BASES DE LA LICITACIÓN PÚBLICA
NÚMERO 006/2014 (LP-006-2014)
PARA EL **"SERVICIO DE LA RED MPLS E INTERNET"**

FONDO DE OPERACIÓN GENÉRICO
NOVIEMBRE 2014

COSTO $40.00

000048

CONTENIDO

BASES DE LA LICITACIÓN PÚBLICA NÚMERO LP-006-2014, REFERENTE AL SERVICIO DE LA RED MPLS E INTERNET.

La Universidad Autónoma del Estado de México, por conducto de la Secretaría de Administración, a través de la Dirección de Recursos Materiales y Servicios Generales, con fundamento en lo dispuesto por los artículos 129 de la Constitución Política del Estado Libre y Soberano de México; 1, 4 fracción I, 9, 10, 11, 14, 26, 28, 29, 30 fracción I, 32, 33, 34 y 35 de la Ley de Contratación Pública del Estado de México y Municipios; 1, 2, I, 11, 16, 38 fracción, 39 primer párrafo, 46, 47, 48, 50, 52, 53, 54, 55, 56, 57, 58, 59, 60 y 61 del Reglamento de Adquisiciones, Arrendamientos y Servicios de la Universidad Autónoma del Estado de México, lleva a cabo la **LICITACIÓN PÚBLICA** número **LP-006-2014**, referente a los servicios de red MPLS e internet, en términos de las siguientes:

B A S E S

I. INFORMACIÓN ESPECÍFICA DE LA CONTRATACIÓN.

I.1. IDENTIFICACIÓN DEL REQUERIMIENTO.

I.1.1. GIRO: **COMUNICACIÓN**
I.1.2. TIPO DE GASTO: (**X**) ORDINARIO ( ) INVERSIÓN **( )** EXTRAORDINARIO
I.1.3. NÚMEROS DE REQUISICIONES:
I.1.4. ÁREA REQUIRENTE: **DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES**
I.1.5. CONVOCATORIA: **PRIMERA.**
I.1.6. NUMERO: 006 **(LP-006-2014)**
I.1.7. PERÍODO DE VENTA DE BASES: **DEL 11 AL 12 DE NOVIEMBRE DE 2014.**

I.2. DESCRIPCIÓN DE LA ADQUISICIÓN.

El objeto de la presente Licitación es contratar **SERVICIOS DE RED MPLS E INTERNET,** cuyas características y especificaciones mínimas que deberán cubrir y satisfacer se detallan en el **ANEXO TÉCNICO**, considerando en todo momento que el o los proveedores adjudicados deberán garantizar la estabilidad de los servicios de red MPLS e internet a proporcionar.

Los servicios incluidos que el o los proveedores adjudicados proporcionarán a la UAEM, incluyen los conceptos contenidos en el Anexo Técnico.

000047

1.3. CONDICIONES BÁSICAS DE LA CONTRATACIÓN QUE LOS OFERENTES DEBEN SEÑALAR EN SUS PROPUESTAS.

1.3.1. CONDICIONES COMERCIALES DE LA CONTRATACIÓN.

1.3.1.1. LUGAR DE ENTREGA.

En los sitios y horarios determinados en el Anexo Técnico de las Bases, mediante un cronograma de suministro e instalación que le será entregado al licitante que resulte adjudicado.

1.3.1.2. PLAZO DE ENTREGA.

Los bienes y/o servicios deberán ser entregados de acuerdo al cronograma que se defina con el proveedor adjudicado y no deberá exceder de **58 días naturales** contados a partir del día siguiente a la fecha de la notificación del fallo; esto es, a más tardar el día **miércoles treinta (30) de enero de 2015,** y de acuerdo al cronograma de suministro.

1.3.1.3. CALIDAD DE LOS SERVICIOS.

Señalar expresamente que los servicios satisfacen ampliamente los requisitos indicados en el **ANEXO TÉCNICO**.

Se hace la aclaración de que los servicios deberán ajustarse a las especificaciones técnicas requeridas en el **ANEXO TÉCNICO.** No se aceptarán bienes y/o servicios que no cumplan con las especificaciones técnicas establecidas en el Anexo Técnico de las Bases.

1.3.1.4. VISITA FÍSICA.

Los oferentes participantes deberán asistir a la visita física en los domicilios de los siguientes espacios académicos y administrativos, conforme a las fechas y horarios que a continuación se señalan:

Sitio	Dirección	Fecha y hora de visita
DTIC	Cerro de Coatepec S/N, Toluca, México	Miércoles 19 de noviembre de 2014 a las 19:00 horas.
CU Amecameca	Carr. Amecameca-Ayapango, Km 2.5, Amecameca, México	Jueves 13 de noviembre de 2014 a las 10:00 horas.
CU Atlacomulco	Km 80 Autopista Toluca-Atlacomulco, Atlacomulco, México	Martes 18 de noviembre de 2014 a las 10:00 horas.
CU Ecatepec	José Revueltas Núm. 17, Ecatepec, México	Jueves 13 de noviembre de 2014 a las 12:00 horas.
CU Tejupilco	Rincón de Aguirre S/N, Tejupilco, México	Martes 18 de noviembre de 2014 a las 16:00 horas.
CU Temascaltepec	Km 67.5 carretera Toluca-Temascaltepec, Temascaltepec, México	Martes 18 de noviembre de 2014 a las 17:00 horas.

CU Tenancingo	Ex. Hacienda Santa Ana, Tenancingo, México	Martes 18 de noviembre de 2014 a las 13:30 horas.
CU Teotihuacán	Santo Domingo Aztacameca, Teotihuacán, México	Jueves 13 de noviembre de 2014 a las 16:00 horas.
CU Texcoco	Km. 8.5 Carretera Texcoco –Los Reyes La Paz. Av. Jardín Zumpango S/N Fracc. El Tejocote Texcoco –Los Reyes la Paz, Edo. de Méx.	Jueves 13 de noviembre de 2014 a las 18:00 horas.
CU Valle de Chalco	Hermenegildo Galeana no.3 Col. María Isabel Valle de Chalco, México	Viernes 14 de noviembre de 2014 a las 19:00 horas.
CU Valle de México	Blvd. Universitario S/N, Atizapán de Zaragoza	Viernes 14 de noviembre de 2014 a las 15:00 horas.
CU Zumpango	Camino viejo a Jilotzingo continuación calle Rayón, Valle Hermoso, Zumpango, México	Viernes 14 de noviembre de 2014 a las 11:30 horas.
Prepa Amecameca	Prolongación Francisco Sarabia S/N, Amecameca, México	Jueves 13 de noviembre de 2014 a las 10:30 horas.
Prepa Atlacomulco	Km 58 Autopista Toluca, Atlacomulco, México	Lunes 18 de noviembre de 2014 a las 10:30 horas.
Prepa Tenancingo	Dr. Genaro Días Mañón S/N, Tenancingo, México	Martes 18 de noviembre de 2014 a las 14:00 horas.
Prepa Texcoco	Av. Benjamin Aguilar Talavera No. 1, Texcoco, México	Jueves 13 de noviembre de 2014 a las 18:30 horas.
UAP Chimalhuacán	Calle primavera S7N esq. Nezahualcóyotl, Chimalhuacán, México	Jueves 13 de noviembre de 2014 a las 12:00 horas.
UAP Cuautitlán Izcalli	Prolongación Isis S/N, Cuautitlán Izcalli, México	Viernes 14 de noviembre de 2014 a las 13:00 horas.
UAP Nezahualcóyotl	Bordo de Xochiaca S/N, Nezahualcóyotl, México	Viernes 14 de noviembre de 2014 a las 18:00 horas.
UAP Tianguistenco	Paraje el Tejocote s/n, san Pedro Tlaltizapan, Tianguistenco, Edo de México	Martes 18 de noviembre de 2014 a las 11:30 horas.
Facultad de Ciencias de la Conducta	Filiberto Gómez S/N, Toluca, México	Miércoles 19 de noviembre de 2014 a las 16:00 horas.
Facultad de Contaduría - Los Uribe	Av. Río Papaloapan, Toluca, México	Miércoles 19 de noviembre de 2014 a las 17:30 horas.
Prepa 2	Av. Nezahualcóyotl S/N, Toluca, México	Miércoles 19 de noviembre de 2014 a las 11:30 horas.
Prepa 3	H. Colegio S/N esq. Diego Rivera S/N, Toluca, México	Miércoles 19 de noviembre de 2014 a las 14:30 horas.
Prepa 4	Chalco S/N, Toluca México	Miércoles 19 de noviembre de 2014 a las 13:00 horas.
Prepa 5	Heriberto Enriquez 200, Toluca, México	Miércoles 19 de noviembre de 2014 a las 10:00 horas.
UAP Huehuetoca	Av. De nuestra Señora de Los Ángeles S/N, Huehuetoca, México	Viernes 14 de noviembre de 2014 a las 10:00 horas.
UAP Acolman	Av. Juárez S/N, Acolman, México	Viernes 14 de noviembre de 2014 a las 17:00 horas.

000046

1.3.1.5. GARANTÍA DE LOS BIENES Y SERVICIOS.

Los servicios deberán apegarse a los niveles de servicio, calidad, disponibilidad y sanciones establecidas en el **ANEXO TECNICO** durante la vigencia del contrato, la cual será de **tres (3) años**.

1.3.2. CONFIDENCIALIDAD DE LA INFORMACIÓN.

Los oferentes participantes deberán requisitar e integrar a su oferta técnica la carta de confidencialidad contenida en los anexos del presente procedimiento adquisitivo.

En todo caso, el licitante adjudicado deberá sujetarse a un contrato de confidencialidad de la información almacenada en los equipos de comunicación y seguridad utilizados para la entrega de los servicios, cuando se tenga contacto con ésta derivado de la operación, configuración, mantenimiento, administración, control, soporte y atención a incidentes derivados de los servicios especificados.

