los identificadores (id STPS): 6, 8, 9 y 193, para los sitios (id STPS): 1 y 3 el servicio deberá iniciar el 01 de enero de 2014.

En caso de que a la fecha señalada en los párrafos que anteceden, AXTEL en caso de resultar el licitante adjudicado no se encuentre en condiciones de prestar el servicio por sus propios medios, realizará por su cuenta y costo, proporcionar el servicio sin menoscabo de las penas convencionales a las que hubiere lugar, para lo cual, deberá instrumentar el o los convenios con los prestadores actuales, con el fin de no interrumpir el servicio materia de la convocatoria en que se actúa.

Atentamente

Bajo protesta de verdad
Jorge Vicente Martínez Rendón
Representante Común



Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2005

This is to certify that:

AXTEL, S.A.B. de C.V.
Blvd. Díaz Ordaz 3.33 L-1
Col. Unidad San Pedro
Garza García
Nuevo León
CP 66215
México

Holds Certificate No: IS 544935

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2005 for the following scope:

The management system of AXTEL IT Governance includes the activities required to deliver quality services to customers with in Operaciones Clientes Division, by ensuring availability, integrity and confidentiality of information, a working philosophy based on a continual improvement of our processes and service reliability within an IT governance framework, under the Statement of Applicability FO-GO-40 Ver. 2.06 dated 02/Sep/2011.

and on behalf of BSI:

Gary Fenton, Global Assurance Director

Originally Registered: 03/11/2009

Latest Issue: 03/05/2012

Expiry Date: 03/10/2015



Page: 1 of 2

This certificate remains the property of BSI and shall be returned immediately upon request.
An electronic certificate can be authenticated at www.bsigroup.com/ClientDirectory. Printed copies can be validated at www.bsigroup.com/ClientDirectory.
To be read in conjunction with the scope above or the attached appendix.
Information and Contact: BSI, Kitemark Court, Davy Avenue, Kingsthorpe, Milton Keynes MK9 8PP, Tel: +44 845 005 9000
BSI Assurance UK Limited, registered in England under number 2806321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.





AXTEL, S.A.B. DE C.V./AVANTEL S. DE R.L. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (COURNE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MEXICO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

extensión sin hacer uso de la Red Telefónica Pública Conmutada (Public Switching Telephone Network o PSTN) para la Convocante.

3.6 En el caso de los aparatos telefónicos, Axtel se compromete a proporcionar una capacitación en las instalaciones centrales de la STPS/CONASAMI/CONAMPROS/PROFEDET al personal designado de la dependencia para que a su vez dicho personal transmita el conocimiento sobre el uso del equipo.

3.7 AXTEL proporcionará un proceso de atención a fallas con el personal del área de Tecnologías de Información de la Convocante, para la atención de todos los requerimientos como altas, bajas y cambios, aspectos de facturación y mantenimientos requeridos durante la vigencia del contrato. Para la acreditación de éste punto, hemos incluido un documento titulado "Proceso de atención a fallas" que detalla con mayor exactitud nuestro modelo operativo de atención a fallas.

3.8 AXTEL cuenta en sus instalaciones con un Centro de Control y Operación, así como un Centro de Seguridad para llevar a cabo el monitoreo, la administración y asistencia técnica remota de la infraestructura instalada en la Convocante; así como para la generación de reportes que serán solicitados de manera recurrente durante la vigencia del contrato. Los detalles del centro de operación NOC y los procedimientos a seguirse por AXTEL, se encuentran en el apartado titulado "Metodología a utilizar" así como, la matriz de escalación de dicho centro.

3.9 Para el proceso de instalación de los servicios AXTEL asignará un Project Manager a fin de coordinar como punto único de contacto, todo el proceso de instalación de los servicios hasta la entrega satisfactoria de los mismos. En su oferta técnica AXTEL entregará documento (copia) que compruebe al menos 2 Project Manager certificados por el Project Management Institute (PMI), para la Convocante. Los certificados de estas personas se encuentran contenidos dentro de la presente carpeta, Apartado "Project Manager"

3.10 En el caso específico el MAAGTIC-SI (Manual Administrativo y de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información), AXTEL confirma conocerlo y se compromete a trabajar de acuerdo al mismo, integrando la documentación que se le solicite por parte de la Convocante en el momento que se le requiera.

3.11 Por lo anterior AXTEL en su oferta técnica confirma que cuenta con un sistema de administración de seguridad de información el cual opera mediante estándares internacionales, para ello proporcionará su certificación ISO 27000 (copia), para la Convocante. El certificado que comprueba éste requerimiento se encuentra localizado en la presente carpeta dentro del apartado "Certificado ISO 27000."

Atentamente

Bajo protesta de ser verdad
Jorge Vicente Martínez Rendón
Representante Común

México, D.F., a 19 de Diciembre de 2013

PROPUESTA TÉCNICA

PROPUESTA INDIVIDUAL () PROPUESTA CONJUNTA (X)

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGSNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

4. RED PRIVADA VIRTUAL NACIONAL MPLS ADMINISTRADA DE TELECOMUNICACIONES PARA VOZ, DATOS Y VIDEOCONFERENCIA.

4.1 ASPECTOS GENERALES QUE DEBE CUMPLIR LA RED VPN DE AXTEL PARA LA CONVOCANTE.

4.1.1 AXTEL se compromete a implementar una Red Privada Virtual Nacional de Telecomunicaciones que permitirá la transmisión de Voz, Datos y Video a través de dicha infraestructura.

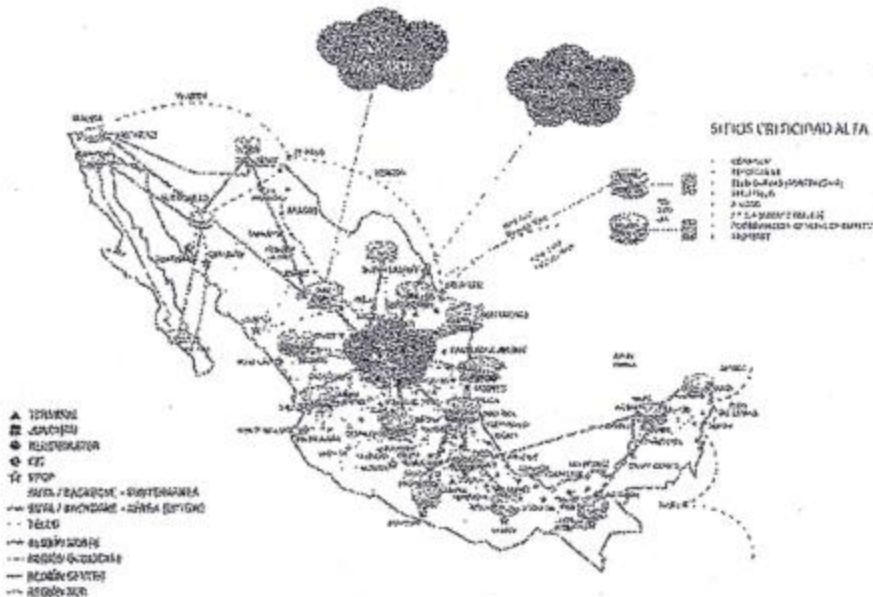
La información Técnica de los equipos propuestos para esta solución se encuentra detallada en la Carpeta 2 sección Referencias Técnicas VPN MPLS

4.1.2 AXTEL cuenta con un red VPN (Red Privada Virtual por sus siglas en Inglés) que funge como backbone nacional propio con tecnología MPLS (Multiprotocol Label Switching por sus siglas en Inglés) basado en protocolo IP el cual es independiente de su infraestructura de Internet.

De acuerdo a la respuesta a la pregunta 37 de la empresa UNINET de la junta de aclaraciones del día 25 de noviembre del 2013, AXTEL confirma que proporcionará el servicio de acceso de la VPN-MPLS e internet en medios y equipos separados.

4.1.3 La red de VPN-MPLS de AXTEL será empleada para interconectar las oficinas y para ello presenta en el siguiente diagrama como parte de su oferta técnica un mapa de la República Mexicana que muestra la topología de cobertura de la red de VPN-MPLS.

Mapa de Cobertura y Topología Red VPN-MPLS



4.1.4 De acuerdo a la precisión 7, de la Junta de Aclaraciones, AXTEL considera que la red VPN será escalable, flexible, eficiente y transparente; de tal forma que en el momento que sea requerido por LA CONVOCANTE, se puedan agregar nuevo equipamiento y servicios, o bien disminuir los existentes, así como ampliar o disminuir nodos de red o ampliar los anchos de banda, sin afectar la operación de la red misma o la operación de los demás nodos.

4.1.5 AXTEL considera y acepta que la ubicación de cada una de las oficinas, se especificarán en el Anexo "A" donde se indica la criticidad del nodo, la dirección, teléfono en sitio y ancho de banda requerido para el servicio de VPN-MPLS.

4.1.6 La red VPN de AXTEL cumple con al menos los estándares RFC 2547Bis y RFC 3031, lo que implica que la red es realmente una red MPLS.

4.1.7 La red VPN de AXTEL opera bajo un esquema de 7x24x365 de manera que cumple con una disponibilidad en su backbone de al menos 99.98% mensual.

4.1.8 La red VPN AXTEL soporta topología malla completa (full mesh por sus siglas en Inglés), tipo estrella (Hub & Spoke) o una combinación de ambas dependiendo de la operación permitiendo así una conectividad conocida como any-to-any.

4.1.9 La red VPN de AXTEL soportará el direccionamiento IP privado que se designe por "La Convocante" o público en caso requerido, de igual forma debe permitir la designación de subredes para conformar la segmentación física o lógica según sea el caso y soportar la configuración de NAT (Network Address Translation) y/o PAT (Port Address Translation).

De acuerdo a la respuesta de la pregunta 75, presentada por la empresa UNINET S.A. de C.V. de la junta de aclaraciones celebrada el 25 de noviembre de 2013, AXTEL considera que las características de NAT y PAT se soportarán en los equipos CPE.

4.1.10 La red VPN de AXTEL contará con tiempos de latencia entre dos nodos de su backbone con valores inferiores a los 100 milisegundos considerando una trayectoria de ida y vuelta (round-trip), mientras que los valores del Jitter deben encontrarse por debajo de los 50 milisegundos en una dirección y pérdida de paquetes menores al 1%.

4.1.11 AXTEL especifica dentro de su propuesta que cuenta con la capacidad en su VPN-MPLS (objeto de esta licitación), de interactuar con una o más VPN-MPLSs de AXTEL (extranets) con características similares, sin costo adicional.

De acuerdo a la respuesta de la re-pregunta técnica 1 presentado por la empresa UNINET S.A. de C.V. de la junta de aclaraciones del día 26 de noviembre de 2013, AXTEL considera que las VRF's se configuraran dentro de la infraestructura MPLS en los puntos más cercanos a los CPE de los sitios que se definan.

4.1.12 AXTEL considera una VPN-MPLS sectorial, por lo cual la comunicación a cada uno de los sitios que conformen la red será de forma directa, es decir, no pasará por ningún sitio central de cualquier otra red.

4.1.13 Para enlaces bajo tecnología de transporte IP AXTEL proporcionará una red maillada en BGPv4, empleando OSPFv2, como protocolo de ruteo que asegurará la transferencia de información entre los enlaces principal y redundante dentro de la red BGP."

4.1.14 La implementación de los enlaces VPN MPLS, AXTEL como parte de su propuesta técnica entrega un plan de despliegue (Gantt) que describe las actividades y los tiempos estimados para llevar a cabo la implementación, mismo que será susceptible de modificarse de conformidad a las necesidades y sugerencias de las áreas técnicas.

De acuerdo a la respuesta de la pregunta No. 87, de la empresa UNINET S.A. de C.V. de la junta de aclaraciones del día 25 de noviembre de 2013, AXTEL entregará un plan de trabajo

por cada uno de los organismos integrantes de la Convocante el cual tendrá todas las tecnologías a implementar. Para el caso del Instituto INFONACOT el plan de trabajo incluirá únicamente la implementación de los enlaces VPN MPLS e Internet dedicado.

AXTEL incluye dentro de su propuesta "Plan de despliegue Gantt, carpeta 3 sección Plan de Trabajo".

4.1.15 AXTEL se compromete a cubrir los gastos que se generen por su personal por el desplazamiento a sitio para la implementación de los enlaces.

4.1.16 AXTEL asume la responsabilidad total en caso de que al proporcionar el servicio de la VPN MPLS, infrinja derechos de propiedad intelectual y/o industrial de terceros sobre patentes, marcas y derechos de autor, entre otros, por lo que se obliga y acepta eximir a "La Convocante" de cualquier responsabilidad civil o penal.

4.1.17 AXTEL cuenta con la concesión y permisos correspondientes para operar y comercializar este tipo de redes MPLS, otorgado por la Secretaría de Comunicación y Transporte.

De acuerdo a la respuesta de la pregunta 6, presentada por ALESTRA, S.A de C.V. de la junta de aclaraciones del día 25 de noviembre de 2013, AXTEL incluye dentro de la presente propuesta copia simple de su título de concesión.

AXTEL incluye dentro de su propuesta "Título de concesión otorgada por la Secretaría de Comunicaciones y Transportes, Carpeta 2 Propuesta Técnica"

4.2 REQUERIMIENTOS DE ACCESO Y REDUNDANCIA EN LA VPN PARA LA CONVOCANTE

4.2.1 La red VPN-MPLS de AXTEL se compromete a interconectar las oficinas de la Convocante a través de un medio de acceso terrestre como fibra óptica.

4.2.2 Cada enlace de acceso contará con una disponibilidad de al menos 99.8% mensual y para ello AXTEL proporcionará dentro de los primeros 5 días hábiles del siguiente mes un reporte donde se especifiquen todas las contingencias presentadas en el mes anterior ya sea por mantenimiento preventivo, correctivo o falla en la continuidad de éste servicio. En caso de que algún evento atribuible a AXTEL se encuentre por debajo del valor de disponibilidad especificado será sujeto de penalización (referirse a la sección de deductivas).

4.2.3 AXTEL establecerá balanceo de tráfico para los nodos de la Secretaría y sus organismos que requiera de esquemas de "NxE1" (Multilink).

4.2.4 AXTEL atenderá crecimientos de la red mediante accesos locales desde "Nx1024 kbps", hasta "NxE1" y adición de localidades, lo cual no requerirá cambios significativos de configuración en ninguno de los sitios ya existentes.

4.2.5 Referente a los incrementos de enlaces VPN-MPLS, AXTEL se compromete a atender los incrementos de la cantidad de enlaces VPN-MPLS derivado de crecimiento de la Convocante, mismos que podrán ser de manera permanente o temporal y obedecerán a solicitud expresa. Así mismo los incrementos de ancho de banda de los enlaces de la VPN-MPLS mediante accesos locales desde "Nx1024 kbps", hasta "NxE1", mismos que podrán ser de manera permanente o temporal y obedecerán a solicitud expresa.

4.2.6 Referente a los movimientos de enlaces VPN-MPLS AXTEL se compromete a atender los requerimientos de reubicación en enlaces de VPN-MPLS que se solicite los derivados por cambio de domicilio de la oficina en donde exista un enlace VPN-MPLS, tomando en consideración que puede ser dentro de la misma ciudad o en cualquier parte de la República Mexicana y que significará el movimiento de infraestructura y enlace. Así mismo cambio de ubicación física de los equipos de comunicaciones derivado de la reubicación de infraestructura para la conexión del enlace dentro del mismo inmueble.

De acuerdo a la respuesta de la pregunta 78 presentada por la empresa UNINET S.A DE C.V. pag.5 de la junta de aclaraciones del día 25 de noviembre de 2013, AXTEL, considera para la STPS/CONASAMI/PREOFEDET se proyecta un 15% de cambios domicilio del total de los sitios por organismo durante la vigencia del contrato, para el caso del instituto INFONACOT, se consideran 15 cambios de domicilio en promedio por año.

4.2.7 En todos los casos la interfaz de entrega del servicio de conectividad a la red VPN-MPLS de AXTEL será a través de un puerto LAN 10/100/1000 (Mbps) en RJ-45 de cobre, del equipo ruteador (CPE) y se conectará y configurará al puerto del switch que designe "La Convocante", ya sea un equipo de conmutación existente o uno nuevo que forme parte de la presente solución.

4.2.8 AXTEL será responsable de la administración de la red VPN-MPLS de punta a punta incluyendo los servicios de acceso también conocidos como última milla.

4.2.9 En oficinas estratégicas de la Convocante, AXTEL se compromete a proveer un servicio ininterrumpido, por lo que la conectividad del acceso a la red VPN-MPLS de AXTEL será redundante.

4.2.10 Para los casos del párrafo anterior, AXTEL considerará como parte de su propuesta, la instalación de dos accesos con la misma capacidad de ancho de banda pero con medios y trayectorias independientes. Asimismo, AXTEL instalará equipos de ruteo también independientes. Las oficinas que deben contar con los servicios de acceso redundante son las que cuentan con criticidad alta y aparecen en el Anexo "A".

4.2.11 Para el caso particular del INSTITUTO FONACOT AXTEL considera en su propuesta la instalación de dos accesos con la misma capacidad de ancho de banda pero con medios distintos y trayectorias independientes. Asimismo, AXTEL instalará equipos de ruteo también independientes. Las oficinas que deben contar con los servicios de acceso redundante son las que cuentan con criticidad alta y aparecen en el Anexo "A".

De acuerdo a la respuesta de la pregunta 123, realizada por la empresa UNINET S.A. de C.V. de la junta de aclaraciones del 25 de noviembre de 2013, AXTEL considera realizar los trabajos o adecuaciones que se requieran para instalar los equipos para el correcto funcionamiento de su infraestructura. Para el caso del instituto FONACOT proveerá estos contactos eléctricos.

4.2.12 Para los casos de las oficinas que cuentan con la solución de acceso redundante, el servicio debe configurarse de tal forma que en caso de falla en cualquier punto de la "trayectoria principal" y de manera automática la "trayectoria redundante" debe tomar el control total de los servicios y posteriormente retornar a su estado anterior cuando la contingencia se haya resuelto. Al respecto, el término "trayectoria" debe interpretarse como el conjunto de componentes que forman la solución de conectividad desde la red VPN-MPLS de AXTEL hasta la salida del equipo de ruteo (CPE) con fuente redundante o puerto LAN.

De acuerdo a la respuesta de la pregunta No. 7 presentada por UNINET S.A. DE C.V. de la junta de aclaraciones celebrada el 26 de Noviembre del 2013, AXTEL proporcionará fuentes redundantes solamente para los sitios catalogados como críticos de INFONACOT.

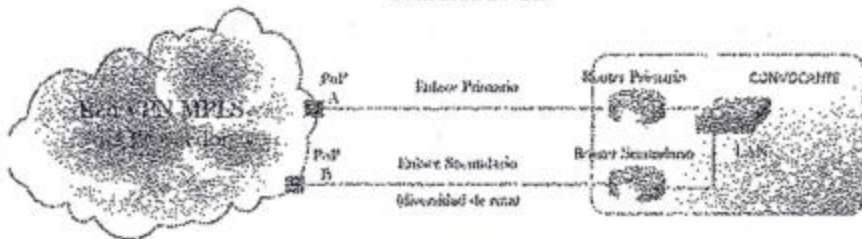
4.2.13 Tipos de Nodos

a) Criticidad Alta:

AXTEL se compromete a instalar éstos nodos vía fibra óptica. El equipo de ruteo con capacidad de redundancia en accesos locales (enlaces) de última milla, que terminen cada uno en una central local distinta de AXTEL como proveedor de la VPN-MPLS en configuración HSRP (Hot Standby Router Protocol).

Enlaces al 100% de su capacidad (ancho de banda).

Criticidad Alta



Ruteo con capacidad de redundancia en accesos locales (enlaces) de última milla, que terminen cada uno en una central local distinta de AXTEL de la VPN-MPLS.

Enlace primario al 100% de su capacidad (ancho de banda), redundancia al 100% de su capacidad (ancho de banda).

Criticidad Media

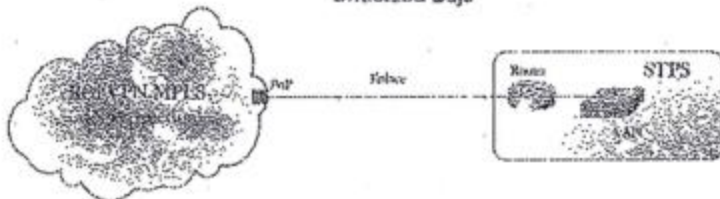


c) Criticidad Baja:

Ruteo para acceso local (enlace) de última milla.

Enlace único al 100% de su capacidad (ancho de banda).

Criticidad Baja



AXTEL considera el Anexo "A" en el cual se especifican los nodos de acuerdo a su criticidad, dicha criticidad aparece con las siguientes letras: B = Baja, M = Media, C = Crítica (Alta), por lo que deben aplicar los criterios arriba mencionados para los servicios de VPN-MPLS a proporcionar.

4.3 CALIDAD DE SERVICIOS EN LA VPN-MPLS

4.3.1 La garantía de Calidad de Servicio o QoS (Quality of Service) se cumplirá de extremo a extremo en la red VPN-MPLS de AXTEL de tal forma que cuente con mecanismos de control de retardo y prioridad de tráfico que aseguren un trato homogéneo para las aplicaciones en todo el trayecto de los paquetes.

4.3.2 Para fines de priorización de tráfico sobre los enlaces de acceso a la red VPN-MPLS AXTEL se compromete a brindar una solución que identifique paquetes en línea sensibles al retardo, garantizando los niveles de servicio, con miras a optimizar la utilización de ancho de banda en cada sitio.

4.3.3 La VPN-MPLS de AXTEL soporta los mecanismos de calidad de servicio como:

- CAR (Committed Access Rate) como mecanismo de limitación de ancho de banda para ciertas aplicaciones.
- WRED (Weighted Random Early Discard) para prevenir congestión.
- LLQ (Low Latency Queueing) prioriza el envío de tráfico sensible a retrasos enviándolos a una cola "Strict Priority" y manejando el resto de los datos con "Weighted Fair Queueing".
- FIRF.12 reduce el jitter fragmentando el tamaño de todos los paquetes.
- Marcado de paquetes basado en códigos de diferenciación de servicios DiffServ o precedencia IP.

4.3.4 Por lo tanto, la red VPN-MPLS AXTEL soportará las calidades de servicio (QoS) para el etiquetado de paquetes en Tiempo Real, Datos que sean Críticos y Datos Normales.

4.3.5 AXTEL proporcionará memoria técnica con la información que contenga la configuración de QoS entregada para cada una de las oficinas a fin de que al cabo de un bimestre sean revisadas y se determine si son los parámetros adecuados o deben cambiarse.

4.3.6 El personal técnico de AXTEL considera en su propuesta llevar a cabo mesas de trabajo con el personal de "La Convocante" que se designe para tal efecto y que al término de dichas mesas se determinen y ejecuten de manera programada las reconfiguraciones en los parámetros de QoS de las oficinas que así lo requieran.

4.3.7 AXTEL considera que las modificaciones de los parámetros de QoS en los distintos nodos que solicite "La Convocante" se llevaran a cabo sin costo adicional.

4.4 EQUIPO DE RUTEO PARA LA RED DE VPN

4.4.1 AXTEL considera en su propuesta proporcionar, instalar, administrar y mantener, en su solución el equipo de ruteo o CPE (Customer Premises Equipment) para interconectar las diversas oficinas de la Convocante.

4.4.2 AXTEL considera y se compromete a que todo el equipo de ruteo debe ser nuevo, de última generación y de la misma marca, no se aceptan soluciones con más de una marca, adicionalmente AXTEL entregará carta del fabricante en papel membretado y firmado por el representante legal del fabricante, dirigida al proceso de licitación que nos ocupa, donde se especifique que AXTEL es distribuidor autorizado por el fabricante y que cuenta con el personal técnico calificado para instalar, configurar, administrar y monitorear los equipos de ruteo que son instalados en la Convocante.

AXTEL incluye dentro de su propuesta "Cartas de proveedores, Carpeta 2 sección Carta de Fabricante Equipo de Ruteo".

4.4.3 AXTEL entrega integralmente con su oferta técnica los documentos que comprueban la capacidad de al menos 4 ingenieros certificados en la marca del fabricante para la instalación de los equipos de ruteo.

AXTEL incluye dentro de su propuesta "Certificaciones del personal, Carpeta 2 sección Certificados del Fabricante"

4.4.4 El equipo de ruteo será administrado y monitoreado de manera remota a través del NOC (Network Operation Center) de AXTEL.

4.4.5 AXTEL considera que el equipo CPE contara con al menos 2 puertos GE del tipo 10/100/1000 (Mbps) con conector RJ-45 en cobre. Con puerto de consola independiente y debe tener la capacidad de soportar las interfaces seriales como T1/E1, T3/E3, cobre y fibra Gigabit Ethernet, según se requieran. Soportará diversos tipos de ruteo y protocolos como BGP, IS-IS, RIP1, RIP2, IGMP, EIGRP, OSPF, IGMPv1, IGMPv2, IGMPv3, PIM SM, SSM, DVMRP, IPSec, GRE, BFD, así mismo debe soportar ruteo estático, IPv4, IPv6, SNMP, IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 y L3 VPN, H323.

De acuerdo a la respuesta de la pregunta 15 realizada por AXTEL S.A. de C.V. de la junta de aclaraciones del 25 de noviembre de 2013, AXTEL proporcionará las funcionalidades Bidirectional Forwarding Detection, denominado BFD y Network Based Advanced Routing.

4.4.6 El equipo de ruteo soporta encapsulación Ethernet, 802.1q VLAN, Point-to-Point Protocol, Multilink Point-to-Point Protocol, High-Level Data Link y V.35. Así mismo debe soportar QoS, CBWFO, WRED, PBR, PIR, NABR para la administración del tráfico (referirse a la sección 4.3.3), SNMP, Telnet y SSH. Así como cifrado por hardware.

4.4.7 Es modular, con sistema operativo multiprotocolo integrado. El equipo cuenta con hardware de procesamiento específico por función, con la idea de no afectar el desempeño del equipo con la adición de nuevos servicios. Soporta las interfaces físicas tales como: módulos seriales sincrónicos, asíncronos, de alta velocidad (T1), Ethernet, FastEthernet, E1, PRI, así como compresión por hardware.

4.4.8 El equipo que AXTEL se compromete a instalar, soporta el manejo de técnicas de gestión de colas (como gestión de colas por prioridad, personalizada o baja latencia) y manejo de precedencia IP tanto en interfaces WAN como LAN para garantizar el correcto tratamiento de los frames o paquetes de datos, voz y video.

4.4.9 Los ruteadores que se compromete a entregar AXTEL, soportan los protocolos VRRP, HSRP o GLBP, así como NetFlow.

4.4.10 Para el caso particular del INSTITUTO FONACOT AXTEL considera en sus nodos de los ID del 259 al 285 del Anexo "A", al menos 2 puertos RJ-45 Ethernet, 10/100/1000 Mbps adicionales a los indicados en el punto 4.4.5.

De acuerdo a la respuesta de la pregunta 3, realizada por la empresa UNINET S.A de C.V. de la junta de aclaraciones del 25 de Noviembre del 2013, AXTEL anexa la tabla en formato Excel en la cual se incluyen las referencias de los puntos indicados en el anexo técnico incluyendo las siguientes columnas: requerimiento, nombre del folleto, manual de referencia original o página WEB con la liga de la página, página del folleto, manual de referencia original o página, traducción simple al español.

AXTEL presenta dentro de su propuesta "Referencias Técnicas, carpeta 2 sección Referencias Técnicas VPN MPLS"

DESCRIPCIÓN GENERAL DE LA SOLUCIÓN DE RED PRIVADA VIRTUAL OFERTA AXTEL A LA CONVOCANTE.

Multiservicios IP es una red de datos desplegada en una infraestructura de red compartida, que garantiza las mismas políticas de seguridad, administración, desempeño y calidad de servicio que en una red privada, pero con mayores beneficios tecnológicos y operativos a un costo menor.

El tráfico de paquetes de datos en una red privada virtual de un cliente, proviene de diversas aplicaciones (correo electrónico, intranets corporativas, Siebel, SAP, e-learning, transacciones electrónicas, voz, video, Internet, etc.), estas aplicaciones tienen una importancia específica para el cliente según sus necesidades.

La infraestructura de la red de AXTEL, cuenta con tecnología MPLS (Multiprotocol Label Switching), que nos permite utilizar mecanismos de Calidad de Servicio (QoS), para asignar prioridades diferenciadas al tráfico de paquetes de datos según la aplicación del cliente.

DESCRIPCIÓN TÉCNICA DEL PRODUCTO

Multiservicios IP es una red privada virtual (Virtual Private Networks) con tecnología MPLS (Multiprotocol Label Switching) que integra los diferentes servicios y aplicaciones (voz, video, datos e Internet) en una sola conexión mediante una convergencia en protocolo IP con capacidades de entrega desde 64 Kbps hasta 155 Mbps.

La tecnología IP/MPLS permite crear VPNs, ingeniería de tráfico y QoS. El Backbone de 20 Gbps se compone de Gigarouters redundantes conectados en Packet over Sxnet (POS) garantizando la mejor confiabilidad de la red.

AXTEL ofrece una red que da seguridad porque es totalmente independiente al Backbone de Internet, por lo que la privacidad y confidencialidad está garantizada.

A cada VPN MPLS se le asigna un identificador y un juego de direcciones IP para cada puerto los cuales sirven para armar una tabla de ruteo independiente por cada Cliente. Con esto las direcciones del Cliente no son visibles para nadie dentro de la Red de AXTEL.

La información de dos Clientes no se mezcla, a menos que decidan crear una Extranet, la cual será configurada por AXTEL previa solicitud.

Con base a las modalidades de **Multiservicios IP**, existe una distribución de ancho de banda asignado a cada aplicación en caso de una congestión en la red del cliente, mismo que será dinámico de acuerdo a las aplicaciones del Cliente.

DISTRIBUCIÓN DE BW	
VOZ	20%
VIDEO	30%
DATOS MC	20%
BEST EFFORT	RESTO

Consideraciones de consumo por tipo de tráfico:

Tamaño del Paquete		
Voz	34 K	Por canal de voz
SAP	30 K	Por paquete Transmido
Video	32 K - 768 K	Depende l del número de cuadros transmitidos
Windows	25%	Del total de BW Best Effort

Además se cuenta con el soporte a IPv6 dentro de MPLS de forma nativa, es decir, no se cuenta con métodos de transición temporales a IPv6 en la red de Axtel. Ver sección de Cobertura para las ciudades soportadas.

CALIDAD EN EL SERVICIO QOS (Quality of Service)

Dado que **Multiservicios IP** es una red de datos desplegada en una infraestructura de red compartida, que garantiza las mismas políticas de seguridad, administración, desempeño y calidad de servicio que en una red privada, a continuación se ilustran los tipos de aplicaciones y el porcentaje de ancho de banda garantizado en caso de una congestión.

Modalidad	Número de Aplicaciones	Tipo de Aplicaciones	AB Garantizado en congestión
Datos	1	Trafico Best Effort	0
Datos Críticos	2	Aplicación de Datos 1	50
		Trafico Best Effort	0
Multimedia	3	VOIP	55
		Aplicación de Datos 1	25
		Trafico Best Effort	0
Multiservicios Datos	4	VOIP	20
		Aplicación de Datos 1	30
		Aplicación de Datos 2	20
		Trafico Best Effort	0
Multiservicios	4	VOIP	20
		VIDEO	30
		Aplicación de Datos 1	20
		Trafico Best Effort	0

*AB= Ancho de Banda

ARQUITECTURA DE LA RED MULTISERVICIOS IP VPN-MPLS DE AXTEL

La arquitectura de la red Multiservicios IP de AXTEL es red basada en el protocolo MPLS la cual permite contar con una red completamente mallada con lo que asegurar un nivel de disponibilidad en el backbone del 99.98%, lo que se traduce al cliente en una alta disponibilidad del servicio, a continuación se mencionan los principales componentes de la red.

Equipos enrutadores del lado del cliente (CPE, Customer Premises Equipment, por sus siglas en inglés).- Este equipo es el encargado de realizar la conexión de la red del cliente hacia el primer punto de conexión de la red VPN-MPLS.

Equipos enrutadores de acceso a la red VPN-MPLS (PE, Provider Edge router, por sus siglas en inglés).- Estos equipos son los encargados de recibir la conexión del router CPE del lado del cliente y es en el PE donde ocurrirá la mayor cantidad de procesos tanto de ruteo como de envío y recepción del tráfico de la LAN del cliente hacia el core de la red VPN-MPLS.

Equipos CORE red VPN-MPLS.- Estos equipos serán los encargados de llevar a cabo la conmutación y transporte del tráfico generado por las redes LAN de los clientes.

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRAL ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFIDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CGSENE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MEXICANO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACUT).



Diagrama de la arquitectura de la red VPN-MPLS

DESCRIPCIÓN DE LA SOLUCIÓN RED VPN-MPLS

AXTEL como parte de su propuesta técnica/económica integra todos los sitios del anexo A con sus diferentes capacidades de ancho de banda y medios de acceso de entrega para la integración de cada uno de estos sitios a la red VPN-MPLS solicitada, cumpliendo en su totalidad con las características y requerimientos realizados por la CONVOCANTE. A continuación AXTEL presenta los siguientes diagramas de conectividad por nivel de criticidad indicados por la CONVOCANTE.

- a) **Criticidad Alta.-** AXTEL entregará dos enlaces de acceso a la VPN-MPLS con diversidad de ruta y conexión a diferente central y con equipo de ruteo independiente para recibir cada uno de los que serán conectados a los routers PE en el primer punto de conexión más cercano al sitio del cliente y a la red VPN-MPLS. El ancho de banda para cada uno de los enlaces será de la misma capacidad.



- b) **Criticidad Media.- AXTEL entregará dos enlaces de acceso a la VPN-MPLS con diversidad de ruta y conexión a diferente central. Para este tipo de nodo los enlaces se interconectaran aún solo equipo de ruteo (CPE) para la conexión a la red VPN-MPLS. El ancho de banda para cada uno de los enlaces será de la misma capacidad.**



- c) **Criticidad Baja.- AXTEL considera la entrega de un solo enlace para la conexión a la red VPN-MPLS y un solo equipo ruteador (CPE) de lado del cliente.**



AXTEL considera el Anexo "A" en el cual se especifican los nodos de acuerdo a su criticidad, dicha criticidad aparece con las siguientes letras: **B = Baja**, **M = Media**, **C = Critica (Alta)**, por lo que deben aplicar los criterios arriba mencionados para los servicios de VPN-MPLS a proporcionar.

AXTEL considera el aprovisionamiento de los equipos de enrutamiento para cada uno de los sitios del ANEXO "A", dicho equipamiento fue dimensionado de acuerdo a las características de criticidad solicitado por la CONVOCANTE y por el ancho de banda del sitio. Los equipos que AXTEL considera en su propuesta son del fabricante Cisco Systems de las familias 2900 y 3900, para los equipos considerados criticos para del INFONACOT se consideraran con fuentes redundantes.

La siguiente tabla muestra la cantidad de equipos ruteadores considerados por AXTEL por modelo.

MODELO DE EQUIPO PARA ROUTERS MPLS	CANTIDAD
CISCO2901/K9	274
CISCO2911/K9	1
CISCO2921/K9	4
CISCO2951/K9	1
CISCO3925E/K9	5

Atentamente

Bajo protesta por verdad
 Jorge Vicente N. Representa. 2 Hendón imún

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS, REDES, SERVICIOS ADMINISTRACION DE VOZ, DATOS, INTERNET Y VOZ/CONFERENCIA PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDT), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO "GEBNE", LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL, NEXTO DE PROTECCION AL SALARIO (CONAPROPS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

México, D.F., a 19 de Diciembre de 2013

REFERENCIAS TECNICAS SECCION MPLS

REQUERIMIENTOS	TEXTO EN EL DOCUMENTO	NOMBRE DEL DOCUMENTO	PARÁMETROS	Figuras	TÍTULOS O USOS DEL EQUIPO
4-4.5 El equipo propuesto cuenta con al menos 2 puertos GE del tipo 10/100/1000 con conector RJ 45 un core	Total Ethernet WAN 10/100/1000 Ports Cisco 2901: 2 Cisco 2911: 3 Cisco 2921: 3 Cisco 2951: 3	Total Sheet - Cisco 2900 Series Integrated Services Routers	11	Tabla 7, Fila 0	Total de puertos WAN sobre el equipo Cisco 2901: 2 Cisco 2911: 3 Cisco 2921: 3 Cisco 2951: 3
Cuenta con puente de control independiente	Serial Console Port Cisco 2901: 1 Cisco 2911: 1 Cisco 2921: 1 Cisco 2951: 1	Data Sheet - Cisco 2900 Series Integrated Services Routers	12	Tabla 7, Fila 2	Puerto de Consola Serial Cisco 2901: 1 Cisco 2911: 1 Cisco 2921: 1 Cisco 2951: 1
Y tiene la capacidad de soportar las interacciones como T1/E1, T3/E3, cobre y fibra Gigabit Ethernet, según se negociaran	All Cisco 2900 Series Integrated Services Routers offer embedded hardware encryption acceleration, voice and video-capable digital signal processor (DSP) slots, optional firewall, intrusion prevention, call processing, voicemail, and application services. In addition, the platform supports the industry widest range of wired and wireless connectivity options such as T1/E1, T3/E3, copper and fiber GE.	Data Sheet - Cisco 2900 Series Integrated Services Routers	1	3	Toda la serie de routers de servicios integrados Cisco 2900 ofrece embebido aceleración de cifrado de hardware, ranuras de voz y procesadores de señales digitales con capacidad de vídeo (DSP), servidor de seguridad aplicación, prevención de intrusiones, procesamiento de llamadas, correo de voz y servicios de aplicación. Además, las plataformas soportan la más amplia gama de opciones de conectividad por cable e inalámbricas, tales como T1/E1, T3/E3, cobre y fibra de GE.

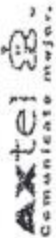


AXTEL S.A.S. DE C.V. JAWANTEL, S. DE R.L. DE C.V.
EN PARTICIPACION CONSULTA

CONTINUACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VEC, DATOS INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE BAMBULO "COBNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONSAMIM), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (COMIPROSAL) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACON).

REQUERIMIENTOS	PRODUCTO ENTREGADO	NOBRE DEL DOCUMENTO	FECHA	ESTATUS	PROCESOS
Debe soportar diversos tipos de rutas y protocolos como BGP, L-3, RIP 1, RIP2, IGRP, EIGRP, OSPF, IGMPv3, RIPv2, IGMPv3, Vlan SM, SRM, DMVPN, IPSec, GRE, BFD, o si incluye todo o parte de los mismos, IPv4, IPv6, SNMP, IPv4-to-IPv6 Multicast, MPLS, L2/L3 VPN, RIB33	Protocols: IPv4, IPv6, Static Routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), Router Reflectors, Intermediate System-to-Intermediate System (IS-IS), Multicast protocols Group Management Protocol (GMP), Protocol Independent Multicast sparse mode (PIM SM), PIM Sparse Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DMVRP), IPSec, Generic Routing Encapsulation (GRE), 802.1Q VLANs, Tunneling, Detection (BFD), IPv4-to-IPv6 Multicast, MPLS, L2/L3 VPN, RIB33	Data Sheet Cisco 2500 Series Integrated Services Routers	9	Tabla 4, Pá. 2	Procesos: IPv4, IPv6, BGP, EIGRP, OSPF, IGRP, Protocolo de Rutas de Enlaces (RIP), Protocolo de Enlace a Protocolo BGP, Sistema Interconectado de Internet (IS-IS), Protocolo de administración de grupos de Internet Multicast (IGMPv3), Protocolo Independiente Multicast de Modo Densidad (PIM SM), PIM fuente específica Multicast (SSM), Protocolo de Encapsulamiento Multicast de Vector de Dirección (DMVRP), IPSec, Encapsulación de ruteo genérico (GRE), In-direccional de Distribución de Ruteo (BFD), Multicast IPv4-a-IPv6, MPLS, L2/L3 VPN, RIB33
	Image info c2500		68	Fila 4	RIP
	Image info c2500		68	Fila 4	RIPv2, RFC 1724 MS Extension
	Image info c2500		34	Fila 9	IP Enhanced IGRP Router Authentication
	Image info c2500		33	Fila 14	ISMP Fast Leave
	Image info c2500		33	Fila 17	ISMP Version 2
	Image info c2500		73	Fila 17	SNMP (Simple Network Management Protocol)
	Image info c2500		30	Fila 15	R.333 Call Restriction Enhancements

Revisado por el Comité de Control de Calidad, el 15 de mayo de 2014, a las 10:00 horas, por el personal de la Gerencia de Operaciones.



COMUNICACIONES
TELÉFONICAS

AXTEL S.A.S. DE C.V. (ANEXOS) S. DE RL. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRATIVOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIAL PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (SETRAT) EN EL PUEBLO FEDERAL DE LA DEFENSA DEL TRABAJO (PROVDEFET), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO (COSENE), LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAL), EL COMITE NACIONAL 1970 DE PROTECCION AL EMPLEO (CONAPROE) Y EL INSTITUTO DEL PUERTO NACIONAL PARA EL COMERCIO DE LOS TRABAJADORES (INSTITUTO FONACOCI).

REQUERIMIENTOS	TIPO DE EQUIPAMIENTO	NUMERO DEL DOCUMENTO	PAIS DE ORIGEN	TIPO DE SERVICIO
4.4.4 El equipo de rutado debe soportar encapsulacion Ethernet, 802.1q VLAN, Point-to-Point Protocol, Frame Relay, Multicast Point-to-Point, Multicast, 802.1q VLAN, High-Level Data Link Control (HDLC), Serial (RS 232, RS-449, X.21, V.35, and EIA-430), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.	Encapsulacion Ethernet, 802.1q VLAN, Point to Point Protocol (PPP), Multicast Point-to-Point Protocol (MPPP), Frame Relay, Multicast, High-Level Data Link Control (HDLC), Serial (RS 232, RS-449, X.21, V.35, and EIA-430), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.	10	Table 4, fila 2	Data Sheet - Cisco 2900 Series Integrated Services Routers
4.4.5 El equipo de rutado debe soportar encapsulacion Ethernet, 802.1q VLAN, Point-to-Point Protocol, Frame Relay, Multicast Point-to-Point, Multicast, 802.1q VLAN, High-Level Data Link Control (HDLC), Serial (RS 232, RS-449, X.21, V.35, and EIA-430), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.	Traffic Management, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Round Robin Scheduling (WRR), Hierarchical Queue Scheduling (HQ), Performance Routing (PFR), and Network-Based Advanced Routing (NBAR).	10	Tabla 4, fila 3	Data Sheet - Cisco 2900 Series Integrated Services Routers
4.4.6 El equipo de rutado debe soportar encapsulacion Ethernet, 802.1q VLAN, Point-to-Point Protocol, Frame Relay, Multicast Point-to-Point, Multicast, 802.1q VLAN, High-Level Data Link Control (HDLC), Serial (RS 232, RS-449, X.21, V.35, and EIA-430), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.	SNMP, RMON, Syslog, NetFlow, and TR-069. Cisco 2900 Series Integrated Services Routers also support SNMP.	10	Tabla 5, fila 5	Data Sheet - Cisco 2900 Series Integrated Services Routers
4.4.7 El equipo de rutado debe soportar encapsulacion Ethernet, 802.1q VLAN, Point-to-Point Protocol, Frame Relay, Multicast Point-to-Point, Multicast, 802.1q VLAN, High-Level Data Link Control (HDLC), Serial (RS 232, RS-449, X.21, V.35, and EIA-430), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.	Layer 3 Enhancements	23	Fila 5	Image Info c2905
4.4.8 El equipo de rutado debe soportar encapsulacion Ethernet, 802.1q VLAN, Point-to-Point Protocol, Frame Relay, Multicast Point-to-Point, Multicast, 802.1q VLAN, High-Level Data Link Control (HDLC), Serial (RS 232, RS-449, X.21, V.35, and EIA-430), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.	802.1q VLAN, Multicast, High-Level Data Link Control (HDLC), Serial (RS 232, RS-449, X.21, V.35, and EIA-430), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.	74	Fila 27	Image Info c2900
4.4.9 El equipo de rutado debe soportar encapsulacion Ethernet, 802.1q VLAN, Point-to-Point Protocol, Frame Relay, Multicast Point-to-Point, Multicast, 802.1q VLAN, High-Level Data Link Control (HDLC), Serial (RS 232, RS-449, X.21, V.35, and EIA-430), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.	All Cisco IOS/IOS-XE Integrated Services Routers offer embedded hardware encryption acceleration.	1	2	Data Sheet - Cisco 2900 Series Integrated Services Routers

2008-09-15 10:00:00 AM - 2008-09-15 10:00:00 AM - 2008-09-15 10:00:00 AM

AXTEL
Comunicate mejor.



AXTEL S.A.B. DE C.V. (AXTEL S. DE R.L. DE C.V.)
EN PARTICIPACION CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONASE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONOPAS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONDOPRO).

REQUERIMIENTOS	DESCRIPCIÓN DEL EQUIPAMIENTO	INDICADOR DEL CUMPLIMIENTO	CANTIDAD	UNIDAD DE MEDIDA	REVISIÓN DE EQUIPAMIENTO
6.4.7 Desea 5K modém, con sistema operativo multiprotocolo integrado. El equipo contará con hardware de procesamiento específico por función, con la idea de no afectar el desempeño del equipo con la adición de nuevas tarjetas, soporte a interfaces fijas tales como módems, tarjetas síncronas, síncronas, de alta velocidad (T1), Ethernet, FastEthernet, F1, F0, así como compramisn per hardware	Monitorize Performance Cisco 2500 Series ISG are highly modular systems with general types of module slots to add connectivity and services for varied branch-office network requirements. Cisco 2500 Series Integrated Services Routers deliver innovative technologies running on industry leading Cisco IOS Software. Routers offer embedded hardware encryption acceleration, voice and video-capable digital signal processor (DSP) slots, optional firewall, intrusion prevention, call scrubbing, watermark, and application services	Nombre del Documento	3	Unidad	Tabla 2, Fila 2
	Data Sheet - Cisco 2500 Series Integrated Services Routers		4	1	
	Data Sheet - Cisco 2500 Series Integrated Services Routers		1	2	
	Interfaces and Modules 2500		3	Fila 22 Fila 24 Fila 25	
	The user experience can be further enhanced through the addition of a Cisco WAAS Network Module which can be used to securely provide more advanced WAN optimization techniques such as TCP optimization, caching, compression, and application acceleration		1	1	La experiencia del usuario se puede mejorar aún más mediante la adición de un módulo de red de Cisco WAAS que se puede utilizar para proporcionar de forma segura las técnicas más avanzadas de optimización de WAN, tales como la optimización de TCP, el almacenamiento en caché, compresión, y la aceleración de aplicaciones

2010-09-08 10:00:00 - 10:00:00 AM - 10:00:00 AM - 10:00:00 AM - 10:00:00 AM



ATIL S.A.S. DE C.V. / AXCEL, S. DE R.L. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRACCIÓN DEL SERVICIO DE RED NACIONAL SE SERVICIOS INTEGRALES ADMINISTRATIVOS DE VOZ, DATOS, INTERNET Y VISION/CONSERVACIÓN PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO Y PREVISIÓN SOCIAL, LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CONSEJO", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MORTO DE PROTECCIÓN AL SABIDO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

REQUERIMIENTOS	TEMAS EN EL DOCUMENTO	MONEDA DEL DOCUMENTO	PÁGINAS	PARCHES	FECHA DEL SUPLENTE
4.4.5 Soportará el manejo de técnicas de gestión de colas como gestión de colas por prioridades, permitiendo o baja latencia y manejo de precedencia por base en interfaces como LAN para garantizar el correcto transcurso de los trámites o peticiones de datos, voz y video.	Traffic Management QoS, Class-based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PBR), and Network-Based Advanced Routing (NBAR).	Dato Sheet - Clavo 2900 Series Integrated Services Router	10	Tabla 4, fila 3	Administración de Tráfico QoS, Anclamiento Basado en Clase de Servicio, Anclamiento Equitativo (CBWFQ), Posicionamiento Algoritmo de Dirección Topológica (WRED), QoS Jerárquico, Ruteo Basado en Políticas (PBR), Buzón de Descarga (PBR), y Ruteo Avanzado Basado en Red (NBAR)
4.4.5 Los subidores soportarán protocolos VRRP, RSTP o GLBP, así como NetFlow	VRRP y Protocol Support RSTP - Hot Standby Router Protocol, Gateway Load Balancing Protocol (GLBP), Multicast NetFlow	Integra Info 42500	RS 31 30 28	Fila 5 Fila 13 Fila 6 Fila 20	Soporte a Protocolo VRRP/3 RSTP Implementado en Router de Tiempo de Espera Caliente Puerta de Balanceo de Cargas (R/B) Netflow Report

01/03

El presente documento es propiedad de ATIL S.A.S. DE C.V. y AXCEL, S. DE R.L. DE C.V. y no debe ser distribuido fuera de la organización.

Axcel
Comunicarte mejor.



AXTEL, S.A. DE C.V. JAVARTEL, S. DE R.L. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARIA DEL TRABAJO Y PREVENCION SOCIAL (STPS), LA PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJADOR (PROFEDT), LA COMISION NACIONAL DEL SERVICIO NACIONAL DE EMPLEO (CONSE), LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONSAM), EL COMITE NACIONAL MORTO DE PROTECCION AL SALARIO (COMINACOS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONDACOTI).

ITEM	DESCRIPCION DEL EQUIPO	CANTIDAD	TIPO DE EQUIPO	TIPO DE EQUIPO	TIPO DE EQUIPO	TIPO DE EQUIPO
3.4.5	El equipo propuesto cuenta con al menos 2 puertos GE del tipo 10/100/1000 (Mbps) con conectores RJ 45 en cobre	4	Total onboard WAN or LAN 10/100/1000 ports Cisco 3825E: 4	11	T802, 7, 64 S	Total de puertos WAN sobre el tipo: 10/100/1000 Cisco 3825E: 4
	Contra con puerto de consola independiente	1	Serial console port (up to 115.2 kbps) Cisco 3825E: 1	11	T802, 7, 64 S	Puerto de Consola Serial Cisco 3825E: 1
	Y tiene la capacidad de soportar las interfaces seriales como T1/E1, T3/E3, cable y fibra Gigabit Ethernet, según se requiera	1	the platform support the industry's widest range of wired and wireless connectivity options such as T1/E1, T3/E3, xDSL, copper, and fiber Gigabit Ethernet.	11	T802, 7, 64 S	Los platformas soportan la más amplia gama de la industria de opciones de conectividad por cable e inalámbricas, tales como T1/E1, T3/E3, xDSL, cobre y fibra Gigabit Ethernet.

01 03

AXTEL, S.A. DE C.V. JAVARTEL, S. DE R.L. DE C.V.
EN PARTICIPACION CONJUNTA

axtel
Comunicate mejor.

AVANZADO

ATEL S.A.B. DE C.V. AVANZADO, S. DE RL. U.C. C.V.
EN INFORMACION CONJUNTA

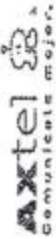
CONTRATORIO DEL SERVICIO DE RED NACIONAL DE SERVICIOS INFORMÁTICOS ADMINISTRADOS DE LOS DATOS, REDES Y TELECOMUNICACIONES PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL, REDES Y TELECOMUNICACIONES FEDERALES DE LA DEFENSA DEL TRABAJO (PROFIDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (COSENE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASALM), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAPROSA) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

REQUISITO	DESCRIPCIÓN	Unidades	Tabla 4, Fila 1 y 2	Procesos:
Debe entregar servicios tipo de estudio y protocolos como BGP, IS-IS, RFP, BPA, IGMP, ISIS, OSPF, RRMPP, IGMPv3, IGMPv3, P2P SM, SSM, DVMRP, IPSEC, GRE, BFD, así mismo debe soportar rutas estáticas	Protocolos: IPv4, IPv6, IPv6 routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Route Reflector, Intermediate System to Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPv6-to-IPv4, IPv6, SNMP, IPv6-to-IPv4 Multicast, MPLS, LTPv3, R2-1as, R02.3uh, L3 y L3 VPN, R323	10		Procesos: IPv4, IPv6, IPv6 Edición, Primera ruta más corta (OSPF), IGMP Mejorada (IGMP), Protocolo de Frontera de Estado (BGP), Activo de Terminación de Sesiones Intermedio - Sistema Intermedio (IS-IS), Protocolo de administración de grupos de Internet Multicast (IGMPv3), Protocolo Independiente Multicast de Modo Esporádico (PIM SSM), PIM fuente específica Multicast (SSM), Protocolo de Enrutamiento Multicast de Vector de Distancia (DVMRP), Multicast IPv4 a IPv6, MPLS, VPN capa 2 y capa 3, IPSEC, Protocolo de Tunneling Capa 3 versión 3 (LTPv3), Distribucional de Director de Rutas (BFD), IEEE802.3uh, and IEEE802.3uh. Encapsulaciones: Encapsulación de túnel genérico (GRE),
	Image info c3900	68	Fila 18	IP
	Image info c3800	68	Fila 19	IPV2: RFC 1724 MIB Extension
	Image info c3500	34	Fila 4	IP Enhanced IGRP Route Architecture
	Image info c3900	33	Fila 30	IGMP Func. Legue
	Image info c3500	33	Fila 34	IGMP Versión 2
	Image info c3900	74	Fila 16	SNMP (Simple Network Management Protocol)
	Image info c3900	30	Fila 17	H.323 Call Redirection Enhancement

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTERSECTORES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARIA DEL TRABAJO Y PROVISION SOCIAL (STR); LA PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJO (PRODEFET); COORDINACION DINAMICA DEL SERVICIO NACIONAL DE EMPLEO (CONSENE); LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI); EL COMITE NACIONAL MEXICO DE PROTECCION AL SALARIO (CONAMPROS); Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

REQUISITOS MINIMOS	DESCRIPCION DEL SERVICIO	INDICADORES DE RENDIMIENTO	UNIDADES DE MEDIDA	TIEMPO DE RESPUESTA
6.4.6 El equipo de redes debe soportar: <ul style="list-style-type: none"> Encapsulacion Ethernet, 802.1q VLAN, PoE-to-PoE, Protocolo (PPS), Multicast Point-to-Point Protocol (MLPPP), Frame Relay, Multicast Frame Relay (MLFR) (FR 35 and FR 16), High-Level Data Link Control (HOLC), SONET (RS-232, RS-448, X.21, V.35). 	Encapsulacion Ethernet, 802.1q VLAN, Protocolo Punto-a-Punto (PPP), Protocolo Punto-a-Punto Multicast, (MLPPP), transmision de Frames, transmision de Frames Multicast (MLFR) (FR 15 and FR 16), Control de Enlace de Alto Nivel (HOLC), Serial (RS-232, RS-448, X.21, V.35)	10	Tabla 4, Tabla 2 y 3	
6.4.7 El equipo de redes debe soportar QoS, CBWFQ, NBAR, NBAR INT2 y administracion del trafico (policias a la seccion 4.3.3), SRR, Telemetry SSH, Ad como estanda por hardware.	Traffic management QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy Based Routing (PBR), Performance Routing, and NBAR, SNMP, RMON, Syslog, NetFlow, ITR-OS9 Cisco 3900 Series Integrated Services Routers also support SNMP	23	Tabla 5, Tabla 5	
6.4.8 El equipo de redes debe soportar: <ul style="list-style-type: none"> Encapsulacion Ethernet, 802.1q VLAN, PoE-to-PoE, Protocolo (PPS), Multicast Point-to-Point Protocol (MLPPP), Frame Relay, Multicast Frame Relay (MLFR) (FR 35 and FR 16), High-Level Data Link Control (HOLC), SONET (RS-232, RS-448, X.21, V.35). 	Image Info c3900 Image Info c3900	75	Tabla 7 Tabla 15	
6.4.9 El equipo de redes debe soportar: <ul style="list-style-type: none"> Encapsulacion Ethernet, 802.1q VLAN, PoE-to-PoE, Protocolo (PPS), Multicast Point-to-Point Protocol (MLPPP), Frame Relay, Multicast Frame Relay (MLFR) (FR 35 and FR 16), High-Level Data Link Control (HOLC), SONET (RS-232, RS-448, X.21, V.35). 	Cisco 3900 Series offers omnibus hardware encryption acceleration	1	2	

Nota: El equipo de redes debe soportar los siguientes requisitos:



AXTEL, S.A.B. DE C.V. JAWANTE, S. DE R.L. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (SETESA), PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONSENA), LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL #1070 DE PROTECCION AL SALARIO (CONASAL) Y EL INSTITUTO DEL PUEBLO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

Descripción del producto y características	Cantidad	Tabla 2, Fila 2	Proforma original
<p>4-4.7 Dúplex ser modular, con sistema operativo multiprotocolo integrado. El equipo cuenta con hardware de procesamiento específico por función, en la idea de no afectar el desempeño del equipo con la adición de nuevas servicios. Separar interfaces (tarjetas) como: módulos seriales, sistemas, analógicos, de alta velocidad (AT), Ethernet, Fast Ethernet, Fx, PRI, así como compression por software.</p>	3	3	<p>Proforma original</p> <ul style="list-style-type: none"> Los routers de la serie Cisco 3900 son plataformas altamente modulares con varias tipos de puertos para estables de añadir conectividad y servicios para diversos requisitos de la red de corporación.
<p>Cisco 3900 Series Integrated Services Routers deliver innovative technologies supporting an industry-leading Cisco IOS Software.</p>	5	2	<p>Cisco 3900 Series Integrated Services Routers ofrecen tecnologías innovadoras que se ejecutan en el software Cisco IOS líder en la industria.</p>
<p>The Cisco 3900 Series offers embedded hardware encryption acceleration, video- and video capable DSP units, optional IPsec, intrusion prevention, call processing, voicemail, and application services.</p>	1	2	<p>La serie Cisco 3900 ofrece una aceleración de cifrado de hardware integrada, la voz y los sistemas de DSP con capacidad de vídeo, servidor de seguridad de aplicación, prevención de intrusiones, procesamiento de llamadas, correo de voz y servicios de aplicación.</p>
<p>T1, E1, and G.703 Multiflex Trunk Voice and WAN Interface Card Ethernet Switch Channelized T1/E1 and SON PRI</p>	3 3 5	Fila 22 Fila 14 Fila 25	<p>T1, E1, y G.703 Multiflex Trunk Voz y tarjetas de Interfaz WAN Conmutador Ethernet Canalizado T1/E1 y SON PRI</p>
<p>You can further enhance user experiences by adding a Cisco Wide Area Application Services (WAAS) Network Module to securely provide more advanced WAN optimization techniques such as TCP optimization, caching, compression, and application acceleration</p>	8	3	<p>Puede mejorar aún más la experiencia del usuario mediante la adición de Cisco Wide Area Application Services de Módulo de red (WAAS) para proporcionar de forma segura las técnicas más avanzadas de optimización WAN como lo optimización TCP, almacenamiento en caché, compresión y aceleración de aplicaciones</p>

3. Anexo 1, folio 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100

AXTEL S.A.
Comunicación mejor.