1.3.3. CONDICIONES ECONÓMICAS DE LA ADQUISICIÓN.

1.3.3.1. FORMA DE PAGO:

De manera mensual a mes vencido, dentro de los **20 días hábiles**, contados a partir de la entrega y presentación de la factura en la Dirección de Recursos Materiales y Servicios Generales de la UAEM; a entera satisfacción del área usuaria. **No aplicarán intereses, ni se otorgarán anticipos.**

1.3.3.2. VIGENCIA DE LA OFERTA:

La vigencia de la oferta deberá ser indicada como mínimo, de **45 días naturales**, contados a partir de la fecha de celebración del acto de presentación y apertura de ofertas, misma que deberá colocarse tanto en su oferta técnica como económica.

2. REQUISITOS QUE DEBERÁN CUBRIR INVARIABLEMENTE LOS OFERENTES Y DOCUMENTACIÓN QUE DEBERÁN PRESENTAR.

2.1. REQUISITOS DE LOS OFERENTES.

2.1.1. Poseer la capacidad administrativa, financiera, legal y, en su caso, técnica, para atender el requerimiento en las condiciones solicitadas.

2.1.2. Estar debidamente acreditado ante la Secretaria de Comunicación y Transportes para prestar los servicios objeto de la presente Licitación Pública, anexando copia simple del documento que lo respalde para efectos del presente acto adquisitivo.

2.1.3. No encontrarse en ninguno de los supuestos que consigna el artículo 42 del Reglamento de Adquisiciones, Arrendamientos y Servicios de la Universidad Autónoma del Estado de México. **(ANEXO DOS).**

2.1.4. Manifestar, bajo protesta de decir verdad, si dentro de su representada participan servidores universitarios. **(ANEXO DOS).**

2.2. REPRESENTACIÓN.

El oferente deberá formalizar cada uno de los actos del presente concurso por Licitación Pública, personalmente **(para el caso de persona física),** o por conducto de su representante o representantes que cuenten con facultades legales suficientes **(para el caso de persona moral);** debiendo presentar copia simple del poder notarial que acredite dicho carácter.

2.3. DOCUMENTOS QUE DEBERÁN PRESENTAR LOS OFERENTES.

2.3.1. Escrito bajo protesta de decir verdad, de ausencia de impedimentos y de que cuenta con capacidad administrativa, financiera, legal y técnica; elaborado en términos del **ANEXO DOS** de estas bases, conforme al texto establecido. (Invariablemente)

2.3.2. La garantía ofrecida en términos del **ANEXO UNO.** (Invariablemente)

2.3.3. Recibo de pago de las bases, correspondiente al presente procedimiento adquisitivo y dentro de la oferta técnica. (Invariablemente)

2.3.4. Certificado de Empresa Mexiquense vigente. (Optativo, Empresas que cuenten con el mismo).

2.3.5. Escrito señalando domicilio para oír y recibir notificaciones.

2.3.6. Requisitar el Anexo Tres de las presentes bases.

2.3.7. Carta bajo protesta de decir verdad mediante la cual indique los servicios que ofrece, así como las especificaciones generales de su infraestructura de comunicaciones y centro de atención que permita verificar que tiene la capacidad de atender requerimientos iguales o superiores a lo solicitado en el Anexo Técnico de las presentes Bases.

2.3.8. Carta bajo protesta de decir verdad, en la que el oferente asume la responsabilidad absoluta para la construcción de la red MPLS y enlaces a Internet.

000045

2.3.9. Estrategia efectiva de manejo del tráfico, con el fin de asegurar los niveles de servicio, así como también optimizar recursos de uso de la RPV, considerando como puntos más importantes para el manejo del tráfico:

- •Calidad de Servicio
- •Clase de Servicio

2.3.10. Las EMPRESAS CON REGISTRO VIGENTE EN EL PADRÓN DE PROVEEDORES de la U.A.E.M. deberán presentar:

(Los oferentes participantes deberán presentar solamente copia simple de los documentos solicitados; el proveedor que resulte adjudicado deberá presentar los originales para su cotejo correspondiente).

- Cédula expedida por el Departamento de Procesos de Contratación y Seguimiento de Adquisiciones en la que se hace constar que es proveedor vigente en el giro correspondiente.
- Declaración Fiscal Anual enterada del ejercicio inmediato anterior (**2013 para personas físicas y personas morales**), en la que se contenga la cadena original y el sello digital de recepción del Servicio de Administración Tributaria (SAT).
- Último pago provisional de impuestos (correspondiente a los meses de **septiembre u octubre de 2014**).
- Identificación personal con validez oficial (credencial de elector o pasaporte) de la persona que firma las ofertas técnica y económica.
- Requisitar el Anexo Dos de las presentes bases.

2.3.11. EMPRESAS SIN REGISTRO EN EL CATÁLOGO DE PROVEEDORES DE LA U.A.E.M.

(Los oferentes participantes deberán presentar solamente copia simple de los documentos solicitados; el o los proveedores que resulten adjudicados deberán presentar los originales para su cotejo correspondiente).

- Acta Constitutiva del oferente o Instrumento Público realizado ante Notario Público, debidamente inscrito; así como sus respectivas modificaciones a partir del año 2000, en el caso de personas jurídico-colectivas o Acta de Nacimiento expedida por autoridad civil competente para el caso de personas físicas.
- Alta ante la Secretaría de Hacienda y Crédito Público, en donde su actividad preponderante sea la fabricación y/o distribución de los bienes y/o servicios solicitados.

- Cédula de identificación fiscal.

- Estados Financieros (Balance General y Estado de Resultados) al 31 de diciembre del ejercicio anterior y parcial de **septiembre u octubre de 2014**, firmados en forma autógrafa por Contador Público titulado, incluyendo el número de Cédula Profesional). No se aceptarán firmas escaneadas.

- Cédula Profesional del Contador Público que firma los Estados Financieros.

- Declaración Fiscal anual, enterada del ejercicio inmediato anterior, (**2013 para personas físicas y personas morales**), en la que se contenga la cadena original y el sello digital de recepción del Servicio de Administración Tributaria (SAT).

- Último pago provisional de impuestos (correspondiente a los meses de **septiembre u octubre de 2014**).

- Identificación personal con validez oficial (credencial de elector o pasaporte) de la persona que firma las ofertas técnica y económica.

- Poder Notarial del apoderado legal ó representante.

- En el caso de asistir persona distinta al representante legal deberá requisitar e integrar a su oferta técnica el ANEXO DOS incluido en las presentes bases.

3. CELEBRACIÓN DE LA PRIMERA Y ÚNICA JUNTA ACLARATORIA.

3.1. Los oferentes que deseen participar en la primera y única junta de aclaraciones (optativa), deberán presentar su recibo de pago de bases, la cual tendrá verificativo el día **21** de ***NOVIEMBRE*** de **2014** a las **10:00 horas**, en las oficinas que ocupa la Dirección de Recursos Materiales y Servicios Generales, ubicada en el edificio marcado con el número 510 de la calle Rayón Sur, colonia Cuauhtémoc; en Toluca, Estado de México.

3.2. Los oferentes interesados deberán registrarse a más tardar a las 10:00 horas del día viernes veintiuno (21) de noviembre de 2014, en el Departamento de Procesos de Contratación y Seguimiento de Adquisiciones, de la Universidad Autónoma del Estado de México.

3.3. A partir de la hora de cierre del registro señalado para la Junta Aclaratoria, no podrá aceptarse la participación de otras personas que hayan adquirido bases, aún cuando ésta no haya iniciado.

000044

3.4. Los oferentes que participen en el acto de Junta de Aclaraciones deberán formular por escrito preguntas o solicitar aclaraciones sobre los plazos o aspectos establecidos en las presentes bases de manera personal. En ningún caso, con motivo de las preguntas o aclaraciones, se podrá sustituir o variar sustancialmente el bien convocado ni adicionar otros distintos. **(ANEXO CINCO).**

3.5. Con el objeto de agilizar el planteamiento y respuesta de las preguntas, los oferentes **deberán entregarlas personalmente, junto con la copia simple del comprobante de pago de Bases, en impreso y en electrónico (archivo Word)**, a más tardar el día **jueves veinte (20) de noviembre de 2014**, en un horario de **9:00 a 11:00 horas**, en las oficinas que ocupa el Departamento de Procesos de Contratación y Seguimiento de Adquisiciones de la Dirección de Recursos Materiales y Servicios Generales, ubicadas en el edificio marcado con el número 510, de la calle Rayón Sur, Colonia Cuauhtémoc, Toluca, Estado de México. **No se recibirán preguntas después de la fecha y horario indicados** en este párrafo.

3.6. Las aclaraciones que se deriven de la Junta formarán parte integral de las bases, y se entregará copia simple del acta correspondiente a los oferentes que acrediten haber adquirido las mismas.

3.7. No se permitirá el uso de celulares, radio localizadores, aparatos de telecomunicación o equipos de cómputo.

3.8. Todas las personas que asistan a este acto deberán observar un comportamiento decoroso, ya que de lo contrario, la Convocante podrá expulsar del lugar a cualquier persona.

3.9. Los oferentes que no asistan a la Junta de Aclaraciones, podrán acudir ante el Departamento de Procesos de Contratación y Seguimiento de Adquisiciones, hasta un día hábil anterior a la fecha de celebración del acto de Presentación y Apertura de Proposiciones correspondiente, para conocer de manera específica los aspectos desahogados en la misma, previa comprobación del pago de bases.

La inatendibilidad de lo dispuesto en el párrafo que antecede será en perjuicio del oferente participante correspondiente.

4. INSTRUCCIONES PARA LA ELABORACIÓN DE OFERTAS.

4.1. INDICACIONES GENERALES PARA LA ELABORACIÓN DE OFERTAS.

4.1.1. Los oferentes **deberán** presentar en sobre cerrado, por separado y en original, una oferta técnica y una oferta económica.