AVANZADA

AXTEL S.A.B. DE C.V. AXTEL, S. DE R.L. DE C.V.
EN PARTICIPACIÓN CONTINUA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL, AFIPREVET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL, AFIPREVET Y VIDEOCONFERENCIA, PARA LA DEFENSA DEL TRABAJO (PROFIDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (COSENE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (COMISARMI), EL COMITÉ NACIONAL JUNTO DE PROTECCIÓN AL SALARIO (COMISARPROSA) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONANCOCI)

REQUISITOS	DESCRIPCIÓN DEL SERVICIO	CANTIDAD	REFERENCIAS	DETALLES
4.4.3 Soportará el manejo de técnicas de gestión de redes como gestión de redes por análisis, personalizadas o bajo demanda y manejo de procedimientos de venta en interfaces WAN como LAN para garantizar el correcto funcionamiento de los frames o paquetes de datos, voz y video.	<p>Tráfico Impresionant</p> <ul style="list-style-type: none"> QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing, and NSAR. 	30	Tabla 4, fila 3	<p>Administración de tráfico QoS, Encolamiento Basado en Clase de Ponderamiento Equitativo (CBWFQ), Ponderamiento Algorítmico de Detección Temprana (WRED), QoS Jerárquico, Ruteo Basado en Política (PBR), Ruteo de Desempeño y NSAR</p>
4.4.9 Las mutaciones operacionales propuestas VRRP, HSRP o GLBP, así como NetFlow	<p>Virtual Router Redundancy Protocol (VRRP), HSRP - Hot Standby Router Protocol, Gateway Load Balancing Protocol (GLBP), NetFlow</p>	<p>85 31 30 58</p>	<p>Fila 12 Fila 14 Fila 8 Fila 16</p>	<p>Procedimiento de redistribución de enrutador virtual HSRP, Protocolo de Reserva de Tiempo de Espera Culleneti Puerta de balanceo de enlaces (GLBP) Netflow</p>

Atentamente

Bajo protesta de decir verdad
Jorge Vicente Martínez Rendón
Representante Común

México, D.F., a 19 de Diciembre de 2013

PROPUESTA TECNICA

PROPUESTA INDIVIDUAL () PROPUESTA CONJUNTA (X)

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGSNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

5. SERVICIOS ADMINISTRADOS DE INTERNET DEDICADO PARA LA CONVOCANTE

5.1 ASPECTOS GENERALES QUE OFERTA AXTEL PARA LA RED DE INTERNET

5.1.1 AXTEL se compromete a instalar los servicios de Internet Dedicado en las oficinas que se indican en el Anexo "B", donde se especifica el ancho de banda requerido para la operación inicial. AXTEL se compromete a entregar un servicio de acceso dedicado a Internet simétrico, con la finalidad de proporcionar servicios de navegación Web, transferencia de archivos vía FTP, correo electrónico externo, así como el acceso a los distintos servicios y sistemas de la Convocante.

La información Técnica de los equipos propuestos para esta solución se encuentra detallada en la Carpeta 2 sección Referencias Técnicas Internet Dedicado.

5.1.2 El servicio de Internet AXTEL compromete a entregarlo mediante un acceso dedicado, exclusivo para la Convocante en cada una de las oficinas mostradas en el Anexo "B" para que reciban el Internet de manera directa (diferente al nodo concentrador del Data Center de AXTEL) por lo que AXTEL confirma que no se presentarán servicios asimétricos, ni tampoco sobresuscritos.

5.1.3 El Internet Dedicado AXTEL se compromete a entregarlo a través de un enlace privado e independiente al de la VPN-MPLS con un ancho de banda simétrico, es decir;

full-duplex. El servicio en cada uno de estos nodos soportará un mínimo y un máximo especificados en el mismo Anexo "B".

5.1.4 El servicio de Internet Dedicado de AXTEL tiene la capacidad de que el ancho de banda es flexible, es decir; con un mínimo y un máximo a fin de que la Convocante pueda realizar incrementos o decrementos de manera escalonada conforme sus requerimientos de operación. Ejemplo: si el valor inicial solicitado es de 35 Mbps, los incrementos podrán proporcionarse de 10 en 10 Mbps hasta alcanzar los 100 Mbps, esto es; 45 Mbps, 55 Mbps, 65 Mbps, 75 Mbps, 85 Mbps, 95 Mbps y 100 Mbps.

5.1.5 Continuando con el ejemplo, si en un mes se estableció un escalón de 65 Mbps la Convocante podrá disminuir de 10 en 10 Mbps hasta el mínimo, esto es; 55 Mbps, 45 Mbps, 35 Mbps, 25 Mbps, 15 Mbps y 10 Mbps. De esta manera el ancho de banda se considera como velocidad real de transferencia de información y no como un ancho de banda multiplexado.

5.1.6 AXTEL cuenta con una conectividad al backbone de Internet en los Estados Unidos de América a través de enlaces redundantes internacionales directos de tal forma que AXTEL se compromete a proporcionar las capacidades de ancho de banda a las oficinas de la Convocante y para ello presenta a continuación el mapa de la República Mexicana y los Estados Unidos que muestra la topología de interconexión entre su red de Internet y los puntos de conexión a Internet en los Estados Unidos.

CONECTIVIDAD DE LA RED DE AXTEL AL BACKBONE DE INTERNET EN LOS ESTADOS UNIDOS DE AMERICA

La red de Internet de AXTEL es un backbone dedicado exclusivamente a transporte IP (Internet Protocol), e integra 5 nodos "core" (Guadalajara, México, Monterrey, Torreón y Reynosa) a la red Internacional de Internet. Esto significa que un cliente conectado a la red de Axtel tiene igual capacidad que un cliente en EU conectado a VERIZON.

El backbone nacional es STM-64 (10 Gbps) en forma de anillo. Tiene 10 Giga-routers conectados directamente por fibra óptica y bajo tecnología POS (PacketOverSonet).

El backbone se integra con VERIZON (backbone "Tier 1") a través de 6 X STM16 (15 Gbps): uno conectado en Houston, Texas, y el otro en San Antonio, Texas, 3 en McAllen y uno en Miami. Esto ofrece redundancia geográfica con conexiones muy próximas a los nodos en México. Lo anterior garantizará a la CONVOCANTE diversidad de rutas para el servicio de internet, alta disponibilidad y capacidad necesaria en ancho de banda para el intercambio de tráfico IP en la red de Internet.

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOR, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (RTPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFDET), LA CONFEDERACIÓN GENERAL DEL SERVIDOR NACIONAL DE EMPLEO (CGSNE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FUNACOT).

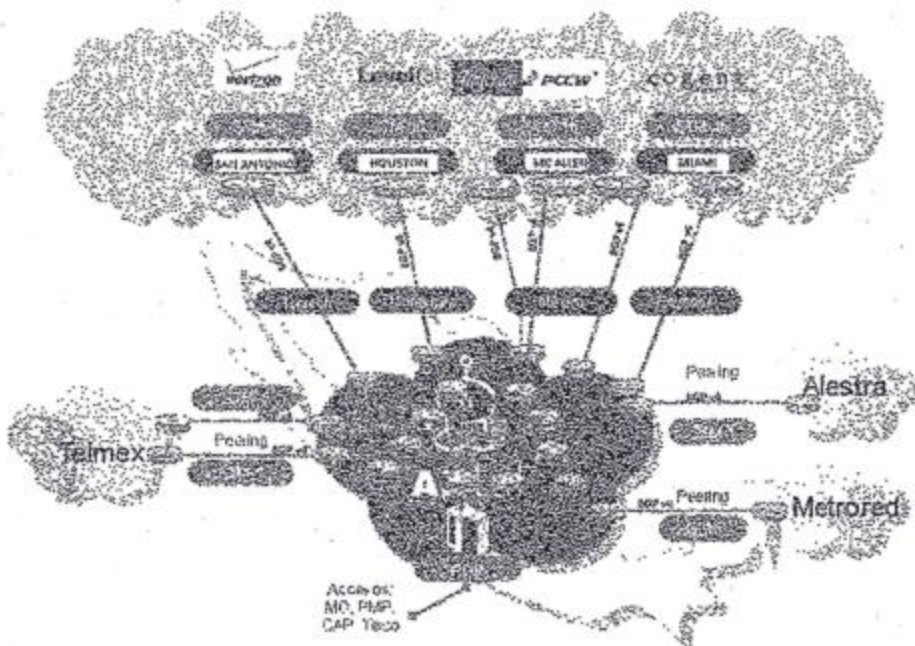


DIAGRAMA.- CONECTIVIDAD AL BACKBONE DE INTERNET EN LOS ESTADOS UNIDOS DE AMÉRICA

5.1.7 AXTEL en su topología cuenta con al menos 4 ciudades distintas de interconexión en los Estados Unidos en donde especifica sus nombres en el gráfico para garantizar la redundancia y continuidad de los servicios de sus clientes en México.

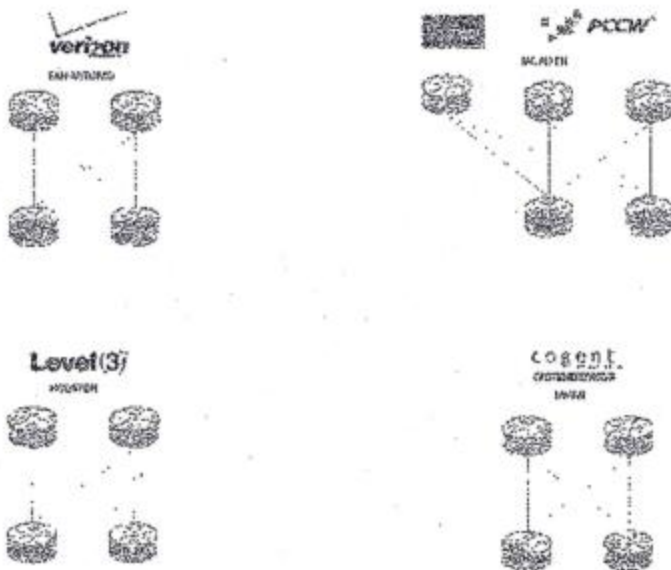


DIAGRAMA TOPOLOGIA DE CONEXIÓN

5.1.8 La capacidad total de los enlaces de conexión a Internet de AXTEL en los Estados Unidos son de al menos el equivalente a 4 veces un STM-16, es decir, al menos el equivalente a un STM-64, este dato de capacidad de conexión de los enlaces de conexión se presenta a continuación en la propuesta que oferta AXTEL a la CONVOCANTE.

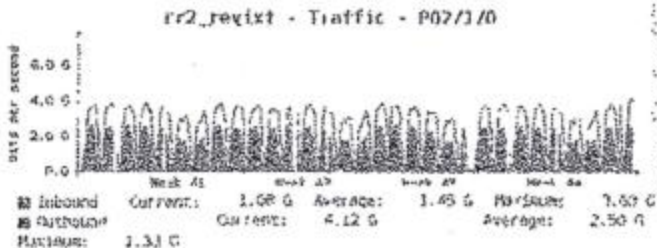
AXTEL tiene diversas conexiones de backbone el cual se integra con VERIZON (backbone "Tier 1") a través de 6 X STM16 (15 Gbps); uno conectado en Houston, Texas, y el otro en San Antonio, Texas, 3 en McAllen y uno en Miami. Esto ofrece redundancia geográfica con conexiones muy próximas a los nodos en México. Lo anterior garantizará a la CONVOCANTE diversidad de rutas para el servicio de Internet.

Alta disponibilidad y capacidad necesaria en ancho de banda para el intercambio de tráfico IP en la red de internet.

5.1.9 El porcentaje de utilización de cada uno de los enlaces de AXTEL no sobrepasa el 80%. Para la comprobación de este punto AXTEL dentro de su propuesta a continuación muestra la de los gráficos y/o estadísticas generados por la herramienta utilizadas por AXTEL en dos diferentes horas del día, a las 10am y a las 16hrs. Las pruebas y/o estadísticas se presentan a continuación:

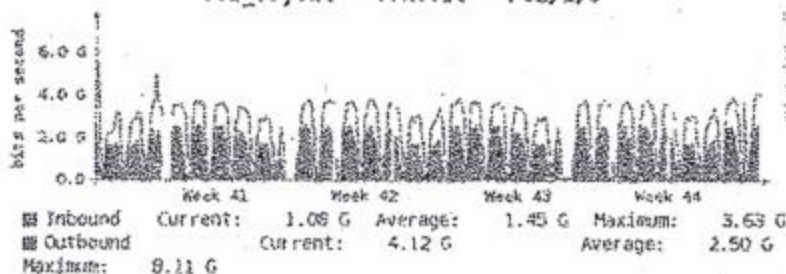
Gráficas de utilización de los enlaces. De acuerdo a las estadísticas que se presentan se puede comprobar que los enlaces de AXTEL no sobrepasan el 80% de uso en los periodos solicitados la convocante.

Level 3 STM-16 (10 A.M.)



Level 3 STM-16 (4:00 P.M.)

ri2_reyixt - Traffic - P02/1/0



5.1.10 Como ya se indicó el servicio de Internet, AXTEL se compromete a instalarlo con infraestructura independiente al servicio de VPN-MPLS, por lo que será escalable, flexible, eficiente y transparente; de tal forma que en el momento que sea necesario se puedan agregar nuevos servicios de Internet o ampliar los anchos de banda, sin afectar la operación de la red misma o la operación de los demás nodos.

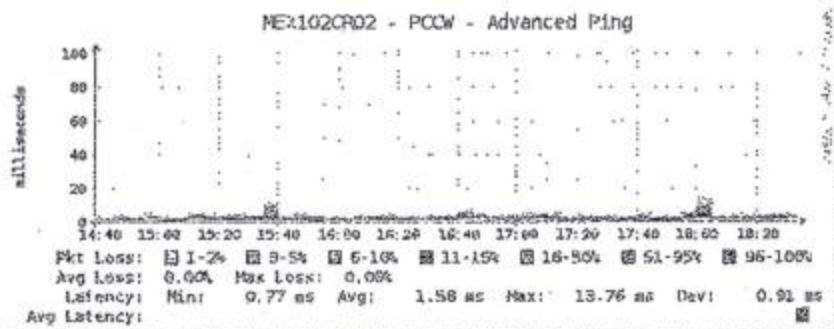
5.1.11 El servicio de Internet de AXTEL opera bajo un esquema de 7x24x365 de manera que cumple con una disponibilidad en su backbone de al menos 99.98% mensual.

5.1.12 AXTEL dentro de su propuesta técnica incluye la muestra de la comprobación de pérdida de paquetes menor a 1% de un muestreo de 1000 paquetes hacia el Tier1 internacional. Esto se comprueba a través de la prueba impresa que se generó con la herramienta con la que AXTEL llevo a cabo estas mediciones.

A continuación, se muestra la evidencia de cumplimiento del requisito del Numeral 5.1.12 en el cual se solicita que Axtel demuestro una pérdida de paquetes menor a 1% de un muestreo de 1000 paquetes hacia el Tier1 internacional. Esto se comprueba a través de una prueba impresa que genera la herramienta con la que Axtel realiza estas mediciones. La prueba impresa se presenta a continuación.

GRÁFICA DE PERDIDA DE PAQUETES.

AXTEL con la siguiente gráfica muestra la medición de pérdida de paquetes hacia la conexión de TIER1 para la conexión con PCCW, en dicha gráfica las estadísticas para pérdida de paquetes esta en 0% tanto para la pérdida promedio como para la pérdida de paquetes máxima.



Gráfica Pérdida de Paquetes

La siguiente estadística generada con la herramienta "ping" muestra que la prueba de conectividad del router PE de AXTEL en Monterrey hacia la conexión del TIER1 CONGENT no tuvo pérdida de paquetes en la secuencia de muestreo de 1000 paquetes solicitado por la CONVOCANTE.

```

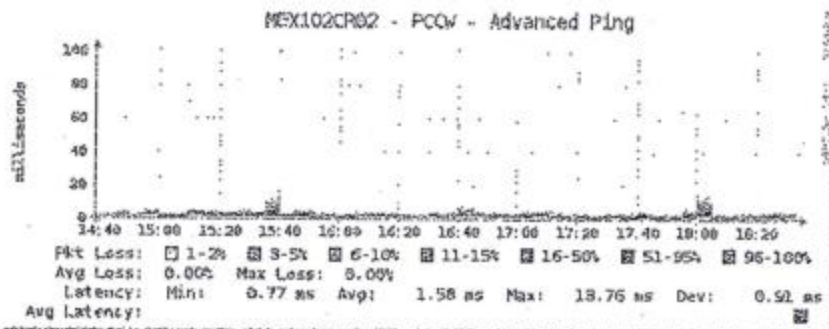
#P>/ns40>ping:caris_aymiping 26.104.197.10 source 109 count 1000
avg dac 13 17:58:04.544 CPU
Type escape sequence in abort.
Sending 1000, 100-byte ICMP Echos to 26.104.197.10, timeout is 2 seconds:
.....
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 0.77/24 ms
  
```

Estadística con herramienta PING

5.1.13 AXTEL cuenta con una latencia internacional menor a 30 mseg. Esto se comprueba a través de la siguiente gráfica que se generó con la herramienta con la que cuenta AXTEL para hacer estas mediciones. La prueba se presenta en la presente propuesta técnica. (AXTEL considera la latencia como el tiempo de respuesta en un sentido entre el Router de core de AXTEL en caso de resultar el licitante ganador y el router del Tier 1 en Estados Unidos de América).

AXTEL con la siguiente gráfica muestra la medición de la latencia internacional entre el router PE de AXTEL en la ciudad de México y la conexión hacia el TIER1 PCCW en los

Estados Unidos de América, en dicha gráfica las estadísticas para el concepto de latencia se encuentra como mínimo en: 0.77 ms, en promedio en: 1.58 ms y Máximo en: 13.76 ms, lo que da como resultado un tiempo de latencia menor al solicitado por la CONVOCANTE el cual es de 30 mseg.



Gráfica de latencia Internacional

5.1.14 AXTEL se compromete a proporcionar junto con la liberación del servicio de internet al menos 8 direcciones IP homologadas (públicas) en cada uno de las oficinas que se conecten de manera directa a este servicio y que podrán ser empleadas y publicadas en Internet durante la vigencia del contrato.

5.1.15 Para el caso particular del INSTITUTO FONACOT AXTEL se compromete a proporcionar 120 direcciones IP homologadas de una clase "C" mismas que estarán reservadas para el INSTITUTO FONACOT durante toda la vigencia del contrato. Estas direcciones IP serán asociadas, anunciadas, enrutadas e inscritas directamente en los "Global Routing Tables" de Internet

5.1.16 AXTEL para el servicio de internet se compromete a proporcionar el servicio de DNS (Domain Name Server) primario y secundario conforme los requerimientos de la Convocante.

De acuerdo a la respuesta de la pregunta 63 realizada por la empresa UNINET S.A DE C.V, de la junta de aclaraciones del día 25 de Noviembre de 2013, AXTEL considera que la convocante cuenta con los siguientes dominios: www.amutep.gob.mx, www.conasami.gob.mx, www.stps.gob.mx,

25/11/13



01 800 700 0000

AXTEL S.A.B. DE C.V./AXTEL S. DE R.L. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRATIVOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO YERREY, LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL CENTRO NACIONAL VIKO DE PROTECCIÓN AL SALARIO (CONAVIKO) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

www.profedet.gob.mx. El Instituto FONACOT cuenta con los siguientes dominios: fonacot.gob.mx, fonacot.mx e infonacot.gob.mx.

De acuerdo a la respuesta a la pregunta 64, presentada por la empresa UNINET S.A DE C.V, de la junta de aclaraciones del día 25 de Noviembre de 2013, AXTEL considera que www.stps.gob.mx, www.profedet.gob.mx. El Instituto FONACOT cuenta con los siguientes dominios: fonacot.gob.mx, fonacot.mx e infonacot.gob.mx. El Instituto FONACOT cuenta actualmente con 20 records, CONASAMI con 2 records y la STPS con 170 Records.

De acuerdo a la respuesta a la pregunta 66 presentada por la empresa UNINET S.A DE C.V, de la junta de aclaraciones del día 25 de Noviembre de 2013, AXTEL considera que el Instituto FONACOT y PROFEDET utilizan Microsoft Windows Server 2003 para sus servicios de DNS interno, la CONASAMI, STPS y CGSNE utilizan Microsoft Windows 2008.

De acuerdo a la respuesta a la pregunta 67 presentada por la empresa UNINET S.A DE C.V, de la junta de aclaraciones del día 25 de Noviembre de 2013, AXTEL considera que la convocante utiliza en sus servidores DNS internos reenviadores a los DNS públicos del actual proveedor del servicio de internet dedicado.

De acuerdo a la respuesta a la pregunta 68 presentada por la empresa UNINET S.A DE C.V, de la junta de aclaraciones del día 25 de Noviembre de 2013, AXTEL considera que la convocante no cuenta con DNS recursivo/caching, toda vez que los DNS internos utilizan reenviadores hacia los DNS públicos del actual proveedor del servicio de internet dedicado.

De acuerdo a la respuesta a la pregunta 69 presentada por la empresa UNINET S.A DE C.V, de la junta de aclaraciones del día 25 de Noviembre de 2013, AXTEL considera que la CONVOCANTE no cuenta con servidores dedicados para DNS Externos, el actual proveedor del servicio de internet ofrece el servicio de DNS externo.

5.1.17 AXTEL ratifica que el servicio de Internet que se compromete a proporcionar a la CONVOCANTE será mediante estándares internacionales de calidad, para ello proporciona certificado ISO 9001:2008 (copia) para sus soluciones de telecomunicaciones y/o tecnologías de la información.

AXTEL incluye dentro de su propuesta "Certificación ISO 9001:2008, carpeta numero 2 sección ISO 9001:2008"

5.1.18 AXTEL se compromete a llevar a cabo los requerimientos de cambios de ancho de banda, los cuales podrán ser solicitados por la Convocante en cualquier fecha durante la vigencia del servicio. Para estos casos la Convocante notificará por escrito o vía correo electrónico a AXTEL con la finalidad de realizar los ajustes técnicos necesarios, así como ajustar el cobro mensual correspondiente.

5.1.19 Para efectuar los cambios de ancho de banda ya sea aumento o disminución, **AXTEL** se compromete a un máximo de 10 días naturales a partir de la fecha de solicitud por escrito o correo electrónico por parte de la Convocante.

5.2 REQUERIMIENTOS DE ACCESO PARA INTERNET

5.2.1. Al igual que los servicios de VPN-MPLS el servicio de Internet de **AXTEL** se interconectará a las oficinas de la Convocante a través de un medio de acceso terrestre como fibra óptica.

De acuerdo a la respuesta a la pregunta 12, presentada por ALESTRA, de la junta de aclaraciones del día 25 de Noviembre del 2013, AXTEL considera que el medio de acceso sea indistinto siempre y cuando cumpla con la disponibilidad solicitada en la convocatoria, considerando el servicio de acceso y solo para los sitios de baja criticidad en un porcentaje máximo del 15% de los sitios de la STPS/PROFEDET/CGSNE, en los sitios de alta y media criticidad de la STPS/PROFEDET/CONASAM/CGSNE e INFONACOT en sus sitios remotos el enlace principal debe ser de fibra óptica y el de respaldo de fibra óptica o microonda. Para el sitio central de INFONACOT el enlace principal deberá ser de fibra óptica y el de respaldo de microonda.

5.2.2. Cada enlace de acceso de **AXTEL** se compromete a tener una disponibilidad de al menos 99.8% mensual y para ello **AXTEL**, se compromete a proporcionar dentro de los primeros 5 días hábiles del siguiente mes un reporte donde se especifiquen todas las contingencias presentadas en el mes anterior ya sea por mantenimiento preventivo, correctivo o falla en la continuidad de éste servicio. En caso de que algún evento atribuible a **AXTEL** se encuentre por debajo del valor de disponibilidad especificado será sujeto de penalización (referirse a la sección de penalizaciones).

5.2.3. En todos los casos la interfaz de entrega del servicio de conectividad a Internet **AXTEL** se compromete a proporcionarlo a través de un puerto LAN 10/100/1000 (Mbps) en RJ-45 de cobre, del equipo ruteador (CPE) el cual será independiente al de VPN-MPLS y se conectará y configurará al puerto del switch que designe la Convocante.

5.2.4. El servicio de Internet de **AXTEL** confirma que será administrado por éste, incluyendo los servicios de acceso también conocidos como última milla. En el Anexo "B" se especifican los sitios que requieren servicio de Internet Dedicado.

5.2.5. Los servicios de Internet Dedicado que oferta **AXTEL** se compromete a conservar los parámetros de criticidad, es decir; que cada uno de los enlaces se proporcionará de manera redundante, de tal forma que sólo en caso de que el enlace principal se pierda,

la redundancia deberá operar durante la ausencia del enlace principal y deberá retornar a su estado original cuando la falla del enlace principal se haya reparado.

5.2.6. Para el caso particular del INSTITUTO FONACOT, AXTEL se compromete a proporcionar redundancia del servicio de internet, siendo obligado que el enlace principal será a través de fibra óptica y el secundario por un medio distinto.

5.3 NODO CONCENTRADOR DE INTERNET EN DATA CENTER.

5.3.1 Dentro de la solución de Internet, AXTEL se compromete a proporcionar además de los nodos estratégicos con Internet Dedicado, un nodo de alta capacidad de conectividad a Internet en las instalaciones del Data Center de AXTEL que reciba el servicio y a través de la infraestructura en su ubicación se debe enrutar (enviar) el

Internet a todos los nodos de la Convocante a través de la VPN-MPLS nacional de telecomunicaciones.

5.3.2 Para el caso de los nodos estratégicos con Internet Dedicado la solución en el Data Center de AXTEL se compromete a restringir el envío de Internet por la VPN-MPLS para esos nodos (Anexo "B") y podrá activarse el envío (enrutamiento) en caso de contingencia de alguno de los nodos a petición expresa de la Convocante a través de la mesa de servicios.

5.3.3 Referente al nodo en el Data Center, antes de enviar el Internet por la VPN-MPLS nacional AXTEL se compromete a asegurarse que todo el tráfico pase por la seguridad perimetral que AXTEL se compromete a instalar y soportar con toda la capacidad del ancho de banda así como a todos los usuarios del servicio de Internet y sus incrementos.

5.3.4 AXTEL para la solución del nodo concentrador de Internet en el Data Center se compromete a entregar un CPE independiente al de la VPN-MPLS que también será instalado para llevar a cabo la conectividad entre las redes siguiendo las consideraciones de criticidad.

5.3.5 La capacidad de los equipos de ruteo de ambos servicios (Internet y VPN-MPLS) AXTEL se compromete a que soportarán los anchos de banda requeridos así como los incrementos, sin costo para la Convocante.

5.3.6 El Data Center de AXTEL cuenta con un certificado vigente de ICREA (International Computer Room Experts Association) al menos nivel 3 por lo que presenta el mismo en su oferta técnica comprobante del mismo (copia).

AXTEL incluye dentro de su propuesta "Certificado ICREA AXTEL, Carpeta 2 sección IDREA

5.4 PEERING AGREEMENTS

5.4.1. AXTEL cuenta con conexiones por lo menos de 3 proveedores (peering agreements) de acuerdo a la respuesta a la pregunta 10, presentada por AXTEL en la junta de aclaraciones celebrada el 25 de Noviembre de 2013, distintos del servicio de Internet (ISP) en México, y para ello a través de un esquema sencillo muestra las capacidades de los enlaces y los 3 proveedores señalados con los que tiene acuerdos de interconexión conocidos como Peering Agreements, a fin de evitar que la información de la Convocante se enrute hasta los Estados Unidos de América. La capacidad total de los enlaces con otros ISP de AXTEL es de al menos el equivalente a un STM-16.

ACUERDOS PEERING AGREEMENTS

AXTEL cuenta con acuerdos para el intercambio de tráfico nacional, optimizado por un acuerdo de "peering" con los principales proveedores de internet nacionales: Telmex, Alestra y Metrorred, de forma que el tráfico nacional no tenga que ser intercambiado o se enrute hasta los Estados Unidos de América,

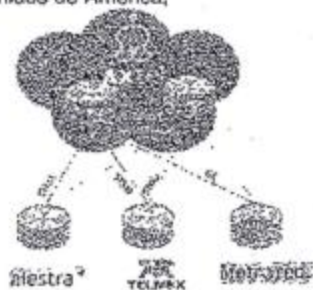


Diagrama Peerings Nacionales

5.5 EQUIPO DE RUTEO PARA LA CONECTIVIDAD A INTERNET

5.5.1. En las oficinas donde se requiere de una conectividad dedicada a Internet (nodos estratégicos) AXTEL se compromete a proporcionar en su solución el equipo de ruteo o CPE (Customer Premises Equipment).

De acuerdo a la respuesta a la pregunta No. 37 de la empresa ALESTRA S.A DE C.V. de la junta de aclaraciones del día 25 de Noviembre de 2013, AXTEL considera que no se requiere servicio de internet en el sitio 195 con el ID 199 del ANEXO "B".

5.5.2. El equipo de ruteo para conectividad a Internet, AXTEL se compromete a administrarlo y monitorearlo de manera remota a través del NOC (Network Operation Center) de AXTEL incluyendo el nodo concentrador de Internet en el Data Center.

5.5.3. El puerto LAN del equipo de ruteo que AXTEL se compromete a entregar será del tipo 10/100/1000 (Mbps) con conector RJ-45 en cobre. Cuenta con puerto de consola independiente y soporta las interfaces seriales como E1/T1, E3/T3, V.35 y cobre y fibra Gigabit Ethernet. Soporta diversos tipos de ruteo como BGP, RIP1, RIP2, IGRP, EIGRP, OSPF, IGMPv1, IGMPv2, IGMPv3, así mismo soporta ruteo estático, IPv4, IPv6 y SNMP.

5.5.4. AXTEL se compromete a que los equipos de ruteo convivirán con el direccionamiento público y/o privado que se requiera, además de soportar la configuración de NAT (Network Address Translation) y/o PAT (Port Address Translation).

5.5.5. Para el caso particular del INSTITUTO FONACOT AXTEL realizará una visita a las instalaciones del INSTITUTO FONACOT, en las fechas señaladas en el presente anexo para revisar la disponibilidad en ductos existentes y en su caso considerar la instalación de fibra óptica necesaria para llegar al centro de datos del edificio central, donde ya se cuenta con el espacio necesario, rack, energía eléctrica regulada (UPS), para los equipos de comunicaciones que soportara el servicio de Internet dedicado.

De acuerdo a la respuesta a la pregunta 123 por parte de la empresa UNINET S.A DE C.V. de la junta de aclaraciones del 25 de Noviembre de 2013, AXTEL considera realizar los trabajos o adecuaciones que se requieran para instalar los equipos para el correcto funcionamiento de su infraestructura. Para el caso del instituto FONACOT proveerá estos contactos eléctricos.

De acuerdo a la respuesta a la pregunta 21 por parte de la empresa UNINET S.A DE C.V. de la junta de aclaraciones del 26 de Noviembre de 2013, AXTEL considera que el Instituto FONACOT proveerá de contactos de energía eléctrica regulada para energizar los CPES. Por lo que se refiere a los demás organismos que integran la CONVOCANTE, AXTEL contempla todos los elementos, instalaciones y adecuaciones necesarias para cumplir con los niveles de servicio solicitados.

De acuerdo a la respuesta a la pregunta 22 por parte de la empresa UNINET S.A DE C.V. de la junta de aclaraciones del 26 de Noviembre de 2013, AXTEL contempla todos los elementos, instalaciones y adecuaciones necesarias para cumplir con los niveles de servicio solicitados. Es decisión de AXTEL la instalación del UPS y determinar los equipos que se deberán conectar a los mismos para cumplir con los niveles de servicio solicitados.

5.5.6. AXTEL se compromete a que el equipo de ruteo será nuevo, de la misma marca que el de la VPN-MPLS.

5.5.7. Para el caso particular del INSTITUTO FONACOT, los equipos de ruteo que AXTEL se compromete a entregar contarán con fuentes redundantes.

5.5.8. Para el caso particular del INSTITUTO FONACOT, el soporte técnico de AXTEL se compromete a atender las actividades para solucionar los distintos requerimientos referentes al servicio de Internet dedicado, observando como punto de marcación el puerto LAN de los equipos de ruteo. La cobertura del soporte técnico que AXTEL se comprometo a entregar será bajo un esquema de operación de 7x24.

5.5.9. Para el caso particular del INSTITUTO FONACOT AXTEL se compromete a atender en cualquier momento durante la vigencia del contrato, la implementación del protocolo IPv6, para lo cual AXTEL proporcionará lo necesario (elementos de hardware y software) así como configurar sus equipos de tal modo que establezca la

comunicación del Instituto con direccionamiento IPv6 hacia Internet. La estrategia para la migración de IPv4 a IPv6, será planeada entre personal del área técnica del INSTITUTO FONACOT y AXTEL.

De acuerdo a la respuesta a la pregunta 3 por parte de la empresa UNINET S.A DE C.V. de la junta de aclaraciones del 25 de Noviembre de 2013, AXTEL anexa la tabla en formato Excel en la cual se incluyen las referencias de los puntos indicados en el anexo técnico incluyendo las siguientes columnas: requerimiento, nombre del folleto, manual de referencia original o página WEB con su liga de la página, página del folleto, manual de referencia original o página, traducción simple al español.

AXTEL incluye dentro de su propuesta " Internet Dedicado", Carpeta 2 sección Referencias Técnicas Internet Dedicado.

DESCRIPCIÓN GENERAL DE LA SOLUCIÓN DE INTERNET PROPUESTA POR AXTEL

La red de Internet de Axtel es un backbone dedicado exclusivamente a transporte IP (Internet Protocol), e integra 5 nodos "core" (Guadalajara, México, Monterrey, Torreón y Reynosa) a la red Internacional de Internet. AXTEL proporcionará a la CONVOCANTE el servicio de acceso a internet para los 10 sitios del Anexo B, de acuerdo a las capacidades de ancho de banda especificadas en dicho documento así como al nivel de criticidad especificado por la CONVOCANTE, AXTEL considera el nivel de disponibilidad del 99.8% mensual para estos sitios, bajo un esquema de atención 7x24x365.

AXTEL ha seguido innovando respecto a los servicios de Internet; hoy que la convergencia de servicios de voz, datos y video en IP (Internet Protocol) es una realidad,

Axtel es pionero en este rubro, al manejar comercialmente los servicios de telefonía, redes VPNs (redes privadas virtuales) y acceso a Internet como una solución integral en un mismo "tubo".

Así, la operación y comunicaciones de nuestros clientes que dependen altamente de Internet están seguras y son eficientes con la Avanzada Ingeniería de Tráfico de Axtel que describimos a continuación:

AXTEL tiene diversas conexiones de backbone el cual se integra con VERIZON (backbone "Tier 1") a través de 6 X STM16 (15 Gbps): uno conectado en Houston, Texas, y el otro en San Antonio, Texas, 3 en McAllen y uno en Miami. Esto ofrece redundancia geográfica con conexiones muy próximas a los nodos en México. Lo anterior garantizará a la CONVOCANTE diversidad de rutas para el servicio de internet, alta disponibilidad y capacidad necesaria en ancho de banda para el intercambio de tráfico IP en la red de Internet.

El backbone nacional es STM-64 (10 Gbps) en forma de anillo. Tiene 10 Giga-routers conectados directamente por fibra óptica y bajo tecnología POS (PacketOverSonet).

ACUERDOS DE INTERCONEXION NACIONALES

AXTEL cuenta con acuerdos para el intercambio de tráfico nacional, optimizado por un acuerdo de "peering" con los principales proveedores de Internet nacionales: Telmex, Alestra y Metrored, de forma que el tráfico nacional no tenga que ser intercambiado o se enrute hasta los Estados Unidos de América.

AQUITECTURA DE LA RED DE INTERNET DE AXTEL

Internet es un servicio de comunicación pública el cual trabaja a través del protocolo IP como estándar mundial, enviando información desde su origen hasta su destino por diferentes routers, buscando siempre la ruta más corta disponible.

Dicha comunicación se realiza por medio de direcciones IP públicas, las cuales pueden ser en IPv4 ó IPv6, que se clasifican en:

- **Dirección IP dinámica (Solo IPv4):** La dirección dinámica es asignada una vez que se realiza la conexión a Internet permitiendo identificarme con esa dirección. Sin embargo, esta puede cambiar al generar una nueva sesión. Se requiere el uso de un servidor DHCP.

- **Dirección IP fijas (IPv4 e IPv6):** Esta IP fija son asignadas por la NIC donde establece a qué proveedor de servicios se le asignan esos rangos y las cuales están reservadas para su uso, de tal manera que solo un equipo podrá identificarse con esa dirección la red de Internet.
- **Dirección IP autoconfigurada (Solo IPv6):** La dirección autoconfigurada se conforma por un prefijo de red IPv6 proporcionado por Axtel que se complementa a la MAC address del dispositivo en cuestión. No requiere de servidor DHCP y solo entrega dirección IP mas default gateway.
- **Dirección IP dinámica DHCP-PD (Solo IPv6):** Este tipo de direccionamiento es otorgado a través de un servidor DHCP con capacidad de otorgar prefijos de IPv6 (comunemente /64) y tiene la capacidad de incluir información adicional tal y como DNSs.

A continuación se mencionan los principales componentes de la red de internet.

Equipos enrutadores del lado del cliente (CPE, Customer Premises Equipment, por sus siglas en inglés).- Este equipo es el encargado de realizar la conexión de la red del cliente hacia el primer punto de conexión a la red de internet de AXTEL.

Equipos enrutadores de acceso a la red de Internet (PE, Provider Edge router, por sus siglas en inglés).- Estos equipos son los encargados de recibir la conexión del router CPE del lado del cliente y es en el PE donde ocurrirá la mayor cantidad de procesos tanto de ruteo como de envío y recepción del tráfico de la LAN del cliente hacia el core de internet de AXTEL.

Equipos CORE red la red de Internet.- Estos equipos serán los encargados de llevar a cabo la conmutación y transporte del tráfico generado por las redes LAN de los clientes.



DIAGRAMA ARQUITECTURA INTERNET AXTEL

La red de internet de AXTEL está compuesta en su totalidad por infraestructura del fabricante Cisco Systems, líder mundial en sistema de enrutamiento. Los equipos ofertados para la interconexión de los sitios del ANEXO B que solicita la CONVOCANTE tengan una salida directa a internet por su nivel de criticidad, son del fabricante Cisco Systems lo que asegura la compatibilidad y flexibilidad para la implementación de los servicios de internet para la CONVOCANTE.

Es importante mencionar que los servicios de internet de los 10 sitios que requieren del servicio de internet excepto el nodo INFONACOT contarán con las siguientes características:

- Direcciones IPv4 Homologadas: 8 direcciones IPv4
- Ancho de Banda: De acuerdo al anexo A
- Soporte técnico: 7x24x365
- Monitoreo de uso del enlaces de internet: incluido

Para el sitio de INFONACOT

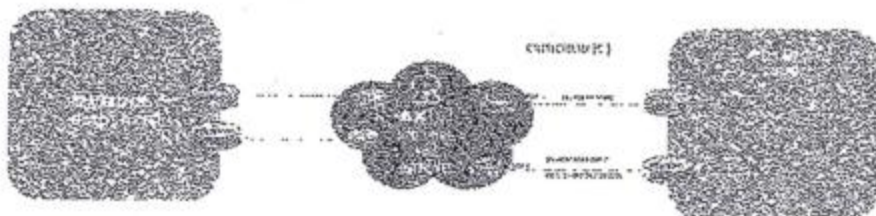
- Direcciones IPv4 Homologadas: 120 direcciones IPv4
- Ancho de Banda: De acuerdo al anexo A
- Soporte técnico: 7x24x365
- Monitoreo de uso del enlaces de internet: incluido

La siguiente tabla muestra los sitios a los que AXTEL proporcionará el servicio de internet, estos sitios están relacionados en el anexo B, indicando el ancho de banda y tipo de criticidad del nodo.

No.	ID STPS	ENTIDAD	UNIDAD	CIUDAD	ESTADO	CRITICIDAD	INTERNET (Ancho de Banda)	
							Inicial (Mbps)	Mínimo M (piso)
42	193	CONASAMI	CONASAMI	México	D.F.	C	4	4
44	198		REFORMA 93	México	D.F.	C	48	10
45	6	STPS	FELIX CUEVAS (CONTRALORIA)	México	D.F.	C	9	5
46	8	STPS	PERIFERICO	México	D.F.	C	18	10
47	9	STPS	AJUSCO	México	D.F.	C	18	10
49	12	STPS/ PROFEDET	J.F.C.A (AZCAPOTZALCO)	México	D.F.	C	17	10
68	1	STPS/ EMPLEO	COORDINACION GENERAL DE EMPLEO	México	D.F.	C	18	10
69	3	PROFEDET	PROFEDET	México	D.F.	C	10	5
196		FONACOT	Centro de Datos Oficinas Centrales del Instituto Fonacot	México	D.F.	C	30	10
194		Data Center	Del Proveedor			C	70	10

Tabla Anexo B Servicio de Internet

ESQUEMA DE ALTO NIVEL PARA CONECTIVIDAD DE INTERNET RESTO DE LOS SITIOS STPS



ESQUEMA DE ALTO NIVEL PARA SITIOS CRITICOS CON SERVICIO DE INTERNET E INFONACOT

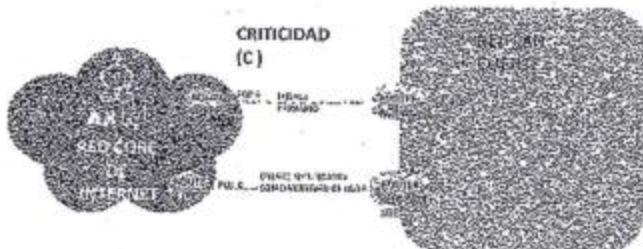


Tabla resumen de equipos a implementar para el servicio de internet.

Modelo de equipo	BOUTER INTERNET
CISCO2901/K9	3
CISCO2911/K9	1
CISCO2921/K9	4
CISCO2951/K9	1
CISCO3925E/K9	1

SERVICIO DE DNS

Con el servicio de Internet, AXTEL se compromete a proporcionar la administración de los dominios de la CONVOCANTE a través del servicio de DNS primario y secundario (Domain Name Server) los equipos servidores que darán este tipo de servicio se ubicarán en el Centro de Datos de AXTEL, con el cual se le permitirá a la CONVOCANTE la posibilidad de resolver el nombre de dominio asociado a una IP en servidores de Axtel.

Características del servicio de resolución de dominios

- Resolución directa por medio del nombre del dominio se obtiene la IP, es decir cualquier persona podrá buscar la página del cliente y con eso se direcciona a la dirección IP fija asociada.
- Resolución Inversa por medio de la IP se obtiene el nombre del dominio, bajo este esquema los usuarios pueden marcar la dirección IP fija asignada y de ahí se resuelve al nombre en el servidor.

Los siguientes dominios de la CONVOCANTE son considerados para la publicación a través del servicio de resolución de DNS de AXTEL.

www.emsac.gob.mx
www.conasami.gob.mx
www.stps.gob.mx
www.profedel.gob.mx
fonacot.gob.mx
fonacot.mx
infonacot.gob.mx

EL número de registros que AXTEL considera para implementación en los servidores de resolución de nombres son los siguientes:

- INFONACOT con 20 registros
- CONASAMI con 2 registros

- STPS con 170 registros

Atentamente

Bajo protesta de la verdad
Jorge Vicenti Méndez Rondón
Representante Común

México, D.F., a 19 de Diciembre de 2013

PROPUESTA TECNICA

PROPUESTA INDIVIDUAL () PROPUESTA CONJUNTA (X)

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGSNE", LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL MIXTO DE PROTECCION AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

6. SERVICIO ADMINISTRADO DE MODELADO DE TRAFICO Y OPTIMIZACION

6.1 ASPECTOS GENERALES QUE CUMPLIRA EL MODELADOR DE TRAFICO Y OPTIMIZACION.

6.1.1 AXTEL se compromete a proporcionar el equipamiento necesario para el monitoreo, optimización de aplicaciones y control del tráfico generado desde las localidades conectadas a la red VPN-MPLS de la STPS/CONASAMI/CONAMPROS/PROFEDET, en los nodos indicados en el Anexo "A" de la columna de modeladores, donde se especifica el ancho de banda requerido en el servicio de VPN-MPLS.

La información Técnica del equipamiento propuesto para esta solución se encuentra detallada en la Carpeta 2 sección Referencias Técnicas Modelado de Tráfico

6.1.2 La solución de AXTEL cuenta con el nivel de criticidad especificado en el mismo Anexo "A" y en consecuencia se compromete a conservar la cantidad de infraestructura requerida (modeladores redundantes).

6.1.3 Los equipos requeridos en cada localidad para la prestación del servicio AXTEL se compromete a suministrarlos, instalarlos, configurarlos y soportarlos en caso de falla y ser monitoreados por parte de AXTEL durante la vigencia del contrato.

6.1.4 AXTEL se compromete a que todos los equipos de modelado y optimización serán nuevos de la misma marca, toma en consideración que la CONVOCANTE no se aceptará

0005

soluciones con más de una marca, adicionalmente AXTEL en su propuesta técnica incluye carta del fabricante en papel membretado y firmado en fecha reciente, donde especifica que AXTEL es distribuidor autorizado por el fabricante y que cuenta con el personal técnico calificado para instalar, configurar, administrar y monitorear los equipos de modelado y optimización que serán instalados en la STPS/CONASAMI/CONAMPHOS/PROFDEFET.

Ver Carpeta 2 Sección Carta Fabricante Modelado de Tráfico y Optimización.

6.1.5 AXTEL entrega como parte de su oferta técnica documentos (copia) que comprueba la capacidad de al menos 2 ingenieros certificados en la marca del fabricante para la instalación de los equipos de modelado y optimización

Ver Carpeta 2 Sección Certificados del Fabricante.

6.1.6 AXTEL se compromete a entregar todas las funcionalidades del servicio a través de un dispositivo físico (hardware) especializado operando en cada localidad el cual es independiente del equipo de ruta. El equipo cuenta con la capacidad de procesamiento y las interfaces necesarias para prestar el servicio requerido, sin afectar o degradar la operación del servicio de la VPN-MPLS con el cual se integrará de forma transparente.

6.1.7 El uso del procesador en los equipos de modelado no excederá del 70%, los dispositivos modeladores cuentan con al menos 2 interfaces Ethernet 10/100/1000 Mbps integradas en un solo chasis para el soporte de la solución.

6.1.8 En caso de que el equipo presente fallas en su operación, se auto configurará en modo puente (bridge o bypass) para no afectar el tráfico cursado por los enlaces dedicados VPN-MPLS.

6.1.9 El equipo ofertado en cada nodo por AXTEL fue dimensionado en función del ancho de banda indicado en el Anexo "A" del enlace VPN-MPLS, considerando su capacidad para cursar tráfico simultáneo, esto es; tanto de entrada como de salida (enlaces tipo full-duplex) a la velocidad indicada.

6.2 FUNCIONALIDADES DE MONITOREO OFERTADAS POR AXTEL EN LA SOLUCIÓN DE MODELADO

6.2.1. AXTEL confirma que la solución permite la visualización del ancho de banda cursado en el enlace, indicando la cantidad de bits transmitidos y recibidos por segundo para el tráfico de entrada, salida y total, así como de la cantidad de conexiones activas.

6.2.2. La solución cuenta con la capacidad de graficar hasta los 50 protocolos, host de entrada, host de salida, conversaciones y aplicaciones que mayor tráfico cursan en el enlace.

6.2.3. La solución cuenta con la capacidad de mostrar el tráfico generado por los protocolos, host de entrada, host de salida y aplicaciones requeridos por el operador del sistema.



AXTEL S.A.R. DE C.V./AVANTEL S. DE RL DE CV.
EN PARTICIPACIÓN JOINTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DE TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDT), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "COBANE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MEXICO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

6.2.4. Los datos podrán ser visualizados en modo de tiempo real con muestreos de al menos cada 30 segundos por las 2 últimas horas y en modo de largo plazo con muestras mínimas de 1 hora. La aplicación tiene la opción de indicar el periodo a graficar y poder seleccionar horarios específicos por cada día dentro del periodo seleccionado.

6.2.5. La solución cuenta con la capacidad para detectar automáticamente las aplicaciones cursadas en la red por firma o protocolo, así como su clasificación y visualización, indicando el ancho de banda utilizado en tiempo real e histórico.

6.3 FUNCIONALIDADES DE CONTROL OFERTADAS POR AXTEL A LA CONVOCANTE EN LA SOLUCIÓN DE MODELADO

6.3.1. La solución ofertada por AXTEL, se compromete a tener la capacidad de asignar dinámicamente un ancho de banda y prioridad por IP, rango de IPs, subredes por tipo de aplicación, garantizando la calidad en el servicio requerida para la transmisión de voz, vídeo y datos generados por las aplicaciones sustantivas de la STPS/CONASAMI/CONAMPROS/PROFEDET.

6.3.2. La solución tiene la capacidad de bloqueo de aplicaciones no deseadas.

6.3.3. AXTEL confirma que el control será aplicado al tráfico de entrada y de salida, de manera simétrica o asimétrica según sea el caso.

6.3.4. Las políticas de calidad en el servicio serán asignadas en los periodos de tiempo determinados por la STPS/CONASAMI/CONAMPROS/PROFEDET.

6.3.5. La relación de aplicaciones permitidas, prioridades requeridas y aplicaciones bloqueadas, será proporcionada por la STPS/CONASAMI/CONAMPROS/PROFEDET a AXTEL, al inicio del periodo de implementación de los servicios y podrán ser modificadas a lo largo de la vigencia del contrato a solicitud expresa de la STPS/CONASAMI/CONAMPROS/PROFEDET vía correo electrónico a la Mesa de Servicios sin cargo adicional para la STPS/CONASAMI/CONAMPROS/PROFEDET.

6.4 CONSOLA CENTRAL DE ADMINISTRACIÓN DE MODELADO PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET

6.4.1. Para la totalidad de equipos de modelado requeridos AXTEL se compromete a administrarlos a través de una única consola central de administración, la cual está considerada dentro de la propuesta de AXTEL a la CONVOCANTE, desde donde se podrá visualizar el estado activo/inactivo de cada dispositivo, generar gráficas, aplicar políticas de calidad en el servicio, políticas de optimización y enviar actualizaciones de software, así como configurar y recibir alertas de cada equipo operando como parte de la solución.



AGC, S.A.B. DE C.V./AVANTEL, S. DE R.L. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (COGNE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MEXICANO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONAOCT).

6.4.2. AXTEL se compromete a que la consola será ingresada por personal del NOC / SOC de AXTEL, vía la red VPN-MPLS y el hardware requerido para su operación se ubicará físicamente en las instalaciones de AXTEL.

6.4.3. Se tendrá la capacidad de exportar las gráficas generadas a un formato PDF y de generar reportes de tráfico cursado por los host, aplicaciones y protocolos definidos por el usuario de la consola, en el periodo de tiempo y resolución de datos indicados.

6.4.4. AXTEL se compromete a asignar cuentas concurrentes de usuario para su acceso con los permisos necesarios para generar las gráficas y los reportes requeridos como parte de la solución.

6.5 ACEPTACIÓN DEL SERVICIO DE MODELADO PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET

6.5.1. AXTEL considera que el Servicio de Modelado de Tráfico se dará por aceptado en cada localidad al cumplir la totalidad de las condiciones siguientes:

- AXTEL se compromete a que el equipo modelador de tráfico llevará a cabo el monitoreo, control del tráfico y optimización solicitados en el presente anexo técnico.
- El equipo de modelado de tráfico se muestra activo y es administrable a través de la consola central.
- Se cuenta con el acceso a la consola central de administración por el personal de NOC / SOC de AXTEL.

6.6 AFECTACIÓN DEL SERVICIO DE MODELADO PARA STPS/CONASAMI/CONAMPROS/PROFEDET

6.6.1. AXTEL queda en el entendido de que el Servicio de Modelado de Tráfico será considerado afectado en cada localidad al presentarse una o más de las condiciones siguientes:

- El equipo modelador de tráfico no lleva a cabo el monitoreo y/o el control del tráfico y/o la optimización solicitados en el presente anexo técnico.
- El equipo de modelado de tráfico no se muestra activo en la consola central de administración.
- El equipo de modelado no es administrable a través de la consola central de administración.
- No se cuenta con el acceso a la consola central de administración.
- El equipo de modelado opera en modo puente (bridge).

6.7 PROTOCOLOS Y APLICACIONES

6.7.1. Los equipos de modelación de tráfico ofertados por AXTEL tienen la capacidad de poder detectar las siguientes aplicaciones y protocolos bajo estas categorías:

- P2P (point to point): BitTorrent, eDonkey, Ares, Gnutella, Thunder, Winny, eMule, Vuze.
- VoIP y Mensajería Instantáneas: Windows Live Messenger, SIP, Skype, Yahoo Messenger, GoogleTalk, Fring, WhatsApp, STUN, ICQ, Viber, y GQ.



AXTEL, S.A.B. DE C.V. (AXTEL, S. DE RL. DE C.V.)
EN PARTICIPACIÓN CONJUNTA

CONTINACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFIDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONASEM), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAM), EL COMITÉ NACIONAL MEXICO DE PROTECCIÓN AL SALARIO (CONAMPRO) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

- c) Juegos: World of Warcraft, Final Fantasy, Guitar Hero, Second Life, QQ Games, League, CounterStrike, Call of Duty, Apple Game Center.
- d) WEB: HTTP, mobile y redes sociales como Facebook.
- e) Aplicaciones Streaming: YouTube, RTMP, QQ live, PPStream, DailyMotion, HTTP streaming, HTTP audio, NetFlix, y Facebook streaming, Claro Video y VuDu
- f) Transferencia de archivos: FTP, HTTP file downloads, Apple App Store y Android Market.

De acuerdo a la respuesta a la pregunta 3, presentada por UNINET S.A. DE C.V., de la Junta de Aclaraciones celebrada el 25 de Noviembre del 2013, AXTEL anexa tabla en formato Excel en el cual se incluye la referenciación de los puntos indicado en los anexos técnicos incluyendo las siguientes columnas: nombre del folleto, manual de referencia original o página web con liga de la página, página del folleto, manual de referencia original o página traducción simple al español.

Ver carpeta 2 sección Referencias Técnicas Modelado de Tráfico

DESCRIPCIÓN GENERAL DE LA SOLUCIÓN DE MODELADO DE TRAFICO PROPUESTO POR AXTEL

La solución de administración de modelado de tráfico y optimización propuesta por AXTEL es una solución basada en hardware de propósito específico de la marca Blue Coat modelo Packet Shaper, capaz de controlar los anchos de banda en la capa de aplicaciones o Capa 7 donde de forma dinámica se logra ajustar los anchos de banda de cada aplicación que cruce por los sitios de la red MPLS que cuentan con este tipo de solución de acuerdo al ANEXO "A" de la CONVOCANTE dentro de cada una de las calidades de servicio proporcionadas a la Secretaría, esto es: En Calidad de Servicio de Datos Críticos es posible controlar y garantizar el ancho de banda de cada sesión de los aplicativos críticos de la Secretaría y priorizar los más críticos de los menos críticos, en el caso de la Calidad de Voz y Video se garantizará el ancho de banda necesario para que cada llamada o sesión de video tenga los recursos necesarios para operar correctamente ya que al ser un protocolo sensible al retardo, retransmisiones y pérdida de paquetes el control por sesión y ancho de banda es indispensable. En las áreas de trabajo que se tendrán con la CONVOCANTE se definirán a detalle las aplicaciones que de acuerdo a la prioridad y a las funciones del negocio de la CONVOCANTE se tomaran en consideración para el modelado de tráfico y optimización de dichas aplicaciones.

En el caso de Datos Normales o Best Effort, normalmente se asigna la navegación a Internet, correo electrónico web y en general cualquier aplicativo que utilice HTTP o HTTPS, en este caso la solución ofertada permitirá generar circuitos virtuales por cada aplicativo que cruce sobre estos protocolos vía web, de tal forma que se logra proteger a los aplicativos más importantes para la Secretaría del tráfico recreativo o no importante garantizando un ancho de banda mínimo y reservado para su correcta operación.