4.1.2. En la elaboración de dichas ofertas, los oferentes **deberán** observar las indicaciones generales siguientes:

4.1.2.1 Se deberá indicar el nombre de la empresa y los documentos correspondientes se elaborarán en papel membretado de la misma y **numerados en orden progresivo.**

4.1.2.2. Se elaborarán en forma mecanográfica, en términos claros e indubitables, sin raspaduras, enmiendas, entrelíneas o tachaduras.

4.1.2.3. Se formularán en idioma español.

4.1.2.4. Se dirigirán a la Dirección de Recursos Materiales y Servicios Generales de la UAEM.

4.1.2.5. Se anotará el nombre del propietario o del representante legal de la empresa de forma mecanográfica, así como su **firma autógrafa en todas y cada una de las hojas (sin excepción), que integran tanto la oferta técnica como la económica; así como en los demás documentos requeridos, como parte integral de las propuestas.**

4.1.2.6. Anotar en la ofertas que correspondan las aclaraciones que, en su caso, se hayan acordado durante la Junta de Aclaraciones; y

4.1.2.7. Señalar expresa y textualmente las condiciones básicas de la adquisición requeridas en los puntos 1.3.1. y 1.3.2. de las bases.

4.2. REQUISITOS ESPECÍFICOS DE LA OFERTA TÉCNICA.

La oferta técnica **deberá** contener, como mínimo, lo siguiente:

4.2.1. La descripción detallada de los servicios descritos en el **ANEXO TÉCNICO,** con las especificaciones técnicas completas, marca, modelo y demás características de los servicios cotizados y bienes involucrados.

4.2.2. El señalamiento textual de las condiciones comerciales de la propuesta, sujetándose, estrictamente a lo establecido en el punto 1.3.1. de las presentes bases.

4.2.3. En su caso, los servicios agregados que, sin costo alguno, ofrece el participante.

4.2.4. Presentación de documentos solicitados en el punto 2.3. de las presentes bases.

4.3. REQUISITOS ESPECÍFICOS DE LA OFERTA ECONÓMICA.

La oferta económica **deberá** contener, como mínimo, lo siguiente:

4.3.1. La descripción genérica de los servicios ofertados en su propuesta técnica.

000043

4.3.2. Los precios unitarios y totales de los bienes ofertados, antes de ser incluido el Impuesto al Valor Agregado (I.V.A.), indicando un subtotal general antes de IVA, el IVA que le corresponde y un total final con éste incluido; así como los demás descuentos y cargos que, en su caso, considere la empresa; debiendo expresarse en moneda nacional. (Se incluye ejemplo)

No. Partida	Nombre del Artículo	Unidad de Medida	Cantidad	Marca que ofrece	Precio Unitario (antes de IVA)	Importe total (antes de IVA)
1	Protector de pantalla 17"	Pieza	20	Steren	$100.00	$2,000.00
2	Botas tipo militar	Pieza	30	Crucero	$200.00	$6,000.00
					Subtotal: (antes de IVA)	$8,000.00
					IVA:	$1,200.00
					Total: (Incluye IVA)	$9,200.00

Importe total neto: $9,200.00 (Nueve mil doscientos pesos 00/100 m.n.)

4.3.3. El importe total neto de la propuesta, con número y letra; en el caso de resultar alguna controversia, se estará a lo propuesto en letra.

4.3.4. El señalamiento de las condiciones económicas de la propuesta, sujetándose estrictamente a lo establecido en el punto 1.3.2. de las presentes bases.

5. PRESENTACIÓN DE PROPUESTAS.

5.1. INDICACIONES GENERALES.

5.1.1. Los oferentes **deberán** presentar, personalmente o a través de su representante legal, una oferta técnica y una oferta económica.

5.1.2. Las ofertas se presentarán en el lugar, día y hora señalados para la celebración del acto de presentación y apertura de propuestas.

5.1.3. Las ofertas se presentarán **por separado**, en sobres cerrados, los cuales **deberán** contener en el anverso los siguientes datos:

5.1.3.1. Nombre, denominación o razón social del oferente.

5.1.3.2. Indicar si la oferta es técnica o económica; y

5.1.3.3. Número de Licitación Pública.

5.2. PRESENTACIÓN DE LA OFERTA TÉCNICA.

5.2.1. La oferta técnica se presentará en sobre cerrado, acompañada, para este caso, de los folletos técnicos y demás documentos relativos en idioma español.

5.2.2. Los documentos que refiere el punto 2.3. y 2.4.5. de estas bases, deberán presentarse simultáneamente con la oferta técnica **dentro del sobre.**

5.3. PRESENTACIÓN DE LA OFERTA ECONÓMICA.

5.3.1. La oferta económica se presentará en el sobre cerrado, acompañada forzosamente del **medio magnético de cotización, en CD-RW**, debidamente requisitado en términos de las presentes bases y respaldado con la información de lo cotizado

EL MEDIO MAGNÉTICO AL QUE SE HACE REFERENCIA, DEBERÁ SER SOLICITADO AL MOMENTO DE ADQUIRIR Y REALIZAR EL PAGO DE SUS BASES EN EL DEPARTAMENTO DE PROCESOS DE CONTRATACIÓN Y SEGUIMIENTO DE ADQUISICIONES.

ES DE SEÑALARSE, QUE LA PROPUESTA CONTENIDA EN EL MEDIO MAGNÉTICO PRESENTADO, DEBERÁ SER EN EL MISMO FORMATO QUE ENTREGUE LA CONVOCANTE, SIN INCLUIR DATOS ALUSIVOS A LA IDENTIFICACIÓN DE SU EMPRESA.

(LOGO, RFC, DIRECCIÓN FISCAL, ETC.) EN ARCHIVO EXCEL, Y PARA EL CASO DE QUE NO COTICE ALGUNA PARTIDA LA LÍNEA CORRESPONDIENTE NO DEBERÁ SER ELIMINADA, SÓLO SE DEBERÁ COLOCAR EN TODA LA LINEA LA LEYENDA NO COTIZO.

SE REITERA A LOS LICITANTES QUE AL ANEXO TÉCNICO PROPORCIONADO POR LA CONVOCANTE NO SE LE DEBERÁ AGREGAR O ELIMINAR NINGUNA CELDA, FILA O COLUMNA.

LOS LICITANTES PARTICIPANTES DEBERÁN AGREGAR EN EL APARTADO DEL ANEXO TÉCNICO "ESPECIFICACIONES DEL BIEN A OFERTAR", LA INFORMACIÓN A DETALLE QUE CONTENGA LA DESCRIPCIÓN Y CARACTERISTICAS DE LAS MARCAS Y MODELOS DE LOS BIENES QUE OFERTEN.

5.3.2. La oferta económica se abrirá sólo en los casos en que, a juicio del Comité de Adquisiciones, Arrendamientos y Servicios de la UAEM, el oferente cumpla con los requisitos de la oferta técnica, o existan razones suficientes para su apertura.

5.3.3. No se tomarán en consideración aquellos documentos que no se encuentren debidamente requisitados e incluidos en el sobre correspondiente.

000042

6. ACTO DE PRESENTACIÓN Y APERTURA DE OFERTAS.

6.1. CELEBRACIÓN DEL ACTO DE PRESENTACIÓN Y APERTURA DE PROPOSICIONES.

6.1.1. El acto de Presentación y Apertura de Proposiciones tendrá verificativo el día **28** de **"NOVIEMBRE"** de **2014**, a las **-10:00-** horas, en la Sala de Juntas de la Dirección de Recursos Materiales y Servicios Generales, sitas en Rayón Sur 510 Segundo Piso, Colonia Cuauhtémoc, Toluca, Estado de México.

6.1.2. Los oferentes interesados deberán registrarse en el Departamento de Procesos de Contratación y Seguimiento de Adquisiciones, a más tardar a las 10:00 horas del día viernes veintiocho (28) de noviembre de 2014.

6.1.3. A partir del momento indicado no podrá aceptarse la participación de otros oferentes, aún cuando el acto de presentación y apertura de propuestas no haya iniciado.

6.1.4. Las ofertas descalificadas serán devueltas por el Departamento de Procesos de Contratación y Seguimiento de Adquisiciones, una vez concluido el acto de apertura de ofertas técnicas y económicas.

6.2. CAUSAS DE DESCALIFICACIÓN DE OFERENTES.

6.2.1. La omisión o incumplimiento de alguno de los requisitos, documentos o lineamientos establecidos en las presentes bases, así como no indicar de manera expresa y textual, las condiciones comerciales y económicas en los términos del punto 1.3 de las presentes bases.

6.2.2. Cuando existan dos o más ofertas atribuibles a un mismo oferente o grupo empresarial.

6.2.3. Cuando se presenten ofertas atribuibles a un oferente distinto al que participó en el acto de Junta Aclaratoria.

6.2.4. Cuando exista discrepancia entre lo contenido en la oferta técnica, los folletos o catálogos y/o la carta de especificaciones técnicas, que dificulten la evaluación técnica o bien, que los bienes y/o servicios ofertados no cumplan con las características técnicas solicitadas en el Anexo Técnico o con lo acordado en el acta de Junta de Aclaraciones.

6.2.5. Cuando solo se copie y pegue las especificaciones técnicas proporcionadas por la Convocante y no coincidan con lo contenido en su folleto y catálogo.

6.2.6. Cuando se compruebe el acuerdo entre oferentes para elevar el precio de los bienes, para disminuir la calidad, o cualquier otro acuerdo que tenga como fin

obtener ventaja sobre los demás oferentes, o afectar en cualquier forma, el procedimiento de la licitación.

6.2.7. Cuando se compruebe la variación de precios entre bienes de la misma marca, modelo y especificaciones técnicas aun y cuando se encuentren contenidos en diversas partidas.