La topología de la solución propuesta de acuerdo a las mejores prácticas de instalación de este tipo de equipos por parte del fabricante se podrá llevar a cabo entre el router CPE de la MPLS y el Switch LAN de cada nodo que solicite el servicio, la forma de implementación es transparente en línea mediante una tarjeta tipo Bridge con capacidad de Pass-Thru o Bypass donde, en caso de falla del equipo la tarjeta entra en modo de Bypass sin afectar el servicio del nodo de MPLS,



AXTEL, S.A.B. DE C.V./AVANTE!, S. DE RL. DE C.V.
EN PARTICIPACION CONJUNTA

CONTINUACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS) LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFDEFET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "COGEM", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MEXICO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

únicamente se pierde la funcionalidad de Asignación Dinámica de Ancho de Banda quedando las 3 calidades de servicio ofertadas dentro de la red MPLS.

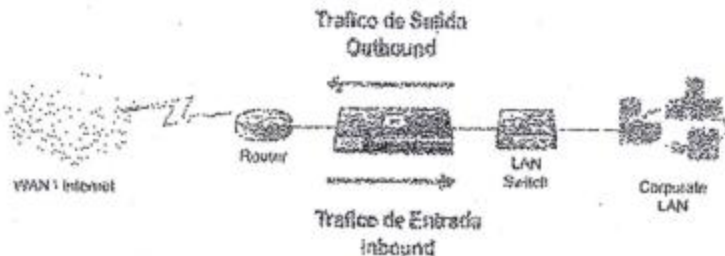


DIAGRAMA DE LA SOLUCIÓN

Atentamente

Bajo protesta de decir verdad
Jorge Vicente Mejía Rendón
Representante Común



MÉXICO, D.F. A 19 DE DICIEMBRE DE 2013

SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y
SERVICIOS GENERALES
DIRECCIÓN DE ADQUISICIONES Y ALMACENES
AVENIDA ANILLO PERIFÉRICO SUR No 4271,
NIVEL 5, EDIFICIO "B", COL. FUENTES DEL PEDREGAL
C.P. 14140, MÉXICO, D.F.

DANIEL CASADOS ROSAS, EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA BLUE COAT MEXICO S. DE R.L. DE C.V., BAJO PROMESA DE DECIR VERDAD, Y EN RELACIÓN AL PROCESO DE ADJUDICACIÓN DIRECTA, OFICIO No. 512.1/16-12-2013/1081 BIS, REFERENTE AL SERVICIO DE CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO Y PREVISIÓN SOCIAL (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGSNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT), MANIFESTAMOS QUE AXTEL, SAB DE CV, ES DISTRIBUIDOR AUTORIZADO Y QUE CUENTA CON EL PERSONAL TÉCNICO CALIFICADO PARA INSTALAR, CONFIGURAR, ADMINISTRAR Y MONITOREAR LOS EQUIPOS DE MODELADO Y OPTIMIZACIÓN QUE SON INSTALADOS EN LA STPS/CONASAMI/CONAMPROS/PROFEDET.

EXTENDEMOS LA PRESENTE A PETICIÓN DE AXTEL, SAB DE CV, Y PARA LOS FINES QUE JUZGUE CONVENIENTES.

ATENTAMENTE

DANIEL CASADOS ROSAS

REPRESENTANTE LEGAL

BLUE COAT MEXICO S DE R.L. DE C.V.

daniel.casados@bluecoat.com

+52 (56)33005800

México, D.F., a 19 de Diciembre de 2013

PROPUESTA TÉCNICA

PROPUESTA INDIVIDUAL () PROPUESTA CONJUNTA (X)

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGSNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

7. SERVICIOS ADMINISTRADOS DE SEGURIDAD PERIMETRAL PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET

7.1 CONSIDERACIONES GENERALES PARA LOS SERVICIOS DE SEGURIDAD PERIMETRAL

7.1.1 AXTEL se compromete a proporcionar los servicios administrados de seguridad perimetral que incluyen los siguientes servicios: Firewall, IPS y Filtrado de Contenido, los cuales contarán con los Firmware y el sistema operativo más actualizado liberados por el fabricante al momento de su instalación.

De acuerdo a la respuesta a la pregunta técnica 88, presentada por UNINET S.A. DE C.V., de la Junta de Aclaraciones celebrada el 28 de Noviembre del 2013, AXTEL NO considera el aprovisionamiento de equipos Firewall, IPS, Filtrado de contenido y Modelado de Tráfico en el sitio FONACOT (Centro de Datos Oficinas Centrales del Instituto Fonacot)

7.1.2 En el caso del nodo concentrador que cuenta con conectividad a Internet Dedicado en el Data Center de AXTEL, la solución de seguridad perimetral ofertada por AXTEL se compromete a habilitarla en alta disponibilidad del tipo activo-activo para todos sus servicios indicados en el punto anterior.

La información Técnica de los equipos propuestos para esta solución se encuentra detallada en la Carpeta 2 sección Seguridad Perimetral.

7.1.3 Para las oficinas que cuenten con una conectividad directa al servicio de Internet (nodos estratégicos) AXTEL también se compromete a habilitar el servicio de seguridad perimetral

administrada, en alta disponibilidad, la ubicación de los nodos que AXTEL consideró para la elaboración de su propuesta aparecen en el Anexo "B".

7.1.4 Los servicios del tipo Activo-Activo que conforman la solución de seguridad perimetral administrada, AXTEL se compromete a entregarlos en dispositivos appliance basados en un sistema propietario del mismo fabricante y de última generación.

De acuerdo a la respuesta a la pregunta técnica 13, presentada por UNINET S.A. DE C.V., de la Junta de Aclaraciones celebrada el 26 de Noviembre del 2013, AXTEL considera que los servicios de Firewall, IPS y Filtrado de Contenido, se pondrán integrar en un solo equipo, siempre y cuando se cumplan los niveles de servicio y características solicitadas.

7.1.5 Cada uno de los elementos que conforman la solución de seguridad perimetral administrada AXTEL se compromete entregarlos nuevos y de la misma marca. AXTEL considera que la CONVOCANTE no se aceptará soluciones con más de una marca, adicionalmente AXTEL dentro de su propuesta técnica entrega carta del fabricante en papel membretado y firmado en fecha reciente, donde especifica que AXTEL es distribuidor autorizado por el fabricante y que cuenta con el personal técnico calificado para instalar, configurar, administrar y monitorear los elementos de seguridad perimetral que serán instalados

Ver Carpeta 2 sección Carta Fabricante Seguridad Perimetral.

7.1.6 AXTEL dentro de su propuesta técnica integra los documentos (copia) que comprueba la capacidad de al menos 2 ingenieros certificados en la marca del fabricante para la instalación de la solución de seguridad perimetral.

Ver Carpeta 2 sección Certificados del Fabricante.

7.1.7 AXTEL se compromete a que Cada uno de los servicios (Firewall, IPS y Filtrado de Contenido) de la solución de seguridad perimetral, será administrada y monitoreada de manera remota a través del SOC (Security Operation Center) de AXTEL.

7.2 SERVICIO ADMINISTRADO DE FIREWALL EN NODO DATA CENTER PARA LA STPS/CONASAMI/CONAMPROS/PROFEDT

7.2.1. Para el caso del servicio de Firewall en el nodo concentrador de Internet, en el Data Center de AXTEL. AXTEL se compromete a proporcionar una solución redundante en Firewall, la cual estará basada en un dispositivo appliance, AXTEL contempla que la CONVOCANTE no se aceptará ninguna solución exclusiva por software y AXTEL confirma que la solución ofertada cuenta con sistema operativo propietario.

De acuerdo a la respuesta a la pregunta técnica 13, presentada por UNINET S.A. DE C.V., de la Junta de Aclaraciones celebrada el 26 de Noviembre del 2013, AXTEL considera que



AXTEL, S.A.B. DE C.V./AVANTEL, S. DE RL DE CV.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE IED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS OR VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDT), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONSEMP), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MEXICO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

los servicios de Firewall, IPS y Filtrado de Contenido, se podrán integrar en un solo equipo, siempre y cuando se cumplan los niveles de servicio y características solicitadas.

7.2.2. AXTEL se compromete a entregar los puertos LAN del equipo firewall en 10/100/1000 (Mbps) con conector RJ-45 en cobre

7.2.3. AXTEL confirma que el equipo firewall ofertado cuenta con al menos 3 certificaciones como ICSA Labs, FIPS 140/2, EAL4 o NSS Labs y cuenta con la capacidad de manejo de tráfico para maximizar la limitación del ancho de banda, ruteo dinámico con protocolos OSPF y BGP, ECMP, soporte a VLANs (802.1q) y ruteadores virtuales, dominios virtuales o la capacidad de crear equipos lógicos.

7.2.4. Así mismo AXTEL confirma que el equipo firewall cuenta con métodos de autenticación requeridos para el Gateway, base de datos interna e interconstruida, RADIUS, RSA SecurID, LDAP.

De acuerdo a la respuesta a la pregunta 103, presentada por UNINET S.A. DE C.V., página 6, de la Junta de Aclaraciones celebrada el 25 de Noviembre del 2013, AXTEL considera que autenticación interconstruida se refiere a una base de datos interna, dentro del Firewall, que no dependa de algún elemento externo.

7.2.5. AXTEL se compromete a entregar las funcionalidades del firewall con un número de sesiones simultáneas procesadas de al menos 28 millones de sesiones, el throughput o rendimiento de al menos 60 Gbps, la solución soporta un mínimo de 200 routers virtuales o dominios virtuales, y más de 210,000 nuevas sesiones por segundo

7.2.6. AXTEL confirma que el firewall tiene la capacidad de manejo de túneles de VPN, por lo que soporta hasta 8,000 túneles de VPN, con throughput de 20 Gbps en modo de VPN (3DES).

7.3 SERVICIO ADMINISTRADO DE IPS (SISTEMA DE PREVENCIÓN DE INTRUSOS) EN NODO DATA CENTER PARA LA STPS/CONASAMI/CONAMPROS/PROFEDT

7.3.1. Para el caso de la solución de IPS (Intrusion Prevention System) en el nodo concentrador de Internet, en el Data Center de AXTEL, AXTEL se compromete a entregar una solución redundante, la solución está basada en un dispositivo appliance, AXTEL considera que la convocante no aceptará ninguna solución exclusiva por software y AXTEL confirma que la solución a ofertar cuenta con sistema operativo propietario.

De acuerdo a la respuesta a la repregunta técnica 13, presentada por UNINET S.A. DE C.V., de la Junta de Aclaraciones celebrada el 25 de Noviembre del 2013, AXTEL considera que los servicios de Firewall, IPS y Filtrado de Contenido, se podrán integrar en un solo equipo, siempre y cuando se cumplan los niveles de servicio y características solicitadas.

7.3.2. AXTEL confirma que los puertos LAN del equipo IPS son del tipo 10/100/1000 (Mbps) con conector RJ-45 en cobre.

7.3.3. El equipo IPS ofertado por AXTEL confirma que bloqueará diferentes tipos de tráfico peer-to-peer, el equipo es capaz de controlar: kaza, morpheus, imesh, edonkey, limewire, boarsshare entre otros; el sistema opera en línea, AXTEL confirma que el sistema no requiere ningún direccionamiento IP en los puertos de inspección, AXTEL confirma que el sistema soporta un rendimiento de inspección de 14 Gbps como mínimo, el sistema maneja al menos 28,000,000 de sesiones (conexiones bidireccionales) y soporta al menos 210,000 nuevas conexiones por segundo con una latencia de menos de 5 microsegundos.

7.3.4. La solución ofertada por AXTEL incluye Anti-DDoS para mitigar este tipo de ataques, el equipo tiene filtros para detectar y bloquear spyware, el equipo es capaz de bloquear y/o administrar el ancho de banda que utilizan las aplicaciones point-to-point y cuenta con servicio de actualización durante la vigencia del contrato.

7.3.5. El sistema cuenta con diferentes perfiles de seguridad por cada segmento y estos segmentos se podrán agrupar de diversas maneras según sea necesario, el control de acceso se puede limitar por perfil, dispositivo o segmento de red.

7.4 SERVICIO ADMINISTRADO DE FILTRADO DE CONTENIDO EN NODO DATA CENTER PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET

7.4.1. Para el caso de la solución de Filtrado de Contenido en el nodo concentrador de Internet, en el Data Center de AXTEL, AXTEL considera la solución redundante, y basada en un dispositivo appliance, AXTEL considera que la CONVOCANTE no se aceptará ninguna solución exclusiva por software.

De acuerdo a la respuesta a la pregunta técnica 13, presentada por UNINET S.A. DE C.V., de la Junta de Aclaraciones celebrada el 26 de Noviembre del 2013, AXTEL considera que los servicios de Firewall, IPS y Filtrado de Contenido, se podrán integrar en un solo equipo, siempre y cuando se cumplan los niveles de servicio y características solicitadas.

7.4.2. AXTEL confirma que los puertos LAN del Filtrado de Contenido son del tipo 10/100/1000 (Mbps) con conector RJ-45 en cobre.

7.4.3. AXTEL como parte de su oferta se compromete a entregar el Filtrado de Contenido para la navegación de 6,036 (seis mil treinta y seis) usuarios al inicio del servicio en el sitio de Internet de alta capacidad, sin embargo, AXTEL considera que el equipo soportará el crecimiento de por lo menos el 35% de usuarios sin ningún costo adicional.



AXTEL S.A.B. DE C.V./AVANTEL S. DE RL DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRATIVOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONASA), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

7.4.4. AXTEL confirma que el equipo de Filtrado de Contenido cuenta con al menos 75 categorías para una navegación segura. El equipo proporcionará un servicio de seguridad que combina medidas preventivas, proactivas y reactivas para crear una solución completa de Filtrado de Contenido Web.

7.4.5. AXTEL se compromete a bloquear el contenido ofensivo de la red, el equipo trabaja a nivel Gateway sin instalar ningún agente en los clientes finales, cuenta con listas blancas y negras, diarias y con servicio de actualización durante la vigencia del contrato. AXTEL confirma que el servicio de clasificación y categorización de URL estará basado en la nube.

7.4.6. AXTEL se compromete a que el equipo de Filtrado de Contenido realizará análisis por normas, firmas, heurística, análisis de comportamiento, servicios de reputación web y categorías de URL, Prevención de elusión de proxy, filtrado para prevenir botnets, keyloggers, phishing y spyware, identificación de contenido malicioso generado por los usuarios a medida que se publica en sitios web.

7.5 SERVICIO ADMINISTRADO DE FIREWALL EN NODOS CON INTERNET DEDICADO PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET

7.5.1. En los nodos (estratégicos) de conectividad dedicada a Internet, AXTEL se compromete a instalar un equipo Firewall administrado considerando la capacidad de ancho de banda especificada en el Anexo "B", así como el número de usuarios.

7.5.2. Para el caso del servicio de Firewall AXTEL confirma que está basado en un dispositivo appliance, AXTEL considera que no se aceptará ninguna solución exclusiva por software y que el servicio de Firewall está basado en sistema operativo propietario.

De acuerdo a la respuesta a la pregunta técnica 13, presentada por UNINET S.A. DE C.V., de la Junta de Aclaraciones celebrada el 26 de Noviembre del 2013, AXTEL considera que los servicios de Firewall, IPS y Filtrado de Contenido, se podrán integrar en un solo equipo, siempre y cuando se cumplan los niveles de servicio y características solicitadas.

7.5.3. AXTEL dentro de oferta técnica/económica incluye la solución mediante un equipo UTM (Unified Threat Management).

7.5.4. AXTEL se compromete a entregar los puertos LAN del equipo firewall en velocidades del tipo 10/100/1000 (Mbps) con conector RJ-45 en cobre.

7.5.5. AXTEL confirma que el equipo firewall soporta al menos: ICSA Labs en Firewall, IPSec, IPS, SSL, VPN.

7.5.6. AXTEL confirma que las funcionalidades del firewall soportan el número de sesiones concurrentes (TCP) especificadas en el Anexo "B" según su capacidad, así como los parámetros especificados para firewall.



AXTEL S.A.B. DE C.V./AVANTEL S. DE RL. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDT), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CONSE" LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI) EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

7.6 SERVICIO ADMINISTRADO DE IPS EN NODOS CON INTERNET DEDICADO PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET

7.6.1 Para el caso de la solución de IPS (Intrusion Prevention System) AXTEL se compromete a entregarla mediante un dispositivo appliance, AXTEL considera que no se aceptará ninguna solución exclusiva por software, AXTEL confirma que la solución está basada en sistema operativo propietario.

De acuerdo a la respuesta a la pregunta técnica 13, presentada por UNINET S.A. DE C.V., de la Junta de Aclaraciones celebrada el 26 de Noviembre del 2013, AXTEL considera que los servicios de Firewall, IPS y Filtrado de Contenido, se podrán integrar en un solo equipo, siempre y cuando se cumplan los niveles de servicio y características solicitadas.

7.6.2 AXTEL confirma que la solución se proporcionará a través de un equipo UTM (Unified Threat Management).

7.6.3 En los nodos de conectividad dedicada a Internet AXTEL se compromete a instalar un equipo IPS administrado considerando la capacidad de ancho de banda especificada en el Anexo "B", así como el número de usuarios.

7.6.4 AXTEL confirma que los puertos LAN del equipo IPS son del tipo 10/100/1000 (Mbps) con conector RJ-45 en cobre.

7.6.5 AXTEL se compromete a que el equipo IPS ofertado bloqueará diferentes tipos de tráfico peer-to-peer; el sistema opera en línea, el sistema no requiere ningún direccionamiento IP en los puertos de inspección, el sistema soporta el throughput listado en el Anexo "B" en función de su capacidad.

7.6.6 AXTEL confirma que el equipo soporta DDoS para mitigar este tipo de ataques, el equipo cuenta con filtros para detectar y bloquear spyware, el equipo es capaz de bloquear y/o administrar el ancho de banda que utilizan las aplicaciones point-to-point y cuenta con servicio de actualización durante la vigencia del contrato.

7.6.7 El sistema tiene diferentes perfiles de seguridad por cada segmento y estos segmentos se podrán agrupar de diversas maneras según sea necesario, el control de acceso se puede limitar por perfil, dispositivo o segmento de red.

7.7 SERVICIO ADMINISTRADO DE FILTRADO DE CONTENIDO EN NODOS DE INTERNET DEDICADO PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET

7.7.1 AXTEL se compromete a entregar para el caso de la solución de Filtrado de Contenido una solución basada en un dispositivo appliance. AXTEL considera que la CONVOCANTE no aceptará ninguna solución exclusiva por software. AXTEL confirma que la solución está basada en sistema operativo propietario.

De acuerdo a la respuesta a la repregunta técnica 13, presentada por UNINET S.A. DE C.V., de la Junta de Aclaraciones celebrada el 26 de Noviembre del 2013, AXTEL considera que los servicios de Firewall, IPS y Filtrado de Contenido, se podrán integrar en un solo equipo, siempre y cuando se cumplan los niveles de servicio y características solicitadas.

7.7.2 AXTEL se compromete a entregar una solución habilitada mediante un equipo UTM (Unified Threat Management).

7.7.3 En los nodos de conectividad dedicada a Internet AXTEL se compromete a instalar la solución de Filtrado de Contenido administrado considerando la capacidad de ancho de banda especificada en el Anexo "B", así como el número de usuarios.

7.7.4 AXTEL confirma que los puertos LAN del equipo de Filtrado de Contenido son del tipo 10/100/1000 (Mbps) con conector RJ-45 en cobre.

7.7.5 AXTEL confirma que aunque el equipo de Filtrado de Contenido se requiere para la navegación de al menos el número de usuarios especificados en el Anexo "B"; AXTEL, dentro de su propuesta incluye el equipo con capacidad de soportar el crecimiento de por lo menos el 20% de usuarios sin ningún costo adicional.

7.7.6 AXTEL confirma que el equipo de Filtrado de Contenido ofertado cuenta con al menos 70 categorías para una navegación segura. El equipo proporcionará un servicio de seguridad que combine medidas preventivas, proactivas y reactivas para crear una solución completa de Filtrado de Contenido Web.

7.7.7 El equipo de AXTEL incluye el bloqueo del contenido ofensivo de la red, trabajando a nivel Gateway sin instalar ningún agente en los clientes finales, cuenta con listas blancas y negras, cuenta con actualizaciones al menos cada 5 minutos y con servicio de actualización durante la vigencia del contrato.

7.7.8 El equipo de Filtrado de Contenido ofertado por AXTEL para la protección realizará análisis por normas, firmas, heurística, análisis de comportamiento, servicios de reputación web y categorías de URL, Prevención de elusión de proxy, filtrado para prevenir botnets, keyloggers, phishing y spyware, identificación de contenido malicioso generado por los usuarios a medida que se publica en sitios web.

De acuerdo a la respuesta a la repregunta técnica 13, presentada por UNINET S.A. DE C.V., de la Junta de Aclaraciones celebrada el 26 de Noviembre del 2013, AXTEL considera que los servicios de Firewall, IPS y Filtrado de Contenido, se podrán integrar en un solo equipo, siempre y cuando se cumplan los niveles de servicio y características solicitadas.

Ver carpeta 2 sección "Referencias técnicas, de seguridad"

DESCRIPCION GENERAL DE LA SOLUCION DE SEGURIDAD PERIMETRAL OFERTADA POR AXTEL

Con el objetivo de dar cabal cumplimiento a los requerimientos solicitados en el documento Técnico del Proceso de Adjudicación Directa de la Secretaría de Trabajo y Previsión Social en lo sucesivo "STPS", AXTEL pone a consideración de STPS la siguiente Propuesta Técnica.

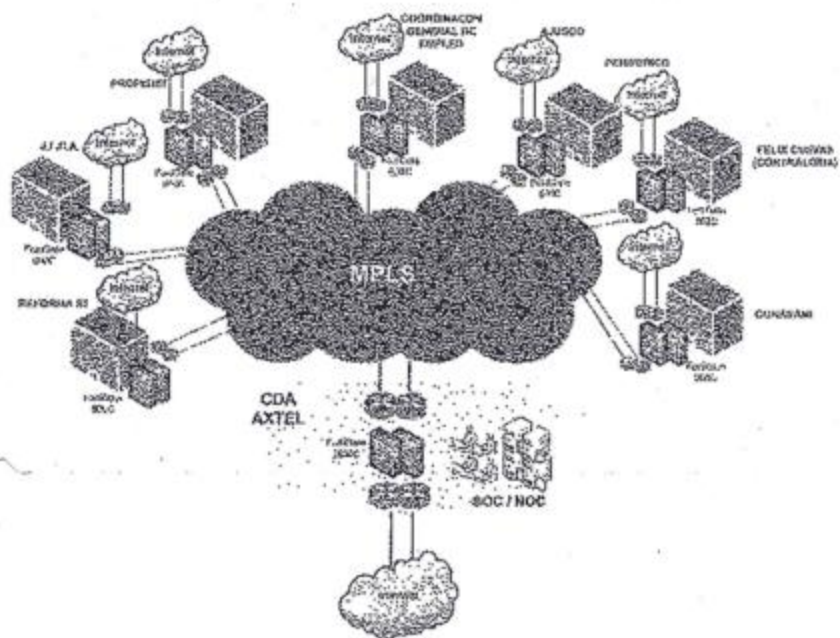
Respecto a los Servicios de Seguridad Perimetral AXTEL considero en su propuesta equipamiento de la Marca Fortinet líder a Nivel Mundial en el mercado de Seguridad Informática. En la Propuesta se ofrece la unificación de las funcionalidades de Firewall, IPS y Filtrado de Contenido tanto para los equipos ofertados en la salida de Internet Dedicado en el Data Center de AXTEL, como para los equipos que brindan seguridad al Internet de los Nodos Estratégicos.

Cada uno de los servicios (Firewall, IPS y Filtrado de Contenido) de los distintos equipos de Seguridad que conforman la Solución de Seguridad Perimetral, serán Administrados y Monitoreados centralmente de forma remota por el SOC (Security Operation Center) de AXTEL mediante un equipo FortiManager-1000D y un FortiAnalyzer-3000D. Todos estos elementos se integrarán a la plataforma de Correlación de eventos de Axtel.

En resumen la plataforma estará compuesta por:

- Dos equipos FortiGate-3600C configurados en Alta Disponibilidad Activo-Activo para la protección del Internet Dedicado del Centro de Datos de Axtel
- Dos equipos FortiGate-300C configurados en Alta Disponibilidad Activo-Pasivo para el Internet del Nodo Estratégico **CONASAMI**
- Dos equipos FortiGate-300C configurados en Alta Disponibilidad Activo-Pasivo para el Internet del Nodo Estratégico **FELIX CUEVAS (CONTRALORIA)**
- Dos equipos FortiGate-600C configurados en Alta Disponibilidad Activo-Pasivo para el Internet del Nodo Estratégico **PERIFERICO**
- Dos equipos FortiGate-600C configurados en Alta Disponibilidad Activo-Pasivo para el Internet del Nodo Estratégico **AJUSCO**
- Dos equipos FortiGate-600C configurados en Alta Disponibilidad Activo-Pasivo para el Internet del Nodo Estratégico **COORDINACIÓN GENERAL DEL EMPLEO**

DIAGRAMA CONCEPTUAL SEGURIDAD



FORTIGATE-3600C

El Firewall de Nueva Generación NGFW FortiGate-3600C con un rendimiento excepcional, flexibilidad en su implementación y características de seguridad sobresalientes está diseñado para proteger los entornos de red más exigentes. Construido específicamente por Fortinet, el FortiGate-3600C ofrece un rendimiento superior a través de una combinación de hardware dedicado y a la medida, incluyendo los procesadores FortiASIC, alta densidad de puertos y características de seguridad consolidadas desde el propio sistema operativo FortiOS.



AXTEL, S.A.B. DE C.V./AVANTELS, S DE RL DE CV.
EN PARTICIPACION CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS
INFORMÁTICOS ADMINISTRADOS DE VOZ, DATOS, INTERNET Y
VIDEOCONFERENCIA PARA LA SECRETARÍA DEL TRABAJO Y
PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA
DEFENSA DEL TRABAJO (PROFEDTEL), LA COORDINACIÓN GENERAL
DEL SERVICIO NACIONAL DE EMPLEO "CONASAMI", LA COMISIÓN
NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), LA COMISIÓN
NACIONAL MIXTA DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL
INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS
TRABAJADORES (INSTITUTO FONACOT).

Ya seas protegiendo su Centro de Datos, el Perímetro de la red o desplegado como parte de un servicio de Seguridad Administrada, los 30 puertos de alta velocidad y los 60 Gbps de rendimiento de Firewall hacen del FortiGate-3600C la plataforma ideal para asegurar las redes demandantes de mucho poder de cómputo y de gran ancho de banda.

Seguridad más allá del Firewall de Siguinte Generación

El Firewall Fortinet FortiGate-3600C de última generación le permite desplegar una combinación adecuada de tecnologías de seguridad con Aceleración por Hardware, esenciales para los entornos de negocio actuales y a futuro para satisfacer sus requerimientos de red en evolución. Estas tecnologías incluyen Firewall, VPN, Prevención de Intrusos y Control de Aplicaciones, todo ello gestionado desde una única Consola de Administración.

A diferencia de otros Fabricantes de seguridad de próxima generación, el FortiGate-3600C incluye tecnologías de seguridad adicionales tales como Antimalware, Filtrado de Contenido Web y Optimización WAN, lo que le permite una consolidación fácil de Servicios de Seguridad.

FORTIGATE-800C

El equipo Fortigate de Administración Unificada de Amenazas (UTM) de Fortinet le ofrece la libertad de seleccionar la solución de seguridad que más se acerque a su requerimiento de densidad de puertos, rendimiento y las necesidades de ancho de banda. Con un rendimiento de Firewall de 20 Gbps y del IPS de 6 Gbps e interfaces de 10 GbE en tan solo una Unidad de Rack. El FortiGate-800C es la plataforma ideal para empresas medianas o sucursales de empresas grandes. La plataforma FortiGate-800C le da la posibilidad de mejorar su nivel de seguridad y acelerar el rendimiento de la red al tiempo que simplifica la infraestructura de red.

El Poder de Gestión Unificada de Amenazas

Como otros miembros de la familia de productos FortiGate, el FortiGate-800C combina Firewall, Control de Aplicaciones, VPNs IPSec y SSL, Prevención de Intrusiones y Filtrado Web en un solo dispositivo. Equipado con estas capacidades de seguridad generales, el FortiGate-800C permite a las organizaciones cumplir los requisitos de Cumplimiento Normativo y proteger contra los últimos ataques dirigidos, vulnerabilidades de la red, aplicaciones maliciosas y proporcionan la protección que necesita contra las amenazas de seguridad actuales.

El FortiGate-800C es compatible con redes avanzadas mediante dos (2) interfaces de 10 GbE y doce (12) 10/100/1000 que pueden ser fácilmente dividida en zonas de seguridad independientes y combinaciones personalizadas de los puertos LAN y WAN. Ocho (8) interfaces GbE de cobre/fibra compartidas que permiten apoyar en redes que puedan estar migrando segmentos de red a fibra. Permite además proteger la disponibilidad de la red con dos (2) pares de puertos de bypass, los cuales permiten la continuidad en la operación de la red en caso de fallo del dispositivo.



AXTEL, S.A.B. DE C.V./AVANTEL, S. DE B.L. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET) LA COOPERACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (COGENSE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MEXICO DE PROTECCIÓN AL SALARIO (CONAMPROSA) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

FORTIGATE-600C

Con la necesidad continua de protección contra amenazas nuevas y viejas, que necesitan una visibilidad sin precedentes y control sobre la totalidad de su tráfico de red. Los equipos FortiGate Unified Threat Management (UTM) de Fortinet le ofrecen la posibilidad de mejorar su postura en materia de seguridad y acelerar el rendimiento de la red al tiempo que simplifica la infraestructura de red.

El dispositivo **FortiGate-600C** ofrece un rendimiento líder del sector y la flexibilidad con la aceleración de hardware de tecnologías de seguridad esenciales, incluyendo Firewall, VPN, Prevención de Intrusiones IPS, Control de Aplicaciones y Filtrado de contenidos web, todo ello gestionado desde una sola consola. Control de aplicaciones avanzada le permite definir y aplicar políticas para miles de aplicaciones que se ejecutan a través de la red independientemente del Puerto o Protocolo que utilicen.

Estos equipos de Fortinet ofrecen un desempeño superior mediante la combinación de hardware dedicado como son los procesadores FortiASIC, una alta densidad de puertos, y la consolidación de una serie de funcionalidades de seguridad dentro del sistema operativo FortiOS.

Con 16 Gbps de rendimiento de Firewall y 4 Gbps de rendimiento IPS el FortiGate-600C cumple con los requisitos de velocidad de las Organizaciones Medianas y Sucursales Remotas Grandes. El FortiGate-600C ofrece 16 puertos Gigabit Ethernet (GbE) puertos RJ-45, dando libertad para crear varias Zonas de Seguridad para los distintos Departamentos, Usuarios, Métodos de acceso, e incluso Dispositivos para reforzar la seguridad de la red a Velocidades Aceleradas.

FORTIGATE 300C

Seguridad Acelerada para el Mercado Empresarial Mediano y Sucursales Remotas

Con la continua evolución de las amenazas de seguridad de red y la llegada de nuevas aplicaciones aparentemente todos los días, toda empresa necesita la visibilidad y el control sobre la totalidad de su tráfico de red. Los sistemas de Fortinet de Administración de Amenazas Unificados (UTM) le ofrecen la posibilidad de mejorar su nivel de seguridad y acelerar el rendimiento de la red al tiempo que simplifica la infraestructura de red.

El dispositivo FortiGate-300C ofrece un rendimiento y una flexibilidad líder en la industria con tecnologías de seguridad esenciales acelerados por hardware, incluyendo Firewall, VPN, Prevención de Intrusos, Control de Aplicaciones y Filtrado de Contenidos Web, todo ello gestionado desde un todo ello gestionado desde una única consola de administración. El FortiGate-300C le da la capacidad para identificar y detener numerosos tipos de amenazas desde un único dispositivo.

El poder de la Seguridad Acelerada

La plataforma FortiGate-300C ofrece la velocidad y la seguridad integral que su red en crecimiento necesita. Integra un procesador de seguridad de propósito específico, el Procesar FortiASIC incluido en los equipos Fortigate que proporcionan seguridad a velocidades de



AXTEL, S.A.B. DE C.V. / AVANTEL, S. DE RL DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA PROCURADURIA FEDERAL DE LA DEFENSA DEL HABAJALO (PROFED), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CUGNE", LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL MEXICO DE PROTECCION AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS HABAJALORES (INSTITUTO FONACOT).

comutación. Otro procesador ASIC de propósito específico el FortiASIC, proporciona aceleración adicional para la inspección de contenido. Ocho interfaces LAN aceleradas por hardware, con un adicional de dos puertos no acelerados WAN le permiten aplicar directivas entre segmentos de red de seguridad en capas con rendimiento de conmutación. Las numerosas interfaces de seguridad aceleradas le dan la libertad para crear varias zonas de seguridad para los distintos segmentos de red, usuarios, métodos de acceso, o incluso los dispositivos para reforzar la seguridad de la red a velocidades aceleradas.

FORTIANALYZER

Administración de amenazas combinadas en tiempo real con generación de reportes, registro, alertas y almacenamiento de contenido

Soluciones para administrar la seguridad dinámica

La familia de sistemas FortiAnalyzer de registro, análisis y generación de reportes en tiempo real en la red consisten en una serie de aplicaciones de equipo dedicado para la red que registra de manera conjunta y segura la información desde los dispositivos de Fortinet y los dispositivos de terceros. Una amplia gama de archivos de registros, incluyendo información de tráfico, eventos, virus, ataques, contenido en la Red y correo electrónico, pueden ser almacenada, filtrada y extraída para efectos de conformidad o análisis históricos. Hemos incorporado un amplio conjunto de reportes estándar y flexibilidad para personalizar reportes específicos. FortiAnalyzer también ofrece funciones avanzadas de administración de seguridad, como son la cuarentena de archivos, la correlación de eventos, la valoración de vulnerabilidades, el análisis de tráfico y el almacenamiento de correo electrónico, acceso a la Red, mensajería instantánea y el contenido de la transferencia de archivos.

Características y beneficios clave de la solución

Correlación de eventos de la Red. Permite que los administradores de TI identifiquen y reaccionen de manera más expedita ante las amenazas de seguridad a la red.

Creación, estandarización y personalización simplificada de reportes. Proporciona reportes de eventos, actividades y tendencias globales de la red que están ocurriendo en los dispositivos FortiGate™ y de terceros.

Desempeño y capacidad escalables. Los modelos de la familia FortiAnalyzer soportan miles de dispositivos FortiGate y FortiClient™.

Amplia gama de archivos de registro. Incluyendo tráfico, eventos, virus, ataques, filtrado del contenido de la Red y filtro de información del correo electrónico que ayudan a cumplir los requerimientos reglamentarios, tales como HIPAA y otras reglamentaciones relacionadas con la privacidad de información/cliente.

Cuarentena y contenido centralizado. Proporciona almacenamiento confiable de información de contenido, tales como contenido del correo electrónico, chat IM y transferencias de archivos, así como cuarentena para archivos infectados.



AXTEL, S.A.B. DE C.V. / AVANTEL, S. DE R.L. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACIÓN DEL SERVICIO DE PFI NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDT), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CGSE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MEXICO DE MUTUACIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

Agrupación centralizada de registros. Soporta escenarios de implementación flexible, tales como modelos de bajo costo de despliegue en oficinas regionales y registros agrupados para oficinas centralizadas.

Integración casi imperceptible con otros productos Fortinet. La perfecta integración maximiza el desempeño y permite que los recursos FortiAnalyzer se administren desde la interfase de usuario de FortiGate o FortiManager™.

FORTIMANAGER

Para la parte de administración de las diferentes tecnologías marca fortinet incluidas en la propuesta se utilizara un dispositivo FortiManager 1000C, el cual ofrece las herramientas necesarias para gestionar, aprovisionar, configurar y administrar actualizaciones con eficacia para las distintas tecnologías de seguridad de Fortinet.

- Proporciona una configuración centralizada fácil, aprovisionamiento basado en la actualización, gestión y monitoreo de red de extremo a extremo para la instalación de Fortinet
- Administración de hasta 5.000 dispositivos y dominios virtuales (VDOMs) desde una única interfaz FortiManager
- Separar la gestión de grandes despliegues de forma fácil y segura por medio de dispositivos de agrupamiento y agentes en dominios administrativos geográficas o funcionales (ADOMs)
- Reduzca su carga administrativa y los costos operativos con dispositivo rápido y aprovisionamiento agente, rastreo detallada revisión y auditoría a fondo
- Administre fácilmente entornos VPN estrellas malla compleja y al mismo tiempo utilice el FortiManager como punto de distribución local para las actualizaciones de software y la política
- La perfecta integración con las aplicaciones FortiAnalyzer permite un descubrimiento a profundidad, análisis, priorización y notificación de eventos de seguridad de red
- Creación y modificación rápida de políticas / objetos con un método fácil de arrastrar y soltar en el modo vista
- Automatización en el aprovisionamiento de dispositivos, que empujan la política, etc con JSON API y construcción de portales web personalizados con la API XML
- Definir y limitar las responsabilidades de gestión mediante la aplicación de administración basada en roles

Manejo de Perfiles de dispositivos para el aprovisionamiento en masa y la configuración de los dispositivos administrados.

Atentamente

Bajo protesta de decir verdad
Jorge Vicente M. Rendón
Representante Común



AXTEL, S.A.B. DE C.V./AVANTEL, S. DE RL. DE CV.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CONSE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPRO) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

México, D.F., a 19 de Diciembre de 2013

SERVICIOS ADMINISTRADOS DE SEGURIDAD PERIMETRAL PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET						
7.1 CONSIDERACIONES GENERALES PARA LOS SERVICIOS DE SEGURIDAD PERIMETRAL						
7.1.1 El Licitante debe proporcionar los servicios administrados de seguridad perimetral que incluyen los siguientes servicios: Firewall, IPS y Filtrado de Contenido, los cuales deberán contar con los Firmware y el sistema operativo más actualizado liberados por el fabricante.	AXTEL proporcionará los servicios administrados de seguridad perimetral que incluyen los siguientes servicios: Firewall, IPS y Filtrado de Contenido, los cuales cuenta con los Firmware y el sistema operativo más actualizado liberados por el fabricante.	NA	NA	NA	NA	AXTEL proporcionará los servicios administrados de seguridad perimetral que incluyen los siguientes servicios: Firewall, IPS y Filtrado de Contenido, los cuales cuenta con los Firmware y el sistema operativo más actualizado liberados por el fabricante.
7.1.2 En el caso del nodo concentrador que cuenta con conectividad a Internet Dedicado en el Data Center del licitante, la solución de seguridad perimetral debe habilitarse en alta disponibilidad del tipo activo-activo para todos sus servicios indicados en el punto anterior.	Active-active (A-A) HA load balances resource-intensive UTM processing among all cluster units.	FortiOS Handbook for FortIOS 5.0	NA	1716	3	Activo-activo (AA) equilibra la carga de procesamiento HA UTM intensivo de los recursos entre todas las unidades de clúster.
7.1.3 Para las oficinas que cuenten con una conectividad directa al servicio de Internet (nodos estratégicos)	An active-passive cluster consists of a primary unit that processes communication	FortiOS Handbook for FortIOS 5.0	NA	1715	7	Un clúster activo-pasivo consiste en una unidad principal que procesa sesiones de comunicación, y una o



AXTEL, S.A.B. DE CV / AVANTEI, S. DE R.L. DE CV
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROSECRETARÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "COSSNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAM), EL COMITÉ NACIONAL MEXTO DE PROTECCIÓN AL SALARIO (CONAMIPROS) Y EL INSTITUTO DE FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

también debe habilitarse el servicio de seguridad perimetral administrada, en alta disponibilidad, la ubicación de los nodos aparecen en el Anexo "B".	sessions, and one or more subordinate units.				más unidades subordinadas.
<p>7.1.4 Los servicios del tipo Activo-Activo que conforman la solución de seguridad perimetral administrada, deben presentarse en dispositivos appliance basados en un sistema propietario del mismo fabricante y de última generación.</p> <p>De acuerdo a la Pregunta técnica 13 de UNINEY respecto a las funcionalidades de Firewall, IPS y Filtrado de Contenido, AXTEL toma en cuenta en su propuesta que la Convocante permite la integración de los Servicios de Firewall, IPS y Filtrado de Contenido en un solo equipo siempre y cuando se cumplan con los niveles de servicio y características solicitados.</p>	<p>Active-active (A-A) HA load balances resource-intensive UTM processing among all cluster units.</p> <p>FortiOS is a security-hardened, purpose-built operating system that forms the foundation of all FortiGate platforms.</p>	<p>FortiOS Handbook for FortiOS 5.0</p> <p>FortiOS 5 Network Security Operating System</p>	<p>NA</p> <p>NA</p>	<p>1716</p> <p>1</p>	<p>3</p> <p>1</p> <p>Activo-activo (AA) equilibra la carga de procesamiento HA UTM intensivo de los recursos entre todas las unidades de clúster.</p> <p>FortiOS es un sistema operativo de propósito-construido seguridad reforzada que forma la base de todas las plataformas FortiGate.</p>



AXTEL, S.A.B. DE C.V./AVANTEL S. DE RL. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDT), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CGSE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAM), EL COMITÉ NACIONAL MEXICO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

<p>7.1.5 Cada uno de los elementos que conforman la solución de seguridad perimetral administrada deben ser nuevos de la misma marca, no se aceptan soluciones con más de una marca, adicionalmente el Licitante debe entregar carta del fabricante en papel membretado y firmado en fecha reciente, donde se especifique que el Licitante es distribuidor autorizado por el fabricante y que cuenta con el personal técnico calificado para instalar, configurar, administrar y monitorear los elementos de seguridad perimetral que son instalados.</p>	<p>Para dar cumplimiento a este punto se anexa la CARTA solicitada</p>	<p>NA</p>	<p>NA</p>	<p>NA</p>	<p>NA</p>	<p>Para dar cumplimiento a este punto se anexa la CARTA solicitada</p>
<p>7.1.6 El Licitante debe entregar documentos</p>	<p>Para dar cumplimiento a este punto se anexan las copias de los</p>	<p>NA</p>	<p>NA</p>	<p>NA</p>	<p>NA</p>	<p>Para dar cumplimiento a este punto se anexan las copias de los CERTIFICADOS solicitados.</p>



AXTEL, S.A.B. DE C.V./AVANTEL, S. DE R.L. IG C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALCS ADMINISTRADOS DE VOZ DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CGSE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

<p>(copia) que compruebe la capacidad de al menos 2 ingenieros certificados en la marca del fabricante para la instalación de la solución de seguridad perimetral.</p>	<p>CERTIFICADOS solicitados.</p>					
<p>7.1.7 Cada uno de los servicios (firewall, IPS y Filtrado de Contenido) de la solución de seguridad perimetral, debe ser administrada y monitoreada de manera remota a través del SOC (Security Operation Center) del Licitante.</p>	<p>Cada uno de los servicios (firewall, IPS y Filtrado de Contenido) de la solución de seguridad perimetral, será administrada y monitoreada de manera remota a través del SOC (Security Operation Center) de AXTEL.</p>	<p>NA</p>	<p>NA</p>	<p>NA</p>	<p>NA</p>	<p>Cada uno de los servicios (firewall, IPS y Filtrado de Contenido) de la solución de seguridad perimetral, será administrada y monitoreada de manera remota a través del SOC (Security Operation Center) de AXTEL.</p>
<p>7.2 SERVICIO ADMINISTRADO DE FIREWALL EN NODO DATA CENTER PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET</p>						
<p>7.2.1 Para el caso del servicio de Firewall en el nodo concentrador de Internet, en el Data Center del Licitante, la solución debe ser redundante en Firewall, este debe estar basado en un dispositivo appliance, no se aceptará ninguna solución exclusiva por software y debe contar con sistema operativo propietario.</p>	<p>Active-active (A-A) HA load balances resource-intensive UTM processing among all cluster units.</p> <p>FortiOS is a security-hardened, purpose-built operating system that forms the foundation of all FortiGate platforms.</p>	<p>FortiOS Handbook for FortiOS 5.0</p> <p>FortiOS 5 Network Security Operating System</p>	<p>NA</p> <p>NA</p>	<p>1716</p> <p>1</p>	<p>3</p> <p>1</p>	<p>Activo-activo (AA) equilibra la carga de procesamiento HA UTM intensivo de los recursos entre todas las unidades de cluster.</p> <p>FortiOS es un sistema operativo de propósito-construido seguridad reforzada que forma la base de todas las plataformas FortiGate.</p>



AXTEL, S.A.B. DE C.V./AVANTEL, S. DE R.L. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE NFO NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDT), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONSE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAM), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

<p>De acuerdo a la Pregunta técnica 13 de UNINET respecto a las funcionalidades de Firewall, IPS y Filtrado de Contenido. AXTEL toma en cuenta en su propuesta que la Convocante permite la integración de los Servicios de Firewall, IPS y Filtrado de Contenido en un solo equipo siempre y cuando se cumplan con los niveles de servicio y características solicitados.</p>						
<p>7.2.2 Los puertos LAN del equipo Firewall deben ser del tipo 10/100/1000 (Mbps) con conector RJ-45 en cobre.</p>	<p>16 x GbE SFP Slots</p>	<p>FortiGate-3600C</p>	<p>NA</p>	<p>2</p>	<p>1</p>	<p>16 x GbE SFP puertos</p>
<p>7.2.3 El equipo Firewall debe contar con al menos 3 certificaciones como ICSA Labs, FIPS 140/2, EAL4 o NSS Labs Debe contar con la capacidad de manejo de tráfico para maximizar la limitación del ancho de banda, ruteo dinámico con protocolos OSPF y BGP, ECMP, soporte a VLANs (802.1q) y ruteadores virtuales, dominios virtuales o</p>	<p>FIPS PUB 140-2 Common Criteria EAL2+ and EAL4+ certifications of FortiOS ICSA Certification of FortiGates and FortiOS Traffic shaping and QOS: shared policy shaping WAN load balancing with ECMP OSPF v2 and v3, BGP4</p>	<p>Inside FortiOS Certifications and Testing FortiOS 5 Network Security Operating System</p>	<p>NA NA</p>	<p>1,2 4</p>	<p>NA Tabla</p>	<p>FIPS PUB 140-2 Criterios EAL2 Common + y EAL4 + certificaciones de FortiOS Certificación de ICSA FortiGates y FortiOS La Administración de Tráfico y Políticas de Ciudad de Servicio Balanceo de carga WAN con ECMP OSPF v2 y v3, BGP4 VLAN (802.1Q y Trunking)</p>



AXTEL, S.A.B. DE C.V. (AVANTEL S. DE R.L. DE C.V.)
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CONSE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONASAPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

<p>la capacidad de crear equipos lógicos.</p>	<p>VLANs (802.1Q and Trunking)</p> <p>Virtual domains (VDOMs) are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units.</p>	<p>FortiOS Handbook for FortiOS 5.0</p>		<p>1591</p>	<p>1</p>	<p>Dominios virtuales (VDOMs) son un método de dividir una unidad de FortiGate en dos o más unidades virtuales que funcionan como múltiples unidades independientes.</p>
<p>7.2.4 Así mismo el equipo firewall debe soportar métodos de autenticación requeridos para el Gateway, base de datos interna e interconstruida, RADIUS, RSA SecurID, LDAP.</p> <p><i>De acuerdo a la Pregunta técnica 103 de UNINET. AXTEL toma en consideración que cuando lo Convocante menciona interconstruida hace referencia a una base de datos interna, dentro del firewall, que no depende de algún elemento externo.</i></p>	<p>FortiOS supports both local and remote authentication services such as LDAP, Radius and TACACS+ to identify users and apply access policies and security profiles accordingly.</p> <p>SecurID is a two-factor system that uses one-time password (OTP) authentication. It is produced by the company RSA.</p>	<p>FortiOS 5 Network Security Operating System</p> <p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p> <p>NA</p>	<p>3</p> <p>960</p>	<p>1</p> <p>1</p>	<p>FortiOS apoya los servicios locales y remotos de autenticación, como LDAP, RADIUS y TACACS+ para identificar a los usuarios y aplicar las políticas de acceso y perfiles de seguridad en consecuencia.</p> <p>SecurID es un sistema de dos factores que utiliza la contraseña (OTP) de autenticación de una sola vez. Es producido por la compañía RSA.</p>
<p>7.2.5 Las funcionalidades del firewall deben soportar un número de sesiones simultáneas</p>	<p>Concurrent Sessions (TCP) 28 Million Firewall Throughput 60 Gbps Virtual Domains (Default / Max) 10 /</p>	<p>FortiGate-3600C</p>	<p>NA</p>	<p>6</p>	<p>Tabla</p>	<p>Sesiones concurrentes (TCP) 28 Millones Firewall Throughput 60 Gbps Dominios virtuales 200 Incluidas</p>



AXTEL S.A.A. DE C.V./AVANTEL S. DE C.V. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCLERADÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "COSPE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

<p>procesadas de al menos 28 millones de sesiones, el throughput o rendimiento será de al menos 60 Gbps, la solución deberá soportar un mínimo de 200 routers virtuales o dominios virtuales, y más de 210,000 nuevas sesiones por segundo</p>	<p>500 New Sessions/Sec (TCP) 235,000</p>				<p>Nueva Sesiones / Sec (TCP) 235000</p>
<p>7.2.6 El firewall debe tener capacidad de manejo de túneles de VPN, por lo que debe soportar hasta 8,000 túneles de VPN, con throughput de 20 Gbps en modo de VPN (3DES).</p>	<p>Gateway-to-Gateway IPSec VPN Tunnels 10,000 IPSec VPN Throughput 75 Gbps</p>	<p>FortiGate-3600C</p>	<p>NA</p>	<p>6</p>	<p>Tabla Gateway-to-gateway IPSec VPN Túneles 10000 IPSec VPN Throughput 25 Gbps</p>
<p>7.3 SERVICIO ADMINISTRADO DE IPS (SISTEMA DE PREVENCIÓN DE INTRUSOS) EN NODO DATA CENTER PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET</p>					
<p>7.3.1 Para el caso de la solución de IPS (Intrusion Prevention System) en el nodo concentrador de Internet, en el Data Center del Licitante, la solución debe ser redundante, éste debe estar basado en un dispositivo appliance, no se aceptará ninguna solución exclusiva por software y debe contar con sistema operativo propietario.</p> <p><i>Pregunta técnica 13 de UNINET respecto</i></p>	<p>Active-active (A-A) HA load balances resource-intensive UTM processing among all cluster units.</p> <p>FortiOS is a security-hardened, purpose-built operating system that forms the foundation of all FortiGate platforms.</p>	<p>FortiOS Handbook for FortiOS 5.0</p> <p>FortiOS 5 Network Security Operating System</p>	<p>NA</p> <p>NA</p>	<p>1716</p> <p>1</p>	<p>Activo-activo (AA) equilibra la carga de procesamiento HA UTM intensivo de los recursos entre todas las unidades de cluster.</p> <p>FortiOS es un sistema operativo de propósito-construido seguridad reforzada que forma la base de todas las plataformas FortiGate.</p>



AXTEL, S.A.B. DE CV / AVANTEL, S. DE RL DE CV.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (COSENE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAPROSA) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

<p>a las funcionalidades de Firewall, IPS y Filtrado de Contenido. AXTEL toma en cuenta en su propuesta que la Convocante permita la integración de los Servicios de Firewall, IPS y Filtrado de Contenido en un solo equipo siempre y cuando se cumplan con los niveles de servicio y características solicitadas.</p>						
<p>7.3.2 Los puertos LAN del equipo IPS deben ser de tipo 10/100/1000 (Mbps) con conector RJ-45 en cobre.</p>	16 x GbE SFP Slots	FortiGate-3600C	NA	2	1	16 x GbE SFP puertos
<p>7.3.3 El equipo IPS del Licitante debe bloquear diferentes tipos de tráfico peer-to-peer, el equipo deberá de poder controlar: kazaa, morpheus, imesh, edonkey, limewire, bearshare entre otros; el sistema debe operar en línea, el sistema no debe requerir ningún direccionamiento IP en los puertos de inspección, el sistema debe soportar un rendimiento de inspección de 14</p>	<p>IPS Throughput 14 Gbps Concurrent Sessions (TCP) 28 Million New Sessions/Sec (TCP) 235,000 Latency 4 us</p> <p>FortiGuard Center Kazaa Morpheus Imesh Edonkey LimeWire Bearshare</p>	<p>FortiGate-3600C</p> <p>FortiGuard Center Kazaa Morpheus Imesh Edonkey LimeWire Bearshare</p>	<p>NA</p> <p>NA</p>	<p>6</p> <p>NA</p>	<p>Tabla</p> <p>NA</p>	<p>Rendimiento del IPS 14 Gbps Sesiones concurrentes (TCP) 28 Millones Nueva Sesiones / Sec (TCP) 235000 Latencia 4 microsegundos</p> <p>Centro FortiGuard Kazaa Morpheus Imesh Edonkey LimeWire Bearshare</p>

178



AXTEL, S.A.B. DE C.V./AVANTEI, S. DE R.L. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRADOS ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFDEF), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONSE), LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAM), EL COMITE NACIONAL MEXICO DE PROTECCION AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FODRACOT).

<p>Gbps como mínimo, el sistema debe manejar al menos 28,000,000 de sesiones (conexiones bidireccionales) y debe soportar al menos 210,000 nuevas conexiones por segundo con una latencia de menos de 5 microsegundos.</p> <p>De acuerdo a la Pregunta técnica 104 de UNINET de la operación en modo en línea sin direccionamiento IP, AXTEL toma en consideración que la Convocante permite la integración del servicio de firewall e IPS en un mismo appliance, considerando que aunque el equipo no actúe como bridge en caso de falla, es decir al momento de fallar físicamente no sería capaz de transmitir tráfico alguno, en comparación a esto contaría con un mecanismo de alta disponibilidad físico (otro equipo, siempre que se mantengan los niveles de servicio solicitados).</p>						
7.3.4 Debe soportar	DoS policies	FortiOS Handbook	NA	555	3	Pulificas DoS

16



AXTEL, S.A. DE C.V. Y AVANTEL, S. DE R.L. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA SECRETARIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO "OGONE", LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAB), EL COMITE NACIONAL MIXTO DE PROTECCION AL SALARIO (CONAMIPES) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONAGOT).