6.2.8. Se descalificará a aquel oferente que durante la celebración de la Junta Aclaratoria o bien durante la celebración del acto de Apertura de Ofertas Técnicas y Económicas, a juicio del Comité, aprecie el intercambio de información referente a sus propuestas.

6.2.9. Haber proporcionado información en la que se aprecie a simple vista la alteración de su documentación, en alguna de las etapas del presente procedimiento.

6.2.10. El no contar con la infraestructura de comunicaciones y centro de atención que permita verificar que se cuenta con la capacidad de atender requerimientos iguales o superiores a lo solicitado en el Anexo Técnico de las presentes Bases.

6.2.11. El suprimir y/o modificar en alguno de sus párrafos los ANEXOS DOS y TRES.

6.2.12. Los que se encuentren en situación de mora o adeudo en la entrega de los bienes o en la prestación de los servicios, o en general, hayan incumplido con sus obligaciones contractuales y se encuentren incluidos en el listado de empresas objetadas de la UAEM, lo que se acreditará con los expedientes que obren en el archivo del Departamento de Procesos de Contratación y Seguimiento de Adquisiciones.

6.2.13. Las que se encuentran en alguno de los supuestos del artículo 42 del Reglamento de Adquisiciones, Arrendamientos y Servicios de la Universidad Autónoma del Estado de México.

Los oferentes podrán ser descalificados por el Comité de Adquisiciones, Arrendamientos y Servicios de la UAEM, en cualquier fase del procedimiento.

7. FALLO DE ADJUDICACIÓN.

7.1. Los cuadros comparativo y de dictamen, así como la evaluación técnica realizada por la Dirección de Tecnologías de la Información y Comunicaciones de la UAEM, servirán como fundamento para el fallo, emitido por el Comité de Adquisiciones, Arrendamientos y Servicios de la Universidad Autónoma del Estado de México.

000041

7.2. CRITERIOS PARA LA EVALUACIÓN Y SELECCIÓN DE LAS OFERTAS:

7.2.1. La capacidad administrativa, financiera, legal y técnica del oferente, para atender el requerimiento; así como su antigüedad y especialización en el ramo. Esto último se deberá acreditar con una carta, bajo protesta de decir verdad, de los servicios que el licitante ofrece, así como las especificaciones generales de su infraestructura de comunicaciones y centro de atención que permita verificar que se cuenta con la capacidad de atender requerimientos iguales o superiores a lo solicitado en el Anexo Técnico de las presentes Bases.

7.2.2. El comportamiento del oferente ante la Universidad Autónoma del Estado de México en cuanto al cumplimiento de contratos adjudicados.

7.2.3. Las especificaciones técnicas de los bienes ofertados, verificando que satisfagan como mínimo lo solicitado en el ANEXO TÉCNICO.

7.2.4. El precio ofertado, **siempre y cuando el bien o bienes ofertado(s) cumpla(n) con las especificaciones y calidad requeridas.** Para este punto se atenderá en todo momento al criterio de costo beneficio para la UAEM.

7.2.5. Las condiciones comerciales y económicas de las propuestas aceptadas como solventes, sean mejores o cumplan con lo requerido en bases.

7.2.6. Para el caso de haberse efectuado una visita técnica, el resultado de la misma, emitido por quien corresponda, se deberá considerar como un elemento para la evaluación y selección de la oferta.

7.2.7. De conformidad con la Ley de Fomento Económico para el Estado de México, y para el impulso de las actividades económicas que incidan en el desarrollo económico de la Entidad, se dará preferencia a las empresas que se encuentren ubicadas en territorio mexiquense o bien, que cuenten con Certificado de Empresa Mexiquense.

7.2.8. En caso de presentarse un empate entre dos o más propuestas, se utilizará como mecanismo de desempate la categoría de empresa que se pueda apreciar en alguno de los documentos que integren su propuesta técnica o económica.

7.3. ADJUDICACIÓN DE LA ADQUISICIÓN.

7.3.1. La adjudicación se efectuará **por lote** al oferente cuya oferta cumpla y satisfaga las condiciones establecidas en bases, resulte la más conveniente en precio, garantice el cumplimiento del contrato y cumpla con la calidad requerida, o a través del procedimiento de abastecimiento simultáneo, según resulte más conveniente para la Universidad Autónoma del Estado de México.

7.3.2. En la adjudicación de las adquisiciones, arrendamientos y servicios, el Comité de Adquisiciones, Arrendamientos y Servicios de la UAEM preferirá, en igualdad de circunstancias, a las personas físicas o morales que cuenten con el Certificado de Empresa Mexiquense, en términos de la Ley para el Fomento Económico del Estado de México.

7.4. COMUNICACIÓN DEL FALLO.

7.4.1. El fallo de adjudicación será dado a conocer a los oferentes, el día **-03-** de **-DICIEMBRE-** de **2014,** a las **–20:00–** horas; para lo cual el Comité de Adquisiciones, Arrendamientos y Servicios de la UAEM **se reunirá anticipadamente**, a fin de determinar la procedente adjudicación.

7.4.2. El fallo de adjudicación se dará a conocer a través de junta pública, o bien el Órgano Ejecutor podrá optar por comunicar por escrito el fallo a cada uno de los oferentes; la cual se llevará a cabo en las oficinas que ocupa la Dirección de Recursos Materiales y Servicios Generales.

Adicionalmente, **se publicará en los tableros informativos** del Departamento de Procesos de Contratación y Seguimiento de Adquisiciones, haciendo constar desde este momento, que **con dicha acción se da por cumplimentada la notificación respectiva del fallo emitido con motivo del presente procedimiento adquisitivo.**

7.4.3. El fallo de adjudicación será irrevocable.

8. SUSCRIPCIÓN DEL CONTRATO Y PRESENTACIÓN DE LA GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.

8.1. CONDICIONES DEL CONTRATO.

El contrato se elaborará en términos de las disposiciones legales aplicables en la materia, e inclusive comprenderá aquellas condiciones aceptadas, expresa o tácitamente por el proveedor adjudicado.

8.2. SUSCRIPCIÓN DEL CONTRATO.

8.2.1. El contrato estará a disposición del proveedor adjudicado, en la Dirección de Recursos Materiales y Servicios Generales, en un horario de 9:00 a 15:00 y de 18:00 a 20:00 horas, en días hábiles.

8.2.2. El proveedor adjudicado, personalmente o a través de su representante legal, **deberá firmar el contrato los días jueves cuatro (04) y viernes cinco (05) de diciembre de 2014**.

000040

La facturación de los bienes y servicios adjudicados habrá de realizarse en los términos establecidos en el contrato-pedido.

8.3. CUMPLIMIENTO DEL CONTRATO.

El proveedor adjudicado deberá cumplir recíprocamente con la Universidad Autónoma del Estado de México, cada una de las obligaciones que a su cargo se describan en el contrato correspondiente.

8.4. PRESENTACIÓN DE LA GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.

8.4.1. Deberá entregarla el proveedor que resulte adjudicado en forma previa a la fecha de suscripción del contrato, **con vigencia mínima de doce meses.**

8.4.2. El importe de la garantía deberá calcularse en moneda nacional y se constituirá por el **diez (10) por ciento** del importe total del contrato.

8.4.3. Se otorgará a través de fianza, cheque certificado o cheque de caja, expedidos a favor de la Universidad Autónoma del Estado de México.

8.4.4. Para el caso de que la presentación de la garantía de cumplimiento sea por medios electrónicos, se deberá adjuntar a la misma la impresión de validación por parte de la afianzadora que la expida.

8.4.5. Para la presentación de la garantía de cumplimiento se deberá adjuntar a la misma copia simple del o los Contratos Pedidos que ampare.

8.5 DEVOLUCIÓN DE LA GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.

8.5.1. La convocante, una vez solicitada la devolución por parte del proveedor adjudicado, la devolverá en un plazo de treinta días hábiles, contados a partir de la fecha en la que éste haya cumplido fehacientemente con todas sus obligaciones contractuales. En todo caso, el proveedor adjudicado tendrá la obligación de recogerla.

8.6. PRESENTACIÓN DE LA GARANTÍA CONTRA DEFECTOS O VICIOS OCULTOS.

8.6.1. Deberá entregarla el oferente que resulte adjudicado dentro del plazo de 5 días naturales siguientes a la fecha de la entrega de los bienes y servicios **con una vigencia mínima de tres (3) años.**

8.6.3. El importe de la garantía deberá calcularse en moneda nacional y se constituirá por el **cinco (5)** por ciento del importe total del contrato.

8.6.4. Se otorgará a través de fianza, cheque certificado o cheque de caja, expedidos a favor de la Universidad Autónoma del Estado de México.

8.6.5. Para el caso de que la presentación de la garantía contra defectos o vicios ocultos sea por medios electrónicos, se deberá adjuntar a la misma la impresión de validación por parte de la afianzadora que la expida.

8.6.6. Para la presentación de la garantía contra defectos o vicios ocultos se deberá adjuntar a la misma copia simple de la o las facturas respectivas.

8.6.7. La devolución de la presente garantía se hará una vez cumplidas las obligaciones garantizadas a petición del proveedor adjudicado.

NOTA: El oferente que resulte adjudicado, deberá exhibir las garantías señaladas en los puntos 8.4 y 8.6 de las Bases de la siguiente manera: para el caso de las **garantías de cumplimiento de contrato deberá** presentar **garantías que contengan Contratos Pedidos que pertenezcan a un mismo ejercicio presupuestal**. Para el caso de las **garantías contra vicios ocultos, podrá** presentar **una garantía que contenga todos los contratos pedidos que le hayan sido adjudicados**. Para el caso de que no se presenten las garantías solicitadas en los puntos 8.4 y 8.6 en los plazos y términos señalados, la UAEM podrá **rescindir el contrato correspondiente por causas imputables al proveedor que incumpla**.