<p>Anti-DDoS para mitigar este tipo de ataques, el equipo debe tener filtros para detectar y bloquear spyware, el equipo debe ser capaz de bloquear y/o administrar el ancho de banda que utilizan las aplicaciones point-to-point y debe contar con servicio de actualización durante la vigencia del contrato.</p>	<p>DDoS attacks vary in nature and intensity. Attacks aimed at saturating the available bandwidth upstream of your service can only be countered by adding more bandwidth. DoS policies can help protect against DDoS attacks that aim to overwhelm your server resources.</p>	<p>for FortiOS 5.0</p>				<p>Los ataques DDoS varían en naturaleza e intensidad. Los ataques destinados a saturar el ancho de banda disponible aguas arriba de su servicio sólo pueden ser contrarrestados mediante la adición de más ancho de banda. Políticas de denegación de servicio pueden ayudar a proteger contra los ataques DDoS que tienen como objetivo saturar los recursos del servidor.</p>
	<p>The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units.</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>319</p>		<p>El equipo FortiGuard se puede encontrar alrededor de las actividades de globo, virus de monitoreo, software espía y vulnerabilidad. Como se encuentran las vulnerabilidades, las firmas se crean y empujaron a las unidades FortiGate suscritas.</p>
	<p>Application protection: Client uses software in risky categories, including Botnet, P2P, Proxy, and Games applications. A subscription to FortiGuard IPS updates is required.</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>776</p>		<p>Protección de aplicaciones: El cliente utiliza el software en categorías de riesgo, incluyendo Botnet, P2P, Proxy, y aplicaciones de juegos. Se necesita una suscripción a las actualizaciones de FortiGuard IPS. (incluida)</p>
	<p>The FortiGuard Distribution Network</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>319</p>		<p>La Red de Distribución FortiGuard (FDN) de</p>



AXTEL, S.A.B. DE C.V. / AXTEL, S. DE RL. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONASA), LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL MIXTO DE PROTECCION AL SALARIO (CONASAPRO) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

	(FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit.					servidores proporciona actualizaciones de antivirus, antispam y definiciones de IPS a su unidad FortiGate.	
7.3.5	Si sistema podrá tener diferentes perfiles de seguridad por cada segmento y estos segmentos se podrán agrupar de diversas maneras según sea necesario, el control de acceso se puede limitar por perfil, dispositivo o segmento de red.	When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number). It also registers the incoming interface, the outgoing interface it will need to use and the time of day. Using this information the FortiGate firewall attempts to locate a security policy that matches the packet.	FortiOS Handbook for FortiOS 5.0	NA	526	3	Quando el servidor de seguridad recibe un paquete de conexión, se analiza la dirección del paquete de origen, dirección de destino, y el servicio (por número de puerto). También registra el interfaz de entrada, la interfaz de salida tendrá que utilizar y la hora del día. Con esta información el servidor de seguridad FortiGate intenta localizar una política de seguridad que coincide con el paquete.
7.4 SERVICIO ADMINISTRADO DE FILTRADO DE CONTENIDO EN MODO DATA CENTER PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET							
7.4.1	Para el caso de la solución de Filtrado de Contenido en el nodo concentrador de Internet, en el Data Center del Licitante, la solución debe ser redundante, éste debe estar basado en un dispositivo appliance, no se aceptará ninguna solución exclusiva por software.	Activo-activo (A-A) HA load balances resource-intensive UTM processing among all cluster units. FortiOS is a security-hardened, purpose-built operating system that forms the foundation of all FortiGate platforms.	FortiOS Handbook for FortiOS 5.0 FortiOS 5 Network Security Operating System	NA	1716	3	Activo-activo (AA) equilibra la carga de procesamiento HA UTM intensivo de los recursos entre todas las unidades de clúster. FortiOS es un sistema operativo de propósito-construido seguridad reforzada que forma la base de todas las plataformas FortiGate.
<i>Pregunta técnica 13 de UNINET respecto a las funcionalidades</i>							



AXTEL S.A.B. DE C.V. JAVIERES DE RELL D.R. C.V.
EN PARTICIPACIÓN CUBUYTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA SECRETARÍA DEL TRABAJO Y DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN FEDERAL DE LA DEFENSA DEL TRABAJO (COFEDETR), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CGSE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL VIKTO DE PROTECCIÓN AL SALARIO (CONAMPRO) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

<p>de Firewall, IPS y Filtrado de Contenido. AXTEL toma en cuenta en su propuesta que la Convocante permite la integración de los Servicios de Firewall, IPS y Filtrado de Contenido en un solo equipo siempre y cuando se cumplan con los niveles de servicio y características solicitadas.</p>						
<p>7.4.2 Los puertos LAN del Filtrado de Contenido deben ser del tipo 10/100/1000 (Mbps) con conector RJ-45 en cobre.</p>	16 x GbE SFP Slots	FortiGate-3600C	NA	2	1	16 x GbE SFP puertos
<p>7.4.3 El Filtrado de Contenido se requiere para la navegación de 6,036 (seis mil treinta y seis) usuarios al inicio del servicio en el sitio de Internet de alta capacidad, sin embargo; el equipo debe tener la capacidad soportar el crecimiento de por lo menos el 35% de usuarios sin ningún costo adicional.</p>	<p>AXTEL está en el entendido que el filtrado de Contenido se requiere para la navegación de 6,036 (seis mil treinta y seis) usuarios al inicio del servicio en el sitio de Internet de alta capacidad, sin embargo; el equipo tiene la capacidad de soportar el crecimiento de por lo menos el 35% de usuarios sin ningún costo adicional.</p>	NA	NA	NA	NA	<p>AXTEL está en el entendido que el Filtrado de Contenido se requiere para la navegación de 6,036 (seis mil treinta y seis) usuarios al inicio del servicio en el sitio de Internet de alta capacidad, sin embargo; el equipo tiene la capacidad de soportar el crecimiento de por lo menos el 35% de usuarios sin ningún costo adicional.</p>
<p>7.4.4 El equipo de Filtrado de Contenido debe contar con al menos 75 categorías para una navegación</p>	<p>FortiGuard Web Filtering is a subscription service that allows you to limit access to web</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	NA	773	13	<p>FortiGuard Web Filtering es un servicio de suscripción que le permite limitar el acceso a sitios web. Más de 60</p>



AXTEL, S.A.B. DE C.V./AVANTEL, S. DE RL. DE C.V.
EN PARTICIPACIÓN CORALITA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA SECRETARÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (COSENE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MEXICO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

<p>segura. El equipo deberá proporcionar un servicio de seguridad que combine medidas preventivas, proactivas y reactivas para crear una solución completa de Filtrado de Contenido Web.</p>	<p>sites. More than 60 million web sites and two billion web pages are rated by category. You can choose to allow or block each of the 77 categories.</p>					<p>millones de sitios web y de dos mil millones de páginas web se clasifican por categoría. Usted puede optar por permitir o bloquear cada una de las 77 categorías.</p>
<p>7.4.5 El equipo del Licitante debe bloquear el contenido ofensivo de la red, debe trabajar a nivel Gateway sin instalar ningún agente en los clientes finales, debe contar con listas blancas y negras, debe contar con diarias y debe contar con servicio de actualización durante la vigencia del contrato. El servicio de clasificación y categorización de URL debe de estar basado en la nube.</p>	<p>This section describes FortiGate web filtering for HTTP traffic. The three main parts of the web filtering function, the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service interact with each other to provide maximum control over what the Internet user can view as well as protection to your network from many Internet content threats. Web Content Filter blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>837</p>	<p>1</p>	<p>En esta sección se describe el filtrado web FortiGate para el tráfico HTTP. Las tres partes principales de la función de filtrado web, el Filtro de Contenido Web, el URL Filter, y el servicio de filtro web FortiGuard interactúan entre sí para proporcionar el máximo control sobre lo que el usuario de Internet puede ver, así como la protección de su red de muchos Internet amenazas de contenido. Filtrar contenido Web bloquea las páginas web que contengan palabras o patrones que usted especifique. Filtrado de URL utiliza direcciones URL y los patrones de URL para bloquear o páginas web exentos de fuentes específicas. FortiGuard Web Filtering ofrece muchas categorías adicionales que puede utilizar para filtrar el tráfico de Internet.</p>



AXTEL, S.A.B. DE C.V./AVANTEL S. DE RL DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO "COORNE", LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL MIXTO DE PROTECCION AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

	<p>web traffic.</p> <p>Allow or block access to specific URLs by adding them to the URL filter list. Add patterns using text and regular expressions (or wildcard characters) to allow or block URLs. The unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message.</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>867</p>	<p>5</p>	<p>Permitir o bloquear el acceso a determinadas direcciones URL mediante su inclusión en la lista de filtros de URL. Añadir patrones usando expresiones de texto y regulares (o caracteres comodín) para permitir o URLs de bloque. La unidad permite o bloquea las páginas web a juego cualquier URL o patrones especificados y muestra un mensaje de reemplazo.</p>
	<p>FortiGuard Web Filter is a managed web filtering solution available by subscription from Fortinet. FortiGuard Web Filter enhances the web filtering features supplied with your FortiGate unit by sorting billions of web pages into a wide range of categories users can allow or block. The FortiGate unit accesses the nearest FortiGuard Web Filter Service Point to determine the category of a requested web page, and then applies the security policy configured for that</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>840</p>	<p>6</p>	<p>FortiGuard Web Filter es una solución de filtrado web gestionada disponible mediante suscripción en Fortinet. FortiGuard Web Filter mejora las funciones de filtrado web que se suministran con la unidad FortiGate clasificando miles de millones de páginas web en una amplia gama de categorías de usuarios pueden permitir o bloquear. La unidad de FortiGate accede al Punto de Servicio Web Filter FortiGuard más cercano para determinar la categoría de una página web solicitada, y luego se aplica la política de seguridad configurado para ese usuario o</p>

	user or interface.					interfaz.
7.4.6 El equipo de Filtrado de Contenido del Ucitante para la protección debe realizar análisis por normas, firmas, heurística, análisis de comportamiento, servicios de reputación web y categorías de URL. Prevención de elusión de proxy, filtrado para prevenir botnets, keyloggers, phishing y spyware. Identificación de contenido malicioso generado por los usuarios a medida que se publica en sitios web.	The three main parts of the web filtering function, the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service interact with each other to provide maximum control over what the Internet user can view as well as protection to your network from many Internet content threats. Web Content Filter blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter web traffic.	FortiOS Handbook for FortiOS 5.0	NA	837	1	Las tres partes principales de la función de filtrado web, el Filtro de Contenido Web, el URL Filter, y el servicio de filtro web FortiGuard interactúan entre sí para proporcionar el máximo control sobre lo que el usuario de Internet puede ver, así como la protección de su red de muchos Internet amenazas de contenido. Filtrar contenido Web bloquea las páginas web que contengan palabras o patrones que usted especifica. Filtrado de URL utiliza direcciones URL y los patrones de URL para bloquear o páginas web exentos de fuentes específicas. FortiGuard Web Filtering ofrece muchas categorías adicionales que puede utilizar para filtrar el tráfico de Internet.
	threats are also becoming increasingly sophisticated. Threats and web-based applications that cause additional problems for corporations include:	FortiOS Handbook for FortiOS 5.0	NA	838	1	amenazas también son cada vez más sofisticados. Las amenazas y las aplicaciones basadas en la Web que causan problemas adicionales para las empresas incluyen:
	<ul style="list-style-type: none"> • spyware/grayware • phishing 					<ul style="list-style-type: none"> • spyware / grayware • phishing • pharming

02:15



AXTEL, S.A. B. DE C.V. AVANTEL, S. DE R.L. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONARVE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

	<ul style="list-style-type: none"> • phishing • instant messaging • peer-to-peer file sharing • streaming media • blended network attacks. <p>FortiGuard Web Filter ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. Users can notify the FortiGuard Web Filter Service Points if they feel a web page is not categorized correctly, so that the service can update the categories in a timely fashion.</p> <p>It also provides behavior-based heuristics</p>	FortiOS Handbook for FortIOS 5.0	NA	840	9	<ul style="list-style-type: none"> • Mensajería Instantánea • Intercambio de archivos P2P • Streaming de Medios • Ataques de red Blended <p>FortiGuard calificaciones Web Filter se realizan mediante una combinación de métodos de propiedad, incluyendo el análisis de textos, la explotación de la estructura de la red, y los calificadores humanos. Los usuarios pueden notificar a los puntos de servicio Web Filter FortiGuard si sienten que una página web no se clasifica correctamente, por lo que el servicio puede actualizar las categorías en el momento oportuno.</p> <p>También proporciona la heurística basada en el comportamiento</p>
7.5 SERVICIO ADMINISTRADO DE FIREWALL EN NODOS CON INTERNET DEDICADO PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET						
7.5.1 En los nodos (estratégicos) de conectividad dedicada a Internet el licitante debe instalar un equipo Firewall administrado considerando la capacidad de ancho de banda especificada en el Anexo "B", así como	En los nodos (estratégicos) de conectividad dedicada a Internet AXTEL instalará equipos Firewalls administrados considerando la capacidad de ancho de banda especificada en el Anexo "B", así como	FortiGate-300C	NA	2		<p>FortiGate-300C</p> <p>Sesiones simultáneas 2 Millones</p> <p>Rendimiento Firewall 8 Gbps</p> <p>Políticas de Firewall 10,000</p> <p>Nueva Sesiones / Sec: 50,000</p> <p>Rendimiento del IP5 1.4 Gbps</p>



AXTEL, S.A. DE C.V./AVANTEL, S. DE R.L. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL, DE SERVICIOS NATIONALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONASE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MEXICO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

el número de usuarios.	el número de usuarios. FortiGate 300C Concurrent Sessions 2 Million Firewall Throughput 8 Gbps Firewall Policies 10,000 New Sessions/Sec 50,000 IPS Throughput 1.4 Gbps FortiGate-600C Concurrent Sessions 3 Million Firewall Throughput 16 Gbps Firewall Policies 10,000 New Sessions/Sec 70,000 IPS Throughput 4 Gbps FortiGate-800C Concurrent Sessions 7 Million Firewall Throughput 20 Gbps Firewall Policies 10,000 New Sessions/Sec 190,000 IPS Throughput 6 Gbps	FortiGate-600C	NA	2	FortiGate-600C Sesiones simultáneas 3 Millones Rendimiento Firewall 16 Gbps Políticas de Firewall 10,000 Nueva Sesiones / Sec 70,000 Rendimiento del IPS 4 Gbps	
7.5.2 Para el caso del servicio de Firewall este debe estar basado en un dispositivo appliance, no se aceptará	An active-passive cluster consists of a primary unit that processes communication sessions, and one or	FortiOS Handbook for FortiOS 5.0	NA	1715	7	Un clúster activo-pasivo consiste en una unidad principal que procesa sesiones de comunicación, y una o más unidades



AXTEL S.A.B. DE C.V. AVANTEL S. DE R.L. DE C.V.
EN PARTICIPACION CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOR DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARIA DE TRABAJO Y PREVISION SOCIAL (STPS), LA SECRETARIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO "COGSE", LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL MIXTO DE PROTECCION AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

<p>ninguna solución exclusiva por software. Debe estar basado en sistema operativo propietario.</p> <p><i>Pregunta técnica 13 de UNINET respecto a las funcionalidades de Firewall, IPS y Filtrado de Contenido. AXTEL toma en cuenta en su propuesta que la Convocante permite la integración de los Servicios de Firewall, IPS y Filtrado de Contenido en un solo equipo siempre y cuando se cumplan con los niveles de servicio y características solicitadas.</i></p>	<p>more subordinate units.</p> <p>FortIOS is a security-hardened, purpose-built operating system that forms the foundation of all FortiGate platforms.</p>	<p>FortIOS 5 Network Security Operating System</p>	<p>NA</p>	<p>1</p>	<p>1</p>	<p>subordinadas.</p> <p>FortIOS es un sistema operativo de propósito-construido seguridad reforzada que forma la base de todas las plataformas FortiGate.</p>
<p>7.5.3 La solución podrá habilitarse mediante un equipo de propósito específico o bien un UTM (Unified Threat Management).</p>	<p>the FortiGate line combines a number of security features to protect your network from threats. As a whole, these features, when included in a single Fortinet security appliance, are referred to as Unified Threat Management (UTM).</p>	<p>FortIOS Handbook for FortIOS 5.0</p>	<p>NA</p>	<p>770</p>	<p>1</p>	<p>la línea FortiGate combina una serie de características de seguridad para proteger su red contra amenazas. En su conjunto, estas características, cuando se incluye en un único dispositivo de seguridad de Fortinet, se les conoce como gestión de amenazas unificada (UTM).</p>
<p>7.5.4 Los puertos LAN del equipo firewall deben ser del tipo 10/100/1000 (Mbps) con conector RJ-45</p>	<p>Total 10/100/1000 interfaces (RJ-45) FortiGate-300C 8 FortiGate-600C</p>	<p>FortiGate-300C FortiGate-600C</p>	<p>NA NA</p>	<p>2 2</p>	<p></p>	<p>Interfaces 10/100/1000 (RJ-45) FortiGate-300C 8 FortiGate-600C</p>



AXTEL, S.A.B. DE C.V. / AVANTEL, S. DE R.L. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRATIVOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGENE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMIPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

en cobre.	16 FortiGate-800C 12	FortiGate-800C	NA	2		16 FortiGate-800C 12
7.7.5 El equipo firewall debe soportar al menos: ICASA Labs on Firewall, IPsec, IPS, SSL, VPN.	ICASA subjects FortiOS security functionality to a variety of independent test methods to validate the Firewall, Intrusion Protection, Antivirus and SSL implementations.	Inside FortIOS Certifications and Testing	NA	2	2	ICASA somete funcionalidad de seguridad FortIOS a una variedad de métodos de pruebas independientes para validar el firewall, protección contra intrusiones, antivirus y las implementaciones de SSL.
7.5.6 Las funcionalidades del firewall deben soportar el número de sesiones concurrentes (TCP) especificadas en el Anexo "B" según su capacidad, así como los parámetros especificados para firewall.	<p>FortiGate 300C Concurrent Sessions 2 Million Firewall Throughput 8 Gbps Firewall Policies 10,000 New Sessions/Sec 50,000 IPS Throughput 1.4 Gbps</p> <p>FortiGate-600C Concurrent Sessions 3 Million Firewall Throughput 16 Gbps Firewall Policies 10,000 New Sessions/Sec 70,000 IPS Throughput 4 Gbps</p> <p>FortiGate-800C Concurrent Sessions 7 Million Firewall Throughput 20 Gbps Firewall Policies 10,000</p>	<p>FortiGate-300C</p> <p>FortiGate-600C</p> <p>FortiGate-800C</p>	<p>NA</p> <p>NA</p> <p>NA</p>	<p>2</p> <p>2</p> <p>2</p>		<p>CONASAMI, CONTRALORIA, FortiGate-300C Sesiones simultáneas 2 Millones Rendimiento Firewall 8 Gbps Políticas de Firewall 10,000 Nueva Sesiones / Sec 50,000 Rendimiento del IPS 1.4 Gbps</p> <p>PERIFERICO, AJUSCO, EMPLEO, PROFEDET, FortiGate-600C Sesiones simultáneas 3 Millones Rendimiento Firewall 16 Gbps Políticas de Firewall 10,000 Nueva Sesiones / Sec 70,000 Rendimiento del IPS 4 Gbps</p> <p>REFORMA 93, I.F.C.A. FortiGate-800C</p>



AXTEL, S.A.B. DE CV / AVANTEL, S. DE I.L. DE CV.
EN PARTICIPACION CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRABLES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA PROSECRETARIA DEL TRABAJO Y DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO "COBINE", LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL MIXTO DE PROTECCION AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

	New Sessions/Sec 190,000 IPS Throughput 6 Gbps					Sesiones simultaneas 7 Millones Rendimiento Firewall 20 Gbps Políticas de Firewall 10,000 Nueva Sesiones / Sec 190,000 Rendimiento del IPS 6 Gbps
7.6 SERVICIO ADMINISTRADO DE IPS EN NODOS CON INTERNET DEDICADO PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET						
<p>7.6.1 Para el caso de la solución de IPS (Intrusion Prevention System) este debe estar basado en un dispositivo appliance, no se aceptará ninguna solución exclusiva por software. Debe estar basado en sistema operativo propietario.</p> <p>Pregunta técnica 13 de UNINET respecto a las funcionalidades de Firewall, IPS y Filtrado de Contenido. AXTEL toma en cuenta en su propuesta que la Convocante permite la integración de los Servicios de Firewall, IPS y Filtrado de Contenido en un solo equipo siempre y cuando se cumplan con los niveles de servicio y características solicitadas.</p>	<p>FortiOS is a security-hardened, purpose-built operating system that forms the foundation of all FortiGate platforms.</p>	<p>FortIOS 5 Network Security Operating System</p>	<p>NA</p>	<p>1</p>	<p>1</p>	<p>FortIOS es un sistema operativo de propósito-construido seguridad reforzada que forma la base de todas las plataformas FortiGate.</p>

0150



AXTEL, S.A.B. DE C.V./AVANTEL, S. DE RL. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CORNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CRECIMIENTO DE LOS TRABAJADORES (INSTITUTO FONACOT).

	10,000 New Sessions/Sec 190,000 IPS Throughput 6 Gbps					10,000 Nueva Sesiones / Sec 190,000 Rendimiento del iPS 6 Gbps
7.6.4 Los puertos LAN del equipo iPS deben ser del tipo 10/100/1000 (Mbps) con conector RJ 45 en cobre.	Total 10/100/1000 interfaces (RJ-45) FortiGate-300C 8 FortiGate-600C 16 FortiGate-800C 12	FortiGate-300C FortiGate-600C FortiGate-800C	NA NA NA	2 2 2		Interfaces 10/100/1000 (RJ-45) FortiGate-300C 8 FortiGate-600C 16 FortiGate-800C 12
7.6.5 El equipo iPS del Licitante debe bloquear diferentes tipos de tráfico peer-to-peer; el sistema debe operar en línea, el sistema no debe requerir ningún direccionamiento IP en los puertos de inspección, el sistema debe soportar un throughput listado en el Anexo "B" en función de su capacidad.	Application protection: Client usage software in risky categories, including Botnet, P2P, Proxy, and Games applications. A subscription to FortiGuard IPS updates is required. Transparent mode is so named because the device is effectively transparent in that it does not appear on the network in the way that other network devices show as a node in the path of network traffic.	FortiOS Handbook for FortiOS 5.0 FortiOS Handbook for FortiOS 5.0	NA NA	776 488	11 6	Protección de aplicaciones: El cliente utiliza el software en categorías de riesgo, incluyendo Botnet, P2P, Proxy, y aplicaciones de juegos. Se necesita una suscripción a las actualizaciones de FortiGuard iPS. (Incluida) Modo transparente se llama así porque el dispositivo es efectivamente transparente ya que no aparece en la red de la manera que otros dispositivos de red muestran como nodos en la ruta del tráfico de red.
7.6.6 El equipo debe soportar DDoS para mitigar este tipo de ataques, el equipo debe tener filtros para detectar y bloquear spyware, el	DoS policies DDoS attacks vary in nature and intensity. Attacks aimed at saturating the available bandwidth upstream of your	FortiOS Handbook for FortiOS 5.0	NA	555	3	Políticas DoS Los ataques DDoS varían en naturaleza e intensidad. Los ataques destinados a saturar el ancho de banda disponible aguas arriba de



AXTEL, S.A.B. DE C.V./AVANTEL, S. DE R.L. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE UNO NACIONAL DE SERVICIOS INTEGRADOS ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CGSENE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONAGOT).

<p>equipo debe ser capaz de bloquear y/o administrar el ancho de banda que utilizan las aplicaciones point-to-point y debe contar con servicio de actualización durante la vigencia del contrato.</p>	<p>service can only be countered by adding more bandwidth. DoS policies can help protect against DoS attacks that aim to overwhelm your server resources.</p>				<p>su servicio sólo pueden ser contratados mediante la adición de más ancho de banda. Políticas de denegación de servicio pueden ayudar a proteger contra los ataques DoS que tienen como objetivo saturar los recursos del servidor.</p>
	<p>The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units.</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA 319</p>		<p>El equipo FortiGuard se puede encontrar alrededor de las actividades de globo, virus de monitoreo, software espía y vulnerabilidad. Como se encuentran las vulnerabilidades, las firmas se crean y empujaron a las unidades FortiGate suscritas.</p>
	<p>Application protection: Client uses software in risky categories, including Botnet, P2P, Proxy, and Games applications. A subscription to FortiGuard IPS updates is required.</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA 776</p>		<p>Protección de aplicaciones: El cliente utiliza el software en categorías de riesgo, incluyendo Botnet, P2P, Proxy, y aplicaciones de juegos. Se necesita una suscripción a las actualizaciones de FortiGuard IPS. [Incluida]</p>
	<p>The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit.</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA 319</p>		<p>La Red de Distribución FortiGuard (FDN) de servidores proporciona actualizaciones de antivirus, antispam y definiciones de IPS a su unidad FortiGate.</p>

02/19



AXTEL, S.A.B. DE CV (AVANTEL, S. DE RL DE CV)
EN PARTICIPACION CONSUMIA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS (Voz, Datos, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONSEMI), LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL MIXTO DE PROTECCION AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONADOT).

<p>7.6.7 El sistema podrá tener diferentes perfiles de seguridad por cada segmento y estos segmentos se podrán agrupar de diversas maneras según sea necesario, el control de acceso se puede limitar por perfil, dispositivo o segmento de red.</p>	<p>You can group signatures into IPS sensors for easy selection when applying to firewall policies. You can define signatures for specific types of traffic in separate IPS sensors, and then select those sensors in profiles designed to handle that type of traffic.</p> <p>When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number). It also registers the incoming interface, the outgoing interface it will need to use and the time of day. Using this information the FortiGate firewall attempts to locate a security policy that matches the packet</p>	<p>FortiOS Handbook for FortiOS 5.0</p> <p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p> <p>NA</p>	<p>826</p> <p>526</p>	<p>2</p> <p>3</p>	<p>Ud puede agrupar firmas en sensores IPS para facilitar la selección cuando se aplica a las políticas de firewall. Puede definir firmas para tipos específicos de tráfico en sensores IPS separados, y luego seleccionar los sensores en los perfiles diseñados para manejar ese tipo de tráfico.</p> <p>Cuando el servidor de seguridad recibe un paquete de conexión, se analiza la dirección del paquete de origen, dirección de destino, y el servicio (por número de puerto). También registra el interfaz de entrada, la interfaz de salida tendrá que utilizar y la hora del día. Con esta información el servidor de seguridad FortiGate intenta localizar una política de seguridad que coincide con el paquete</p>
<p>7.7 SERVICIO ADMINISTRADO DE FILTRADO DE CONTENIDO EN NODOS DE INTERNET DEDICADO PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET</p>						
<p>7.7.1 Para el caso de la solución de Filtrado de Contenido este debe estar basado en un dispositivo appliance, no se aceptará ninguna solución exclusiva por software. Debe estar</p>	<p>FortiOS is a security hardened, purpose built operating system that forms the foundation of all FortiGate platforms.</p>	<p>FortiOS 5 Network Security Operating System</p>	<p>NA</p>	<p>1</p>	<p>1</p>	<p>FortiOS es un sistema operativo de propósito-construido seguridad reforzada que forma la base de todas las plataformas FortiGate.</p>



AXTEL S.A.B. DE CV (AVANTEL S. DE R.L. DE CV)
EN PARTICIPACION CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO (COGSE), LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL MIXTO DE PROTECCION AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

<p>basado en sistema operativo propietario.</p> <p><i>Pregunta técnica 13 de UNINET respecto a las funcionalidades de Firewall, IPS y Filtrado de Contenido. AXTEL toma en cuenta en su propuesta que la Convocante permite la integración de los Servicios de Firewall, IPS y Filtrado de Contenido en un solo equipo siempre y cuando se cumplan con los niveles de servicio y características solicitados.</i></p>					
<p>7.7.2 La solución podrá habilitarse mediante un equipo de propósito específico o bien un UTM (Unified Threat Management).</p>	<p>the FortiGate line combines a number of security features to protect your network from threats. As a whole, these features, when included in a single Fortinet security appliance, are referred to as Unified Threat Management (UTM).</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>770</p>	<p>1</p> <p>la línea FortiGate combina una serie de características de seguridad para proteger su red contra amenazas. En su conjunto, estas características, cuando se incluye en un único dispositivo de seguridad de Fortinet, se les conoce como gestión de amenazas unificada (UTM).</p>
<p>7.7.3 En los nodos de conectividad dedicada a Internet el Licitante debe instalar la solución de Filtrado de Contenido administrado</p>	<p>FortiGate 300C Concurrent Sessions 2 Million Firewall Throughput 8 Gbps Firewall Policies 10,000</p>	<p>FortiGate-300C</p>	<p>NA</p>	<p>2</p>	<p>FortiGate-300C Sesiones simultáneas 2 Millones Rendimiento Firewall 8 Gbps Políticas de Firewall 10,000</p>



AXTEL, S.A.B. DE C.V./AVANTEL, S. DE RL. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA DEL TRABAJO Y LA DEFENSA DEL TRABAJO (PROFUTET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGEREF", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (COMIPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

<p>especificados en el Anexo "B"; el equipo debe tener la capacidad soportar el crecimiento de por lo menos el 20% de usuarios sin ningún costo adicional.</p>	<p>Anexo "D"; el equipamiento ofertado por AXTEL tiene la capacidad soportar el crecimiento de por lo menos el 20% de usuarios sin ningún costo adicional</p>					<p>ofertado por AXTEL tiene la capacidad soportar el crecimiento de por lo menos el 20% de usuarios sin ningún costo adicional</p>
<p>7.7.6 El equipo de Filtrado de Contenido debe contar con al menos 70 categorías para una navegación segura. El equipo deberá proporcionar un servicio de seguridad que combine medidas preventivas, proactivas y reactivas para crear una solución completa de Filtrado de Contenido Web.</p>	<p>FortiGuard Web Filtering is a subscription service that allows you to limit access to web sites. More than 60 million web sites and two billion web pages are rated by category. You can choose to allow or block each of the 77 categories.</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>773</p>	<p>13</p>	<p>FortiGuard Web Filtering es un servicio de suscripción que le permite limitar el acceso a sitios web. Más de 60 millones de sitios web y de dos mil millones de páginas web se clasifican por categoría. Usted puede optar por permitir o bloquear cada una de las 77 categorías.</p>
<p>7.7.7 El equipo del Licitante debe bloquear el contenido ofensivo de la red, debe trabajar a nivel Gateway sin instalar ningún agente en los clientes finales, debe contar con listas blancas y negras, debe contar con actualizaciones al menos cada 5 minutos y debe contar con servicio de actualización durante la vigencia del contrato.</p>	<p>This section describes FortiGate web filtering for HTTP traffic. The three main parts of the web filtering function, the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service interact with each other to provide maximum control over what the Internet user can view as well as protection to your network from many Internet content</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>837</p>	<p>1</p>	<p>En esta sección se describe el filtrado web FortiGate para el tráfico HTTP. Las tres partes principales de la función de filtrado web, el Filtro de Contenido Web, el URL Filter, y el servicio de filtro web FortiGuard interactúan entre sí para proporcionar el máximo control sobre lo que el usuario de Internet puede ver, así como la protección de su red de muchos Internet amenazas de contenido. Filtrar contenido Web bloquea las páginas web que contengan palabras o</p>



AXTEL, S.A.B. DE C.V./AVANTE!, S. DE RL. 03 CV
EN PARTICIPACION CONJUNTA

CONTRATACION DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARIA DEL TRABAJO Y PREVISION SOCIAL (STPS), LA PROCURADURIA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDDT), LA COORDINACION GENERAL DEL SERVICIO NACIONAL DE EMPLEO "COSNE", LA COMISION NACIONAL DE LOS SALARIOS MINIMOS (CONASAMI), EL COMITE NACIONAL MIXTO DE PROTECCION AL SALARIO (CONAMIPRO) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

<p>threats. Web Content Filter blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter web traffic.</p>					<p>patrones que usted especifique. Filtrado de URL utiliza direcciones URL y los patrones de URL para bloquear o páginas web exentas de fuentes específicas. FortiGuard Web Filtering ofrece muchas categorías adicionales que puede utilizar para filtrar el tráfico de Internet.</p>
<p>Allow or block access to specific URLs by adding them to the URL filter list. Add patterns using text and regular expressions (or wildcard characters) to allow or block URLs. The unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message.</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>867</p>	<p>5</p>	<p>Permitir o bloquear el acceso a determinadas direcciones URL mediante su inclusión en la lista de filtros de URL. Añadir patrones usando expresiones de texto y regulares (o caracteres comodín) para permitir o URLs de bloque. La unidad permite o bloquea las páginas web a juego cualquier URL o patrones especificados y muestra un mensaje de reemplazo.</p>
<p>FortiGuard Web Filter is a managed web filtering solution available by subscription from Fortinet. FortiGuard Web Filter enhances the web filtering features supplied with your FortiGate unit by sorting</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>840</p>	<p>6</p>	<p>FortiGuard Web Filter es una solución de filtrado web gestionada disponible mediante suscripción en Fortinet. FortiGuard Web Filter mejora las funciones de filtrado web que se suministran con la unidad FortiGate clasificando miles de millones de</p>

Axtel 
Comunicate mejor.

Avantel

AXTEL, S.A.B. DE C.V./AVANTEL, S. DE RL DE C.V.
EN PARTICIPACION CONSULTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS) LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO (CONSE), LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAM), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

	billions of web pages into a wide range of categories users can allow or block. The FortiGate unit accesses the nearest FortiGuard Web Filter Service Point to determine the category of a requested web page, and then applies the security policy configured for that user or interface.					páginas web en una amplia gama de categorías de usuarios pueden permitir o bloquear. La unidad de FortiGate accede al Punto de Servicio Web Filter FortiGuard más cercano para determinar la categoría de una página web solicitada, y luego se aplica la política de seguridad configurado para ese usuario o interfaz.
7.7.8 El equipo de Filtrado de Contenido del licitante para la protección debe realizar análisis por normas, firmas, heurística, análisis de comportamiento, servicios de reputación web y categorías de URL. Prevención de efusión de proxy, filtrado para prevenir botnets, keyloggers, phishing y spyware. Identificación de contenido malicioso generado por los usuarios a medida que se publica en sitios web.	The three main parts of the web filtering function, the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service interact with each other to provide maximum control over what the internet user can view as well as protection to your network from many internet content threats. Web Content Filter blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories	FortiOS Handbook for FortiOS 5.0	NA	837	1	Las tres partes principales de la función de filtrado web, el Filtro de Contenido Web, el URL Filter, y el servicio de filtro web FortiGuard interactúan entre sí para proporcionar el máximo control sobre lo que el usuario de Internet puede ver, así como la protección de su red de muchos Internet amenazas de contenido. Filtrar contenido Web bloquea las páginas web que contengan palabras o patrones que usted especifique. Filtrado de URL utiliza direcciones URL y los patrones de URL para bloquear o páginas web exentos de fuentes específicas. FortiGuard Web Filtering ofrece muchas categorías adicionales que puede utilizar para filtrar el tráfico de Internet.



AXTEL, S.A.B. DE C.V./AVANTELL, S. DE R.L. DE C.V.
EN PARTICIPACIÓN CONJUNTA

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRABLES ADMINISTRATIVOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS) LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CONEM", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAM), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMIPOSI) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT).

<p>you can use to filter web traffic.</p> <p>threats are also becoming increasingly sophisticated. Threats and web-based applications that cause additional problems for corporations include:</p> <ul style="list-style-type: none"> • spyware/grayware • phishing • pharming • instant messaging • peer-to-peer file sharing • streaming media • blended network attacks. <p>FortiGuard Web Filter ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. Users can notify the FortiGuard Web Filter Service Points if they feel a web page is not categorized correctly, so that the service can update the categories in a timely fashion.</p> <p>It also provides behavior-based heuristics</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>838</p>	<p>1</p>	<p>amenazas también son cada vez más sofisticados. las amenazas y las aplicaciones basadas en la Web que causan problemas adicionales para las empresas incluyen:</p> <ul style="list-style-type: none"> • spyware / grayware • phishing • pharming • Mensajería Instantánea • Intercambio de archivos P2P • Streaming de Medios • Ataques de red blended <p>FortiGuard calificaciones Web Filter se realizan mediante una combinación de métodos de propiedad, incluyendo el análisis de textos, la explotación de la estructura de la red, y los calificadoros humanos. Los usuarios pueden notificar a los puntos de servicio Web filter FortiGuard si sienten que una página web no se clasifica correctamente, por lo que el servicio puede actualizar las categorías en el momento oportuno.</p> <p>También proporciona la heurística basada en el comportamiento</p>
<p>FortiGuard Web Filter ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. Users can notify the FortiGuard Web Filter Service Points if they feel a web page is not categorized correctly, so that the service can update the categories in a timely fashion.</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>840</p>	<p>9</p>	<p>FortiGuard calificaciones Web Filter se realizan mediante una combinación de métodos de propiedad, incluyendo el análisis de textos, la explotación de la estructura de la red, y los calificadoros humanos. Los usuarios pueden notificar a los puntos de servicio Web filter FortiGuard si sienten que una página web no se clasifica correctamente, por lo que el servicio puede actualizar las categorías en el momento oportuno.</p>
<p>It also provides behavior-based heuristics</p>	<p>FortiOS Handbook for FortiOS 5.0</p>	<p>NA</p>	<p>319</p>	<p>13</p>	<p>También proporciona la heurística basada en el comportamiento</p>

México, D.F., a 19 de Diciembre de 2013

PROPUESTA TECNICA

PROPUESTA INDIVIDUAL () PROPUESTA CONJUNTA (X)

CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGSNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT)

8. SOLUCIÓN DE CABLEADO ESTRUCTURADO CONVERGENTE PARA LA STPS/CONASAMI/CONAMPROS/PROFEDET

8.1 ASPECTOS GENERALES QUE DEBEN CONSIDERARSE EN EL CABLEADO ESTRUCTURADO

8.1.1 AXTEL considera que del total de los nodos en las oficinas principales ubicadas en la Ciudad de México, descritos en el Anexo "D" cuentan con cableado estructurado, sin embargo; los cableados que interconectan entre los IDFs y el MDF de los inmuebles se tiene a través de cableado UTP.

8.1.2 AXTEL se compromete a realizar el cambio del cableado de UTP a fibra óptica que soporte velocidades de 10 Gbps el cual será nuevo, redundante por la misma trayectoria; de tal forma que el MDF se interconecte con los IDFs mediante fibra óptica en los nodos especificados en el Anexo "D". AXTEL confirma que la conectividad del cableado (horizontal) que va de los jacks (puertos del usuario) a switches de acceso no será alterada, es decir permanecerá con cableado UTP existente.

8.1.3 AXTEL considera que es importante señalar que la CONVOCANTE no aceptará ningún tipo de solución improvisada, el cableado ofertado por AXTEL se compromete a entregarlo cuidando la mejor relación precio-calidad en los nodos en cuestión.

8.1.4 AXTEL se compromete a que en todo el proceso de solución desde su diseño, instalación, identificación, tendido y aceptación cumplirá con la normatividad vigente para cableado estructurado y referida en el Anexo "C".

8.1.5 AXTEL considera que para llevar a cabo el proceso de cambio de cableado de UTP a fibra óptica, todos los Licitantes podrán llevar a cabo las visitas a las instalaciones y presentar su constancia durante el proceso de apertura técnica de oferta.

8.1.6 Para todos los casos en donde se habilite el cableado de fibra óptica AXTEL se compromete a entregar al término de 20 días hábiles posteriores a la fecha de aceptación y por cada oficina (nodo) una memoria técnica que contenga entre otros un croquis a escala y con dimensiones, especificando las rutas del cableado de fibra óptica instalado y si fuera el caso el que ya estaba instalado.

8.1.7 Para el caso del cableado estructurado AXTEL, se compromete a tomar en cuenta los siguientes conceptos a fin homogeneizar criterios.

8.1.8 Suministro, Instalación, Pruebas y Memoria Técnica para Enlaces de Fibra Óptica a 10 Gbps AXTEL contempla en su propuesta tanto técnica como económica todos los elementos de conexión necesarios para el correcto funcionamiento de los enlaces como son:

8.1.8.1. Distribuidores Ópticos de 2UR para montaje en rack con organizadores de fibra incluidos.

8.1.8.2. Paneles precargados con por lo menos 6 coples tipo LC.

8.1.8.3. Módulos ciegos para distribuidor de fibra óptica.

8.1.8.4. Conectores LC pre pulidos que manejen velocidades a 10 Gbps

8.1.8.5. Jumper de fibra óptica tipo dúplex OM3 de 3mts de longitud.

8.1.8.6 Todos los materiales misceláneos necesarios para su conectorización e instalación como son epóxidos, fanouts, lijas, etiquetas, etc.

8.1.8.7 Además AXTEL contempla el suministro e instalación de tubería conduit pared delgada de por lo menos 32mm de diámetro en toda la trayectoria de la fibra óptica y registros tipo Minnel en cada nivel por donde pase la trayectoria.

8.1.8.8 Nota importante: La fibra óptica será para Interior / exterior tipo Riser a 10G tipo OM3.

8.1.8.9 El metraje tanto de fibra como de tubería será calculado por AXTEL y por ningún motivo se pagarán adicionales al proyecto ofertado.

8.1.9 Rehabilitación de Nodo de Red con Pruebas de Funcionamiento Incluidas. AXTEL se compromete a llevar a cabo la habilitación del cableado UTP Cat. 5e y/o 6 que actualmente se encuentra rematado a regletas tipo 110 como un nodo de cableado estructurado que cumpla las normas ANSI/TIA/EIA. Esto implica que AXTEL contempla dentro de su propuesta todos los

materiales pertinentes para el correcto funcionamiento del nodo de red, pruebas y memoria técnica.

8.1.10 AXTEL se compromete a entregar paneles para montaje en rack de 2UH tipo modulares vacíos de 24 puertos, Jacks RJ45 Cat. 6 negros para montaje en panel modular, tapas ciegas negras para panel modular, cordones de parcheo de fábrica de 7ft y 10ft y materiales misceláneos como son etiquetas, velcros, etc.

8.1.11 Nota importante: AXTEL se compromete a que en caso que la tirada de cable UTP actualmente existente rebase los 100 metros o no pase las pruebas de certificación, AXTEL informará a la STPS/CONASAMI/CONAMPROS/PROFEDET con pruebas fehacientes del informe. De esta manera en caso acordado por las partes le será pagado como rehabilitación completa y además por separado se le solicitará un nodo de red nuevo a AXTEL.

8.1.12 Suministro, Instalación, Pruebas y Memoria Técnica para Nodo de Red Cat. 6. AXTEL incluye dentro de su propuesta todos los elementos de conexión necesarios para el correcto funcionamiento del nodo de red como es:

- a. Cable UTP tipo Riser Cat. 6 con certificación de garantía de por lo menos 25 años sobre defectos de fabricación y/u mano de obra.
- b. Jacks Cat. 6, Patch Cord de 7 y 10FT. Cat. 6.
- c. Face Plate de 2 ventanas.
- d. Módulos ciegos blancos para face plate.
- e. Cajas aparentes PVC.
- f. Canalización perimetral y/u conduit.
- g. Canalización horizontal con escalerilla tipo malla.
- h. Materiales misceláneos y demás elementos que se deban contemplar en un nodo de red certificado.
- i. Nota importante, la volumetría de materiales es responsabilidad de AXTEL, y podrá ser validada en la visita a sitio.
- j. Finalmente se debe recordar que en cada una de las instalaciones indicadas en el Anexo "D" AXTEL se compromete a planear y entregar sus trabajos bajo la normatividad vigente para cumplir con ésta en todo momento conforme se especifica en el Anexo "C"

incluye la ductería flexible o rígida para la protección de la fibra. AXTEL aplicará el mismo procedimiento en inmuebles tipo campus donde se requiera unir dos o más edificios.

Las tareas que se llevarán a cabo en el servicio de instalación de cableado estructurado por parte de AXTEL, se listan de manera enunciativa, más no limitativa, a continuación:

- Manejo de los equipos, materiales y elementos. (Esto incluye transporte, carga, descarga y retiro de sobrantes, todo esto bajo responsabilidad y costo de AXTEL).
- Manejo, almacenamiento y control de los materiales en los inmuebles de la STPS.
- AXTEL incluye dentro de su oferta el suministro e instalación de los elementos y materiales asociados a la canalización del cableado estructurado, tales como las canaletas, tuberías, cajas de paso, ductos, amarres, soportes, marquillas y demás accesorios de instalación, correrán a cargo de AXTEL.
- AXTEL incluye dentro de su oferta que se hará cargo del suministro e instalación de los materiales de cableado estructurado tales como cables UTP, fibras ópticas, conectores de fibra óptica y de cobre, paneles de conexión, tapas plásticas, bandejas de fibra óptica y demás elementos de cableado necesarios para terminar totalmente la instalación.
- AXTEL incluye las pruebas de desempeño y verificación de calidad según se requiera por la STPS y de acuerdo como se indica más adelante en este documento.
- Todos los costos asociados a estas actividades correrán por cuenta de AXTEL.
- AXTEL incluye dentro de su propuesta la marcación y rotulación de la totalidad de los elementos de cableado estructurado y de instalación tales como cables, salidas de información, paneles, canaletas, racks, etc., de acuerdo con lo especificado en el estándar TIA/EIA 606A. Todos los costos que impliquen esta actividad se encuentran incluidos en la oferta que presenta AXTEL a la STPS.
- AXTEL incluye dentro de su presupuesto, los costos en que deba incurrir para la ejecución de tareas complementarias requeridas para la correcta instalación de cableado estructurado; listando de manera enunciativa, más no limitativa tareas como perforación de muros, pisos, remoción e instalación de cielos rasos, reparación de pinturas, entre otros.
- AXTEL incluye dentro de su propuesta todos los trabajos de instalación, reparación o mantenimiento se darán por concluidos tras la aprobación por parte de la STPS.

Consideraciones generales de AXTEL para el servicio de instalación y mantenimiento del cableado estructurado.

- AXTEL incluye dentro de su propuesta la instalación de cableado estructurado contempla una solución completa e integral para los componentes, tales como: cable UTP, conectores y jacks RJ-45, paneles de parcheo cuando el volumen de servicios a instalar así lo requiera, cordones de parcheo y placas de pared compatibles con estos

componentes; en el caso de reparación y mantenimiento AXTEL incluye los elementos necesarios para estos propósitos.

- AXTEL dentro de su oferta confirma que el cable será cable par trenzado de tipo UTP (sin blindar), Categoría 6 con 8 conductores sólidos, 24 o 23 AWG soportando un ancho de banda de 250 Mhz ó superior.
- El color de la cubierta será estandarizado.
- AXTEL confirma que todos los componentes propuestos para el cableado horizontal de cobre cumplen con la categoría 6 / Clase E a 250 Mhz o superior; en lo que respecta a Jacks, paneles de parcheo, cable UTP y conectores RJ45 son de marca que cumple con los estándares internacionales.
- AXTEL incluye las prácticas de instalación de cableado estructurado, de acuerdo a norma, por ejemplo: nivel de torcido, parte desnuda en remates, sujeción de cableado, no doblar el cable más de lo especificado por la norma, entre otros.
- AXTEL dentro de su propuesta incluye que en los cableados de fibra óptica solicitados por la STPS cuando así se requiera ofrecerá un sistema que utilice cable para uso interno con cubierta del tipo OFNR, multimodo 50/125 µm OM3 según sea el caso que aplique en distancias que soporte 10G BASE-S, así como los conectores del tipo que le indique la STPS para el sistema vertebral (BackBone).
- AXTEL confirma que es el responsable de reparar los desperfectos que se generen durante la instalación, reparación y mantenimiento de cableado, tales como: pintura en paredes y techos, sellados de barrenos, plafones, entre otros.
- AXTEL para el sistema de cableado confirma que las trayectorias serán diseñadas evitando cruces con posibles fuentes de interferencia como EMI, RFI e impulsos, generadas por líneas de alta tensión, cableado de pararrayos, balastro, conductores eléctricos, radiación solar, radares, motores, interruptores, entre otros.
- Los canales de comunicación de cableado estructurado que se instalarán por AXTEL se ajustan a lo estipulado al menos en las normas y estándares que se indican a continuación:
 - ✓ NMX-I-248-2005-NYCE.- Telecomunicaciones, Cableado, Cableado Estructurado, Cableado de Telecomunicaciones para Edificios Comerciales, Especificaciones y Métodos de Prueba.
 - ✓ NOM-001-SEDE-2005 (utilización) Artículo 770 - cables de fibra óptica y sus canalizaciones.
 - ✓ NFPA 70 y NOM-001-SEDE-2005. Sistema de Barrera contra Incendios Artículo 300-21, Propagación de fuego o productos de combustión, Artículo 645-7 Cables a través de paredes, Artículo 770-2 Lugares de Instalación y otros artículos, Artículo

800-52 (inciso b) Instalación de cables, alambres y equipos de comunicación
(Propagación de fuego o productos de combustión)

- ✓ ISO/IEC/FDIS 11801- Clase E - 2002 (E).- Estándar Internacional para cableados Estructurados en edificio local o comercial. (Information Technology - Generic cabling for customer premises)
- ✓ ANSI/TIA/EIA-568-B.1- 2001.- Estándar U.S.A. Requerimientos Generales de cableado para comunicaciones en edificio (Commercial Building Telecommunications Cabling Standard).
- ✓ ANSI/TIA/EIA-568-B.2- 2001.- Estándar U.S.A. Parte: 2 Componentes para cables balanceados de par trenzado (Balanced Twisted-Pair Cabling Components).
- ✓ ANSI/TIA/EIA-568-B.2-1 2002.- Estándar U.S.A. Parte: 2 Proyecto 1. Componentes para cables balanceados de par trenzado, Especificaciones para cableado de Cat. 6 (Transmission Performance Specifications for 4-pair 100Ω Category 6 Cabling).
- ✓ ANSI/TIA/EIA-568-B.3- 2000.- Estándar U.S.A. Componentes para cableado de Fibra Óptica (Optical Fiber Cabling Components Standard).
- ✓ TIA/EIA 604 FOCIS Estándar de conectores de fibra óptica tipo SFFC
- ✓ EIA/TIA-569-A. -Lineamientos para rutas y espacios de comunicaciones en Edificios Comerciales (Commercial Building Standard For Telecommunications Pathways and Spaces).
- ✓ EIA/TIA-606. -Lineamientos de Administración para la infraestructura de telecomunicaciones en Edificios Comerciales (Administration Standard for the Telecommunications Infrastructure of Commercial Building)
- ✓ J-STD-607-A. -Lineamientos estándares de aterrizaje para telecomunicaciones en Edificios Comerciales.

Características técnicas ofertadas por AXTEL para los elementos utilizados en el servicio de instalación de cableado estructurado

AXTEL dentro de su oferta incluye los servicios del cableado estructurado horizontal los cuales tendrán una topología tipo estrella, cada servicio con un solo cable desde el Panel de Patcheo hasta la salida de telecomunicaciones del usuario, con una longitud máxima de 90 metros, sin empalmes y quedarán colocados dentro de la canalización instalada para estos fines (u excepción, en su caso, de aquellos servicios que se identifiquen), formando canas y amuradas con cinturones de plástico o velcro sobre la escalerilla según sea la necesidad y considerando el futuro mantenimiento, dentro de la canaleta o ductos perimetrales que se instalen, con la finalidad de facilitar los trabajos de mantenimiento y reubicación de los servicios de telecomunicaciones.

Para los cables de servicio provenientes de las estaciones de trabajo, AXTEL suministrará en paneles de patcheo de 48 o 24 puertos dependiendo de la cantidad de servicios, éstos equipados con espacio frontal para rótulos en colores o identificación de acuerdo a la EIA/TIA 606.

Todos los elementos del cableado se identificarán mediante el formato propuesto en el último draft de la norma TIA/EIA 606B.

Todos los extremos de los cables que llegan al sistema de paneles de parcheo y a las tomas de telecomunicaciones (placas frontales), quedarán completamente identificados mediante etiquetas integradas y protegidas.

AXTEL dentro de su propuesta incluye las siguientes características al menos para los elementos de calidad móvil para los servicios de instalación, reparación y mantenimiento de cableado estructurado en las cuales los elementos pueden ser de diferentes marcas:

Cable UTP (instalación):

- ✓ Trenzado de 4 pares, Categoría 6, con un desempeño probado a 250MHz o superior
- ✓ Conductor 23-24 AWG sólido
- ✓ Cubierta retardante de flama
- ✓ Impedancia de 100±5 Ohms.

Jack Modular RJ45 Cat. 6/Clase E

- ✓ Conector hembra (Jack) categoría 6 a 250Mhz o superior
- ✓ De 4 pares (8 conductores) tipo RJ-45
- ✓ Con etiqueta de código de colores para alambrado tipo T 568A o T 568B
- ✓ Fabricado con plástico de alto impacto retardante a la flama UL-40

Placa Frontal

- ✓ Fabricada en PVC de alto impacto y retardante a la flama UL-40
- ✓ Con capacidad de 2 o 4 ventanas
- ✓ Cuenta con ventanas para etiquetación.
- ✓ Incluye tornillería para su montaje

Cables de Parcheo

- ✓ Categoría 6 / Clase E
- ✓ Para el cuarto de telecomunicaciones, con una longitud de 3 ft.
- ✓ Para la salida del usuario, con una longitud de 10 ft.
- ✓ Terminación en cada extremo con plugs RJ-45
- ✓ Manufacturados y terminado de fábrica.
- ✓ Dos tipos de patch cord, para usuario (Más Flexible) y para rack (Más Rígido)

Panel de parcheo Cat. 6/Clase E (en caso de requerirse dado el volumen)

- ✓ Paneles de 24 o 48 puertos (ZUR), con conectores hembra RJ-45.
- ✓ Montable en rack de 19"

Instalaciones que contemplen fibra óptica:

- ✓ AXTEL incluye los siguientes elementos al menos para fines de instalación y mantenimiento:

01/07/2018

Cable Fibra Óptica Horizontal y Backbone de 50/125µm, del tipo de Tubo Apretado (Tight Buffer) para uso Interior

- ✓ Fibra óptica multimodo de Índice gradual de 50/125 µm OM3 LOMMF, tipo interior, que cumple con los parámetros de transmisión especificados en EIA/TIA 568B.3, con 6 conductores (hilos) ópticos y las siguientes características:
- ✓ Diámetro del núcleo de los conductores ópticos = 50 µm.
- ✓ Diámetro del recubrimiento del núcleo (cladding) = 125 µm.
- ✓ Diámetro de la cubierta protectora (buffer) = 900 µm.
- ✓ Resistencia mecánica suficiente para ser instalada en las canalizaciones para interior.
- ✓ Ventanas de transmisión 850 y 1300 nm.
- ✓ Atenuación máxima de 3.0 dB/km @850 nm y 1.0 dB/km @1300 nm
- ✓ Ancho de banda mínimo, OFL 1500 MHz-km @850 nm y 500 MHz-km@1300nm
- ✓ Ancho de banda mínimo, Láser 2000 MHz-km @850 nm y 500 MHz-km@1300nm
- ✓ Retraso en modo diferencial que cumpla o exceda la TIA-492AAAC-A [IEC-60793-2-10ed2]@850nm y 0.88 ps/m @1300nm
- ✓ Código de colores individuales en los conductores ópticos para facilitar su identificación, conforme a lo especificado en TIA-598.

Conectores para fibra óptica

- ✓ Los conectores son compatibles con los paneles y fibra propuestos en este proyecto.
- ✓ La tolerancia de pérdida promedio de 0.1 dB, desviación estándar 0.1 dB
- ✓ Cambio de pérdida de inserción <0.3 dB
- ✓ Temperatura de operación = -40° a 75° C y retardante a la flama según UL-94 V-0.
- ✓ Son para el tamaño de las fibras 125µm
- ✓ Ancho de banda aprobada a 500 MHz/km, OFL.
- ✓ Durabilidad de conexión (dB) 500 ciclos
- ✓ Cumple con los estándares ISO/IEC 11801, EIA/TIA 568 y TIA 604.

Panels de Distribución de Fibra Óptica

- ✓ Son metálicos 1 UR, y montables en rack 19"
- ✓ Cuentan con paneles de conectorización con acopladores según requerimiento, que cumpla con las especificaciones del estándar TIA/EIA-568B.3, TIA/EIA 606, ISO11801 2d. Ed. y EN50173 para la interconexión de cables de fibra óptica de 50/125µm, tipo interior y el cordón de parcheo duplex.
- ✓ Incluye accesorios para garantizar el radio mínimo de curvatura de 10 veces el diámetro exterior de la fibra.

- ✓ Capacidad para 12 fibras
- ✓ Cumple con los estándares Internacionales ISO/IEC 11801 y EIA/TIA 568.

Jumpers de Fibra Óptica según requerimiento

- ✓ Configuración duplex, de 50/125 μ m con conectores según el equipo activo que le indique la STPS, de 1mt.
- ✓ Cubierta en OFNR

Racks

- ✓ Todos los componentes del cableado a instalar tales como paneles de patcheo, regletas, organizadores verticales y horizontales se montarán en los racks destinados para estos fines, en caso de requerirse nuevos racks, éstos serán abiertos y de 4 o 7 pies de altura, dependiendo de la cantidad de nodos a instalar y equipos de comunicaciones, de aluminio, pintado con pintura horneada en color negro, cuenta con la numeración de unidades de Rack para su fácil identificación.
- ✓ En el rack se identificarán los cables de cada salida con el número de servicio, segmento asignado y el símbolo del servicio.
- ✓ Cuentan con los organizadores verticales y horizontales necesarios para una correcta organización del cableado.
- ✓ Cuentan con barra vertical de al menos 10 contactos de 20 Amperes, montada en el rack.

Canalización (de ser necesaria)

- ✓ La canalización es de canaleta plástica de PVC para cable UTP categoría 6, de 1 o 3 vías según los servicios que se requieran; se instalará con los accesorios y acopladores requeridos, tales como esquineros, coples, piezas tipo L o tipo T, etc., con los radios de curvatura que corresponden a sistemas de cableado estructurado categoría 6.
- ✓ En caso de que por características del inmueble se requiera usar tubería, ya sea de pared gruesa o pared delgada, será galvanizada con un diámetro que garantice, al menos, el 60% de espacio libre en el interior del tubo y quedará aterrizada eléctricamente.
- ✓ Siempre que sea necesario librar una columna, se usará también tubo conduit pared delgada o gruesa galvanizado preparando manualmente la curvatura que cada caso requiera. Se usaran codos prefabricados, siempre y cuando no se afecte el nivel de calidad requerido en estas especificaciones.
- ✓ Para la sujeción de ductería se utilizará unicanal de 4X2 cms, abrazaderas tipo pera y soportaría por medio de varilla roscada. Se usará herramienta de impacto para la instalación de soportes y utilizar clips tipo U de acero para montar la ductería sobre el soporte.

- ✓ Todo el sistema de tubería quedará perfectamente acoplado, utilizando los componentes de acoplamiento requeridos, tales como coples, codos, terminadores, cajas de paso, etc.
- ✓ En exteriores, AXTEL incluye los elementos necesarios para garantizar el adecuado funcionamiento del sistema de cableado, por ejemplo, sellar acoplamientos de tuberías, garantizar su seguridad, pintado, etc.
- ✓ De requerirse AXTEL empleará escalerilla electrosoldada en la conducción general del cableado.

Atentamente

Bajo protesta decir verdad
Jorge Vicente Martínez Rendón
Representante Común

11/01/11

**CARTA DE DISTRIBUIDOR AUTORIZADO
Y DE CONTAR CON EL PERSONAL CAPACITADO.**

MÉXICO, D.F. A 19 DE DICIEMBRE DE 2013

SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y
SERVICIOS GENERALES
DIRECCIÓN DE ADQUISICIONES Y ALMACENES
AVENIDA ANILLO PERIFÉRICO SUR No 4271,
NIVEL 5, EDIFICIO "B", COL. FUENTES DEL PEDREGAL
C.P. 14140, MÉXICO, D.F.

JOSÉ FRANCISCO MAZÓN ESCUTIA, EN MI CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA FORTINET INC., BAJO PROTESTA DE DECIR VERDAD, Y EN RELACIÓN AL PROCESO DE ADJUDICACIÓN DIRECTA, OFICIO No. 512.1/16-12-2013/1091 BIS, REFERENTE AL SERVICIO DE CONTRATACIÓN DEL SERVICIO DE RED NACIONAL DE SERVICIOS INTEGRALES ADMINISTRADOS DE VOZ, DATOS, INTERNET Y VIDEOCONFERENCIA, PARA LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL (STPS), LA PROCURADURÍA FEDERAL DE LA DEFENSA DEL TRABAJO (PROFEDET), LA COORDINACIÓN GENERAL DEL SERVICIO NACIONAL DE EMPLEO "CGSNE", LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS (CONASAMI), EL COMITÉ NACIONAL MIXTO DE PROTECCIÓN AL SALARIO (CONAMPROS) Y EL INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES (INSTITUTO FONACOT), MANIFESTAMOS QUE AXTEL, SAB DE CV, ES DISTRIBUIDOR AUTORIZADO Y QUE CUENTA CON EL PERSONAL TÉCNICO CALIFICADO PARA INSTALAR, CONFIGURAR, ADMINISTRAR Y MONITOREAR LOS ELEMENTOS DE SEGURIDAD PERIMETRAL QUE SON INSTALADOS.

EXTENDEMOS LA PRESENTE A PETICIÓN DE AXTEL, SAB DE CV, Y PARA LOS FINES QUE JUZGUE CONVENIENTES.