8.7. GARANTÍA DE BIENES Y SERVICIOS.

Se garantizarán los bienes y servicios, por un período mínimo de **tres (3) años**, a partir de su entrega en el área solicitante; deberá entregarla el oferente que resulte adjudicado, mediante escrito bajo protesta de decir verdad, en el que se indique que la garantía ampara la totalidad del importe de los bienes materiales, considerando mano de obra y componentes sin costo adicional.

8.8. SUBCONTRATACIÓN Y CESIÓN DE CONTRATOS.

8.8.1. El proveedor adjudicado no podrá encomendar a un tercero el suministro o, en su caso, la fabricación del bien o bienes que le fue (ron) adjudicado (s) que ampara el contrato relativo.

8.8.2. El proveedor adjudicado no podrá, bajo ninguna circunstancia, ceder a terceras personas los derechos y obligaciones derivados de la suscripción del contrato.

8.9. CANCELACIÓN Y SUSPENSIÓN DE CONTRATOS.

Podrá decretarse la cancelación o suspensión del contrato, por el Comité de Adquisiciones, Arrendamientos y Servicios de la UAEM.

000039

9. SANCIONES A PROVEEDORES.

9.1. El oferente que no firme el contrato adjudicado por causas imputables al mismo, será sancionado en términos de lo dispuesto por el Título Cuarto, Capítulo III del Reglamento de Adquisiciones, Arrendamientos y Servicios de la Universidad Autónoma del Estado de México; además, se hará efectiva la garantía de cumplimiento de contrato.

9.2. El atraso en la fecha de entrega de los bienes y servicios adjudicados objeto del contrato, será sancionado con una pena convencional del **cinco al millar** sobre el importe total del contrato correspondiente por cada día de desfasamiento.

9.3. La Universidad Autónoma del Estado de México podrá aplicar al proveedor adjudicado, una sanción de **cincuenta y hasta mil veces el salario mínimo general** vigente en la ciudad de Toluca, en la fecha de la infracción, así como una pena convencional hasta por el importe de la garantía de cumplimiento del contrato cuando se presente alguna de las hipótesis siguientes:

9.3.1. El proveedor adjudicado incumpla con cualesquiera de las obligaciones que se deriven del contrato correspondiente; y a lo especificado en el ANEXO TÉCNICO en el apartado de penalizaciones.

9.3.2. El proveedor adjudicado incumpla de cualquier otra forma, con las disposiciones contenidas en la normatividad indicada en los párrafos que anteceden.

Independientemente de la aplicación de la sanción señalada, así como de la pena convencional pactada, la Universidad Autónoma del Estado de México podrá exigir el cumplimiento del contrato.

9.4. La Universidad Autónoma del Estado de México podrá operar la rescisión administrativa del contrato, aplicando la sanción y la pena estipuladas en el punto que antecede, y proceder a la readjudicación al segundo mejor precio, previa autorización del Comité de Adquisiciones, Arrendamientos y Servicios de la Universidad Autónoma del Estado de México cuando el proveedor adjudicado:

9.4.1. Omita entregar la garantía de cumplimiento del contrato en los términos y bajo las condiciones señaladas; o

9.4.2 Incumpla con cualesquiera de las condiciones pactadas en el propio contrato.

En su caso, el proveedor adjudicado estará obligado a pagar los daños y perjuicios ocasionados a la Universidad Autónoma del Estado de México.

000038

10. INCONFORMIDADES Y CONTROVERSIAS.

10.1. INCONFORMIDADES.

Las inconformidades que, en su caso, presenten los oferentes, se sujetarán a lo dispuesto por la Ley en la materia.

10.2. CONTROVERSIAS.

La interpretación y cumplimiento de las presentes bases y del contrato respectivo se resolverán en forma administrativa. En caso de controversia, las partes se sujetarán a lo dispuesto por el Reglamento de Adquisiciones, Arrendamientos y Servicios de la Universidad Autónoma del Estado de México; renunciando expresamente, al fuero que pudiera corresponderles por razón de su domicilio o vecindad, presente y futuro.

El proveedor adjudicado tendrá la obligación de señalar domicilio para oír y recibir notificaciones y todo tipo de documentos relacionados con la adjudicación de que se trate, dentro del territorio del Estado de México, toda vez que de no hacerlo, las mismas se realizarán por estrados que se ubicarán en sitio abierto de la Dirección de Recursos Materiales y Servicios Generales.

11. LICITACIÓN DESIERTA O CANCELADA.

11.1. La Licitación Pública podrá declararse desierta en los siguientes casos:

11.1.1. Cuando ningún oferente adquiera las bases de la licitación.

11.1.2. Cuando en el acto de apertura de propuestas o de evaluación, el número de oferentes participantes sea inferior al permitido.

11.1.3. Cuando ninguna de las propuestas presentadas reúna los requisitos de las bases de la Licitación, o sus precios sean mayores a los del registro correspondiente.

11.1.4. Cuando todas las propuestas presentadas sean desechadas o descalificadas; y

11.1.5. Los demás que establezcan las disposiciones legales aplicables.

11.2. La Licitación podrá declararse cancelada en los siguientes casos:

11.2.1. Cuando exista alguna causa de fuerza mayor o caso fortuito; y

11.2.2. Los demás que establezcan las disposiciones legales aplicables.

000038

La Licitación podrá declararse desierta o cancelada por el Comité de Adquisiciones, Arrendamientos y Servicios de la UAEM, **en cualquier fase del procedimiento.**

12. DISPOSICIONES GENERALES.

12.1. SOBRE LOS BIENES Y SERVICIOS.

12.1.1. El proveedor que resulte adjudicado entregará un escrito, bajo protesta de decir verdad, al momento del fincamiento del contrato, por el que garantice los bienes ofertados que le han sido adjudicados, describiéndolos como en su oferta técnica, por el período establecido en el ANEXO UNO, contado a partir de la fecha de entrega y el compromiso de cambiarlos o repararlos en caso de que tengan defectos o vicios ocultos. Así mismo, indicará de manera expresa que los bienes que suministrará cumplen con las características requeridas, conforme a lo cotizado en las ofertas presentadas.

Este escrito deberá elaborarse en papel membretado del proveedor y contener el nombre y firma del representante legal, y lo presentará al suscribir el contrato. En todo caso, se estará a lo dispuesto por los capítulos noveno y décimo primero de la Ley Federal de Protección al Consumidor.

Adicionalmente, y como lo indica el punto 1.3.1.3 deberá para efecto de verificar la calidad, especificaciones y entrega de los bienes adjudicados, exhibir una muestra física.

12.1.2. La entrega de los bienes que le han sido adjudicados, se hará bajo la responsabilidad del proveedor, quien deberá garantizar su adecuado empaque y transportación.

12.1.3. El proveedor será responsable de los gastos de carga, flete y descarga del bien o bienes que le han sido adjudicados y de cualquier gravamen fiscal que se origine sobre el mismo hasta el momento de su entrega.

12.1.4. El proveedor será responsable de cualquier violación de patentes, registros o derechos de autor, que se origine con motivo de la utilización del bien o bienes que le han sido adjudicados.

12.2. DE LAS INSPECCIONES Y PRUEBAS.

12.2.1. La Universidad Autónoma del Estado de México podrá inspeccionar y realizar pruebas a los bienes y servicios adjudicados a fin de verificar la calidad del los mismos y su conformidad con las especificaciones del contrato correspondiente; los gastos que se deriven, serán con cargo al proveedor que resulte adjudicado.

12.2.2. Las inspecciones o pruebas deberán realizarse en las instalaciones de la Universidad Autónoma del Estado de México de acuerdo al lugar de entrega de los servicios especificados en el ANEXO TÉCNICO.

12.2.3. Cuando los servicios no se ajusten a las especificaciones consignadas en el contrato, la Universidad Autónoma del Estado de México podrá rechazarlos y, en su caso, el proveedor deberá, sin cargo para el primero, reemplazarlos o incorporarles las modificaciones necesarias para cumplir con dichas especificaciones, aplicando para el caso las sanciones a las que haya lugar.

12.3. DEL TRÁMITE Y PRESENTACIÓN DE FACTURAS.

12.3.1. Las facturas de los servicios suministrados, se presentarán en original y cinco copias, en papel corporativo, con los requisitos fiscales vigentes.

12.3.2. Las facturas deberán consignar: La descripción detallada de los servicios adjudicados incluyendo el precio unitario y total, el desglose del I.V.A. y el de los descuentos adicionales ofrecidos por el proveedor, así como el importe total con número y letra.

12.3.3. Las facturas deberán emitirse a nombre de la Universidad Autónoma del Estado de México y contar con la firma del servidor público responsable de la recepción del bien o bienes adjudicado(s), así mismo deberá contar con el sello de la unidad administrativa correspondiente y la partida presupuestal que será afectada.

12.4. DE LAS PRESENTES BASES.

12.4.1. El oferente participante sufragará todos los gastos relacionados con la preparación y presentación de su oferta y, en caso que así lo determine la Universidad Autónoma del Estado de México, los demás que deriven de las verificaciones o pruebas de calidad del bien o bienes relativos.

12.4.2. Iniciado el acto de presentación y apertura de propuestas no podrán modificarse o negociarse las condiciones contenidas en las bases de la presente licitación o en las propuestas presentadas por los oferentes.

12.4.3. **La presentación de ofertas significa, de parte del oferente, el pleno conocimiento y aceptación de los requisitos y lineamientos establecidos en las bases de ésta Licitación.**

000037

12.4.4. La vigencia y contenido de las presentes bases se limita a esta Licitación. Únicamente se recibirán proposiciones de los oferentes que las adquirieron.

Las presentes bases se emiten el día **once (11) de noviembre de 2014**, en la ciudad de Toluca de Lerdo, capital del Estado de México.

A T E N T A M E N T E
PATRIA, CIENCIA Y TRABAJO
"2014, 70 Aniversario de la Autonomía ICLA-UAEM"

L. EN A. KARLA LÓPEZ CARBAJAL
DIRECTORA DE RECURSOS MATERIALES
Y SERVICIOS GENERALES DE LA UAEM

000038

ANEXO UNO

◈ DOCUMENTOS QUE DEBERÁN PRESENTAR LOS OFERENTES PARTICIPANTES DENTRO DE SU OFERTA TÉCNICA.

1. Los oferentes participantes deberán presentar por escrito las garantías de la siguiente forma:

   - Se garantizará el servicio contra cualquier defecto de instalación o vicio oculto, por un período mínimo de **36 meses** a partir de su entrega en el área solicitante.

   - Se garantizará el servicio, por un período mínimo de **36 meses**, a partir de su entrega en las áreas solicitantes; deberá entregarla el oferente que resulte adjudicado, mediante escrito bajo protesta de decir verdad que la garantía ampara la totalidad del monto del importe del servicio.

   - Todas aquellas que la empresa proponga.

Este escrito **deberá** elaborarse en papel membretado del oferente, suscrito por su representante legal y ser dirigido a nombre de la Universidad Autónoma del Estado de México.

ANEXO TÉCNICO

EL PRESENTE SE INTEGRA EN HOJAS ADICIONALES Y FORMA PARTE DE LAS MISMAS BASES DEL CONCURSO.

NP	CENTRO DE COSTO	CLAVE DE REQUISICIÓN	FONDO	ARTÍCULO	COMPO-NENTE	ESPECIFICACIONES	Especificaciones del bien a ofertar	UNIDAD DE MEDIDA	CANTIDAD	MARCA	PRECIO UNITARIO	IMPORTE MÍNIMO
1.1	DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES		FONDO DE OPERACIÓN GENÉRICO	RED MPLS		Los sitios a interconectar con la red MPLS son:		LOTE	1	N/A		

Sitio	Tipo	Ancho de banda VPN
DTIC	Central	256 Mbps
CU Amecameca	Remoto	8 Mbps
CU Atlacomulco	Remoto	8 Mbps
CU Ecatepec	Remoto	8 Mbps
CU Tejupilco	Remoto	8 Mbps
CU Temascaltepec	Remoto	8 Mbps
CU Tenancingo	Remoto	8 Mbps
CU Teotihuacan	Remoto	8 Mbps
CU Texcoco	Remoto	8 Mbps
CU Valle de Chalco	Remoto	8 Mbps
CU Valle de México	Remoto	8 Mbps
CU Zumpango	Remoto	8 Mbps
Prepa Amecameca	Remoto	8 Mbps
Prepa Atlacomulco	Remoto	8 Mbps
Prepa Tenancingo	Remoto	8 Mbps
Prepa Texcoco	Remoto	8 Mbps
UAP Chimalhuacan	Remoto	8 Mbps
UAP Cuautitlan Izcalli	Remoto	8 Mbps
UAP Nezahualcoyotl	Remoto	8 Mbps
UAP Tianguistenco	Remoto	8 Mbps
Facultad de Ciencias de la Conducta	Remoto	8 Mbps

000035

Facultad de Contaduria - Los Uribe	Remoto	8 Mbps
Prepa 2	Remoto	8 Mbps
Prepa 3	Remoto	8 Mbps
Prepa 4	Remoto	8 Mbps
Prepa 5	Remoto	8 Mbps
UAP Huehuetoca	Remoto	8 Mbps
UAP Acolman	Remoto	8 Mbps

El medio de entrega de todos los servicios deberá ser a través de fibra óptica desde la infraestructura del proveedor hasta el equipo de ruteo considerado para la entrega del servicio.

El núcleo debe operar con protocolo de capas 2/3 IP-MPLS, que ofrezca al menos 4 clases de servicio para el servicio de RPV basado en diffserv, con accesos a través de comunicaciones punto a punto, de acuerdo al RFC 2547 bis."

a) Instalación de la infraestructura para los servicios requeridos bajo el protocolo IP.

b) La red debe de ser escalable, es decir, debe de tener la flexibilidad, eficiencia, y transparencia suficiente para que en el momento que sea necesario se puedan agregar nuevos servicios o nodos de red, sin afectar la operación de la red misma o la operación de los demás nodos.

c) La red debe de cumplir con los siguientes estándares:

- RFC 2547bis – MPLS
- RFC 3031 - Arquitectura MPLS

d) Que opere bajo un esquema 7x24 los 365 días del año.

e) Debe operar con una disponibilidad de al menos 99.99% en el "backbone" de la red del proveedor.

f) Se requiere una topología Malla completa ("Full Mesh", en sus siglas en inglés) para la red privada virtual IP-MPLS de la UAEM, esto es, cada sitio de la red podrá comunicarse directamente en datos (Institucionales), voz y video de acuerdo a la tabla en este documento con cualquier otro sitio, sin tener que pasar por un tercer nodo de la red, evitando congestión y carga de tráfico.

g) El añadir un nuevo sitio a la red no debe de requerir cambios significativos de configuración en ninguno de los sitios ya existentes.

h) Capacidad de soportar los servicios de datos (Institucionales), voz y video sobre un mismo acceso, reduciendo la complejidad de administración y operación.

i) Administración efectiva de servicios IP centrales tales como un esquema de direccionamiento IP privado, basado en subredes, segmentación de la red a niveles físico y lógico.
j) Todos los equipos para el acceso a la red MPLS e Internet deberán ser nuevos, de última generación y de un solo fabricante.
k) Dentro del servicio se deberá considerar la instalación, mantenimiento y puesta en operación de todos los equipos que deberán integrar la red MPLS y conectividad a Internet.
l) La operación, gestión y administración de la red MPLS y enlaces a Internet deberá ser dentro de las instalaciones propiedad del proveedor.
m) La red debe ser capaz de proporcionar todas las ventajas de la tecnología MPLS, en particular lo siguiente:

- Separación entre las funciones de control de la información sobre la topología y tráfico en la red (routing) de las funciones de envío en sí de datos entre elementos de la red (forwarding).
- Escalabilidad de la propia red MPLS y la calidad de servicio end-to-end, habilitando la utilización eficiente de la red para su futuro crecimiento y rápida corrección de errores de enlace y fallas de nodos. En esta escalabilidad deberán tomarse en cuenta los parámetros de expansión referentes a la previsión del crecimiento de la red.

n) Para la construcción de la red MPLS y enlaces a Internet es necesario que consideren lo siguiente:

- Los requerimientos de anchos de banda descritos en el "Listado de sitios donde se deberá prestar el servicio."
- Entregar el enlace de la red MPLS e Internet con la interface WAN (Ethernet) en cada uno de los sitios involucrados en el proyecto.
- El tráfico de datos críticos generado en cada uno de los nodos deberá ser capaz de utilizar en forma dinámica el ancho de banda asignado para datos sin interferir con el utilizado por el tráfico de voz y video, para los sitios que aplique.
- Cumplir con niveles de servicios descritos en la tabla de disponibilidad y latencia señalados.
- Se requiere una distribución del ancho de banda total en cada nodo de acuerdo a las calidades de servicio indicadas.
- El proveedor del servicio será el único responsable ante "la UAEM".
- La infraestructura propuesta deberá soportar los incrementos de ancho de banda para crecimiento futuros.

El proveedor deberá incluir en su propuesta una estrategia efectiva de manejo del tráfico, con el fin de asegurar los niveles de servicio, así como también optimizar recursos de uso de la RPV. Los puntos más importantes a considerar para el manejo del tráfico son:

- Calidad de Servicio
- Clase de Servicio

La estrategia para manejo de tráfico en la red MPLS de "la UAEM", deberá consistir en una red privada virtual construida dentro de una infraestructura IP.

000034

						Este servicio deberá proporcionar transporte diferenciado de Datos no prioritarios, Datos de Misión Crítica, Voz y soporte para implementar servicios de Video garantizando su correcta operación, asignándole mayor prioridad a las comunicaciones de voz, las cuales son aplicaciones que no pueden sufrir retardos. La calidad de servicio (QoS) deberá ser proporcionada hacia la red a través del marcado de la precedencia del paquete IP. El tráfico generado por las aplicaciones de los usuarios deberá ser clasificado y tratado de acuerdo con la calidad de servicio asociada a dicha aplicación. Las herramientas que se deberán utilizar para construir servicios RPV deberán incluir técnicas para modelar la manera en que se comportan las colas de paquetes y para priorizar el tráfico basado en clases de servicio. • Calidad de Servicio (QoS) y Clase de Servicio (CoS) La calidad de servicio (QoS) es uno de los aspectos fundamentales con el que deberá contar la Red MPLS, ya que en el caso de una congestión de la red, las aplicaciones más críticas deberán tener mayor prioridad. Las garantías de Calidad de Servicio (QoS) son de punto a punto en la red, es decir, del puerto del CPE que se conecta a la red LAN de un nodo participante hasta el otro extremo, incluyendo todos los elementos de las soluciones que conformen el nodo y la nube de la RPV MULTISERVICIO MPLS. La red MPLS deberá soportar calidades de servicio para la priorización de los paquetes IP, la cual será manejada por los equipos ruteadores CPE, de acuerdo a las necesidades de "la UAEM" y de cada espacio universitario. Los servicios sensibles al retardo (voz y video) deberán ser tratados de manera preferencial con los mecanismos de calidad de servicio, dándoles mayor prioridad y precedencia que a los servicios de datos. En ausencia de tráfico del resto de las calidades de servicio, cualquier calidad de servicio de datos podrá transmitir hasta el 100% del ancho de banda disponible en el enlace/puerto de acceso a la red RPV. Las garantías de calidad de servicio deberán cumplirse de extremo a extremo en la red, es decir, de equipo CPE a CPE entre los diferentes sitios de "la UAEM", incluyendo ambas soluciones de CPE y la nube de la RPV. Los mecanismos para habilitar esta calidad de servicio deberán ser homogéneos de extremo a extremo en toda la infraestructura de comunicaciones de acuerdo a los sitios indicados. La calidad de servicio se deberá alcanzar implementando mecanismos de control de retardo y prioridad de tráfico que aseguren un trato homogéneo para las aplicaciones en todo el trayecto de los flujos.							

Se requiere que sean soportados los siguientes mecanismos de calidad de servicio:

- CAR (Commited Acces Rate) como mecanismo de limitación de ancho de banda para ciertas aplicaciones.
- WRED (Weighted Random Early Discard) para prevenir congestion
- LLQ (Low Latency Queueing) para priorizar el envío de tráfico sensible a retrasos enviándolo a una cola "Strict Priority" y manejando el resto de los datos con "Weighted Fair Queueing"

Cada una de las clases de servicio antes mencionadas, deberá estar garantizada conforme a los niveles de servicio que más adelante se establezcan en cada uno de los sitios de "la UAEM" y el marcado de los paquetes para el soporte de QoS deberá ocurrir en el CPE de la RPV.

La disponibilidad mínima deberá ser de del 99.9% y se deberá entregar un reporte mensual de la disponibilidad del servicio.

ARQUITECTURA GENERAL

La red de "la UAEM" deberá constar de un sistema de interconexión de equipos de telecomunicaciones distribuidos geográficamente, a través de la tecnología de redes privadas virtuales basada en una plataforma MPLS (Multiprotocol Label Switching por sus siglas en inglés).

Deberá ser una red de área amplia (WAN por sus siglas en inglés) la cual proporcionara la integración de múltiples servicios mediante la transmisión de voz y datos y la posibilidad del envío de paquetes de video con el manejo de calidad de servicio a través de los medios de transmisión utilizados para la interconexión de todos los nodos que componen la red.

Deberá considerarse el siguiente equipamiento para la entrega de servicios:

Para el nodo central:

Producto	Descripción	Ctd
ASR1001-X	Cisco ASR1001-X Chassis6 built-in GE	1
ASR1001-X-PWR-AC	Cisco ASR1001-X AC PowerSupply	2
CAB-AC	AC Power Cord (North America), C13, NEM	2
SASR1K1XU-312S	Cisco ASR1001-X IOS XE UNIVERSAL - NO EN	1
SLASR1-IPB	Cisco ASR 1000 IP BASE License	1

000033

SFP-GE-T	1000BASE-T SFP (NEBS 3 ESD)	1
GLC-SX-MMD	1000BASE-SX SFP transceiver module, MMF,	1
M-ASR1001X-8GB	Cisco ASR1001-X 8GB DRAM	1
NIM-BLANK	Blank faceplate for NIMslot on Cisco IS	1
CON-PSUP-ASR1001X	PRTNR SUP 24X7X4 Cisco ASR1001-X Chassis	1
CON-PSUP-SLASR1IK	PRTNR SUP 24X7X4 Cisco ASR 1000 IP BASE	1

Para cada uno de los 27 sitios remotos:

Producto	Descripción	Ctd
CISCO2911/K9	Cisco 2911 w/3 GE,4 EHWIC,2 DSP,1 SM,256	1
S29UK9-15204M	Cisco 2901-2921 IOS UNIVERSAL	1
MEM-2900-512U2.5GB	512MB to 2.5GB DRAM Upgrade (2GB+512MB)	1
PWR-2911-AC	Cisco 2911 AC Power Supply	1
CAB-AC	AC Power Cord (North America), C13, NEM	1
PI-MSE-PRMO-INSRT	Insert, Packout - PI-MSE	1
SL-29-IPB-K9	IP Base License for Cisco 2901-2951	1
HWIC-BLANK	Blank faceplate for HWICslot on Cisco.	4
ISR-CCP-EXP	Cisco Config Pro Expresson Router Flash	1
MEM-CF-256MB	256MB Compact Flash forCisco 1900; 2900	1
SM-S-BLANK	Removable faceplate forSM slot on Cisco	1
CON-PSUP-2911	PRTNR SUP 24X7X4 Cisco 2911 w/3 GE,4	1

1.2	DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES		FONDO DE OPERACIÓN GENÉRICO	ENLACES DEDICADOS DE INTERNET		Los sitios en donde se instalarán los enlaces son:		LOTE	1	N/A		

Sitio	Internet dedicado	Tipo equipo
CU Amecameca	30 Mbps	Tipo I
CU Atlacomulco	30 Mbps	Tipo I
CU Ecatepec	30 Mbps	Tipo I
CU Tejupilco	30 Mbps	Tipo I
CU Temascaltepec	30 Mbps	Tipo I
CU Tenancingo	30 Mbps	Tipo I
CU Teotihuacan	30 Mbps	Tipo I
CU Texcoco	40 Mbps	Tipo II
CU Valle de Chalco	30 Mbps	Tipo II
CU Valle de México	50 Mbps	Tipo I
CU Zumpango	30 Mbps	Tipo I
Prepa Amecameca	30 Mbps	Tipo I
Prepa Atlacomulco	30 Mbps	Tipo I
Prepa Tenancingo	30 Mbps	Tipo I
Prepa Texcoco	30 Mbps	Tipo I
UAP Chimalhuacan	30 Mbps	Tipo I
UAP Cuautitlan Izcalli	30 Mbps	Tipo I
UAP Nezahualcoyotl	30 Mbps	Tipo I
UAP Tianguistenco	30 Mbps	Tipo II
Facultad de Ciencias de la Conducta	30 Mbps	Tipo II
Facultad de Contaduria - Los Uribe	30 Mbps	Tipo I
Prepa 2	30 Mbps	Tipo I
Prepa 3	30 Mbps	Tipo I
Prepa 4	30 Mbps	Tipo I

000032

Prepa 5	30 Mbps	Tipo I		
UAP Huehuetoca	30 Mbps	Tipo I		
UAP Acolman	30 Mbps	Tipo I		

El medio de entrega de todos los servicios deberá ser a través de fibra óptica desde la infraestructura del proveedor hasta el equipo de ruteo considerado para la entrega del servicio.

Los servicios deberán contar con una disponibilidad mínima de 99.90%.
Todos los enlaces deberán contar con el siguiente equipo de ruteo:

Número Parte	Descripción
CISCO2911/K9	Cisco 2911 w/3 GE,4 EHWIC,2 DSP,1 SM,256MB CF,512MB DRAM,IPB
S29UK9-15001M	Cisco 2901-2921 IOS UNIVERSAL
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m
CAB-CONSOLE-RJ45	Console Cable 6ft with RJ45 and DB9F
PWR-2911-AC	Cisco 2911 AC Power Supply
MEM-2900-512MB-DEF	512MB DRAM for Cisco 2901-2921 ISR (Default)
MEM-CF-256MB	256MB Compact Flash for Cisco 1900, 2900, 3900 ISR
SL-29-IPB-K9	IP Base License for Cisco 2901-2951
ISR-CCP-EXP	Cisco Config Pro Express on Router Flash
CON-CSSPP-2911	SHARED SUPP 24X7X4 Cisco 2911 w/3 GE,4

Los enlaces tipo I deberán estar equipados con un dispositivo de seguridad UTM Fortigate modelo FG-1000C o superior.

Los enlaces tipo II deberán estar equipados con un dispositivo de seguridad UTM Fortigate modelo FG-1500D o superior.

Los dispositivos de seguridad UTM arriba referidos deberán cumplir con las siguientes características y servicios activos

						SOLUCIÓN DE SEGURIDAD "La UAEM" requiere el Aprovisionamiento de las Soluciones de Seguridad Informática descritas a continuación, junto con los Servicios de Consultoría necesarios para la Instalación, Configuración, Puesta a Punto y Soporte de las Soluciones listadas. **SOLUCIÓN DE FIREWALL PERIMETRAL DEL TIPO ADMINISTRACIÓN UNIFICADA DE AMENAZAS (UTM)** "La UAEM" requiere una solución de Seguridad Informática Perimetral que sea del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés), así como una consola de administración centralizada y un módulo externo de reporteo, donde por cada equipo ofrecido se deberán tener ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan: **FUNCIONALIDADES Y CARACTERÍSTICAS DEL DISPOSITIVO DE SEGURIDAD UTM** El dispositivo debe ser un equipo de propósito específico. • Basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o Servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, Freebsd, Sun Solaris, Apple OS-X o GNU/Linux. • Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC). • Capacidad de reensamblado de paquetes para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC). • El equipo deberá poder configurarse en modo gateway o en modo transparente en la red. • En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP. • El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local consultas de acuerdo a la configuración del administrador. • El equipo de seguridad debe soportar el uso del protocolo ICAP con el fin de poder delegar tareas a equipos terceros con el fin de liberar procesamiento del mismo.						

						FIREWALL • Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. • Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall. • Deberá definir políticas de firewall que sean independientes del puerto de origen y puerto de destino. • Las reglas del firewall deberán tomar en cuenta dirección IP origen (puede ser un grupo de direcciones IP), dirección IP destino (puede ser un grupo de direcciones IP) y servicio (grupo de servicios) de la comunicación que se está analizando. • Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto origen, puerto destino, direcciones IP origen, direcciones IP destino. • Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo. • Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año). • Deberá soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos. • Deberá poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP). • Capacidad de hacer traducción de direcciones estático, uno a uno, NAT. • Capacidad de hacer traducción de direcciones dinámico, muchos a uno, PAT. • Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface- Interfaz de línea de comando) como por GUI (Graphical User Interface - Interfaz Gráfica de Usuario). • Deberá tener la capacidad de balancear carga entre servidores, es decir, realizar una traducción de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas. • La solución de balanceo de carga entre servidores deberá soportar persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID. • La solución de balanceo de carga entre servidores deberá soportar mecanismos para detectar la disponibilidad de los servidores, es decir, evitar el envío de tráfico a un servidor no disponible. • Deberá permitir la creación de políticas de Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios o identificador de dispositivos para el caso de dispositivos móviles como smartphones y tabletas.						

						• El equipo deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN. • Deberá tener la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. • La solución de seguridad deberá permitir la creación de servicios de firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada. • La solución será capaz de integrar los servicios dentro de las categorías de firewall predefinidas o personalizadas y ordenarlos alfabéticamente. • Deberá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas. • La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo. • Deberá ser capaz de crear e implementar políticas de tipo Multicast y determinar el sentido de la política, así como también la habilitación del NAT dentro de cada interface del dispositivo. • Deberá ser capaz de crear e integrar políticas contra ataques DoS (Denegación de Servicio) las cuales se deberán poder aplicar por interfaces. • Deberá generar logs (bitácoras) de cada una de las políticas aplicadas. • La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o especifica. • Deberá ser capaz de configurar bloqueo de archivos o correos electrónicos por tamaño o por certificados SSL inválidos. • Integrará la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados. • Será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo qué certificado será válido este tráfico. • Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis. • La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH. **LICENCIAMIENTO Y ACTUALIZACIONES** El licenciamiento de todas las funcionalidades del equipo UTM debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.						

030000

						La vigencia de las actualizaciones para los servicios de las funcionalidades debe proveerse durante la vigencia del contrato. **CONECTIVIDAD Y SISTEMA DE RUTEO** • Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. • Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs. • Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. • Soporte a políticas de ruteo (policy routing). • El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace • Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS • Soporte a ruteo dinámico RIPng, OSPFv3 • La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes. • Soporte de ECMP (Equal Cost Multi-Path) • Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador. • Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico, en este punto se comenzará a utilizar en paralelo una ruta alternativa. • Soporte a ruteo de multicast • La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow. • La solución podrá habilitar políticas de ruteo en IPv6. • La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6. • La solución será capaz de habilitar funcionalidades de UTM (Antivirus, Filtrado Web, Control de Aplicaciones, IPS, Filtrado de correo, DLP, ICAP y VoIP) dentro de las políticas creadas con direccionamiento IPv6. • El dispositivo deberá integrar la autenticación por usuario o dispositivo en IPv6. • El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explícito. • Deberá ser capaz de integrar políticas con proxy explícito en IPv6. • La solución podrá restringir direcciones IPv6 en modo proxy explícito. • Deberá hacer NAT de la red en IPv6.						

						• La solución será capaz de comunicar direccionamiento IPv6 a servicios con IPv4 a través de NAT. • La solución deberá ser capaz de habilitar políticas de seguridad con funcionalidades IPS, Filtrado Web, Control de Aplicaciones, Antivirus y DLP, para la inspección de tráfico en IPv6 basado en flujos. • La solución deberá contar con una base de administración de información interna generada por sesiones sobre IPv6. • Deberá ser capaz de habilitar la funcionalidad de Traffic Shaper por IP dentro de las políticas creadas en IPv6. • El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6. • La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interfaz. • La solución deberá contar con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad. • El dispositivo podrá ser configurado mediante DHCP en IPv6 para comunicarse con un servidor TFTP donde se encontrará el archivo de configuración. • El dispositivo podrá hacer la función como servidor DHCP IPv6. • La solución será capaz de configurar la autenticación por usuario por interfaz en IPv6. **VPN IPSec/L2TP/PPTP** • Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site). • Soporte para IKEv2 y IKE Configuration Method. • Debe soportar la configuración de túneles PPTP. • Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES. • Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits • Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14. • Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256. • Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site. • La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN) • En modo interfaz, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interfaz y deberá ser capaz de estar presente como interfaz fuente o destino en políticas de firewall. • Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.					

620000

						VPN SSL • Capacidad de realizar SSL VPNs. • Soporte a certificados PKI X.509 para construcción de VPNs SSL. • Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN. • Soporte de renovación de contraseñas para LDAP y RADIUS. • Soporte a asignación de aplicaciones permitidas por grupo de usuarios. • Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet. • Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL. • Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning). • La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS. • Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL. • Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente. • Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios. • Los portales personalizados deberán soportar al menos la definición de: o Widgets a mostrar. o Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC. o Esquema de colores. o Soporte para Escritorio Virtual. • Política de verificación de la estación de trabajo. • La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información. • Para la configuración de cluster, en caso de caída de uno de los dispositivos, la VPN SSL que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente.						

						TRAFFIC SHAPPING / QOS • Capacidad de poder asignar parámetros de traffic shaping sobre reglas de firewall. • Capacidad de poder asignar parámetros de traffic shaping diferenciados para el tráfico en distintos sentidos de una misma sesión. • Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general. • Capacidad de poder definir ancho de banda garantizado en KBps (KiloBytes por Segundo). • Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KBps (KiloBytes por Segundo). • Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en kilobytes por segundo. • Capacidad de definir prioridad de tráfico en al menos tres niveles de importancia (Alto, Medio y Bajo). **AUTENTICACIÓN Y CERTIFICACIÓN DIGITAL** • Capacidad de integrarse con servidores de autenticación RADIUS. • Capacidad nativa de integrarse con LDAP. • Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles nombre de usuario o contraseña. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "SINGLE-SIGN-ON". • El sistema deberá de brindar un esquema para proveer el acceso a la comunidad universitaria a Internet ya sea de manera inalámbrica o cable. A los usuarios se les debe presentar una pantalla de inicio de sesión cuando realice la primera apertura de su navegador web, una vez que se autentifica con usuario y password el sistema deberá darle acceso, no deberá instalarse o configurarse algo en el dispositivo del usuario. • Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet. • Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet. • Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).						

820000

						• La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios. • Deben poder definirse usuarios y grupos en un repositorio local del dispositivo. • Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo: o Longitud mínima permitida o Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc. o Expiración de contraseña. • Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP. **FILTRAJE DE URLS (URL FILTERING)** • Control de sitios a los cuales naveguen los usuarios mediante categorías. Deberá tener por lo menos 75 categorías y 54 millones de sitios web en la base de datos. • Deberá categorizar contenido Web requerido, mediante IPv6. • Filtrado de contenido basado en categorías en tiempo real. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. • Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso. • Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo del origen de la conexión o grupo de usuario al que pertenezca la conexión que se establezca. • La solución deberá permitir realizar el filtrado de contenido, tanto en la reconstrucción de toda la sesión (modo proxy) como en la inspección paquete por paquete. • Los mensajes entregados al usuario por parte del URL Filter deberán ser personalizables (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida). Estos mensajes de remplazo deberán poder aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo. • Los mensajes de remplazo podrán personalizarse por categoría de filtrado de contenido. • Capacidad de filtrado de scripts en páginas web (JAVA/Active X). • La solución de filtrado de contenido deberá forzar el uso de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el navegador del usuario. Esta funcionalidad no						

						permitirá que los buscadores retornen resultados considerados como potencialmente maliciosos. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing. • Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos. • Será posible exceptuar la inspección de HTTPS por categoría. • Deberá contar con la capacidad de implementar el filtro de educación de Youtube por perfil de filtrado de contenido para trafico HTTP, garantizando de manera centralizada que todas las sesiones aceptadas por una política de seguridad con este perfil van a poder acceder solamente a contenido de tipo educativo en Youtube, bloqueando cualquier tipo de contenido no educativo. • El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección: 1. Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa. 2. Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad. 3. Modo DNS: La inspección se basa únicamente en la categorización del dominio accedido. • Se debe incluir la funcionalidad de reputación basada en filtrado de URLs. • La funcionalidad de reputación busca que al acceder a páginas de contenido no deseado (tales como malware, pornografía, consumo de ancho de banda excesivo, etc.) se asigne un puntaje a cada usuario o IP cada vez visita una página de esta índole. De acuerdo a esto se extraen los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar equipos infectados. • El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido. • Se debe incorporar la funcionalidad de filtrado educativo de YouTube (YouTube Education Filter). • En dicho sistema cada organismo obtiene un ID de YouTube para habilitar el contenido educativo del mismo. Se deberá insertar dicho código en la configuración de filtrado de urls del equipo para poder habilitar únicamente el contenido educativo de YouTube. **SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS)** • El detector y preventor de intrusos deberá poder implementarse en línea o a través de un puerto espejo. En línea, el tráfico a ser inspeccionado pasará a través del equipo. A través de un puerto espejo, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. • Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.						

420000

						• Capacidad de detección de más de 4000 ataques. • Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas) • El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. • La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. • El IPS deberá detectar ataques por variaciones de protocolo y por firmas de ataques conocidos (signature based / misuse detection). • Actualización automática de firmas para el detector de intrusos • El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios. • Métodos de notificación: o Alarmas mostradas en la consola de administración del appliance. o Alertas vía correo electrónico. • Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado. • La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto. • Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP. • Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir: 1. Protección contra botnets: Se deben bloquear intentos de conexión a servidores de Botnets, para ello se debe contar con una lista de los servidores de Botnet más utilizados. Dicha lista debe actualizarse de forma periódica por el fabricante.						

						2. Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una accion sobre el mismo. **CONTROL DE APLICACIONES** • Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. • La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. • La solución debe tener un listado de al menos 2000 aplicaciones ya definidas por el fabricante. • El listado de aplicaciones debe actualizarse periódicamente. • Para aplicaciones identificadas deben poder definirse al menos las siguientes acciones: permitir, bloquear y registrar en bitácora. • Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes acciones: permitir, bloquear y registrar en bitácora. • Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping. • Preferentemente deben soportar mayor granularidad en las acciones. **INSPECCIÓN DE CONTENIDO SSL** • La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S. • La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle). • La inspección de contenido cifrado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario. • Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado. • El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS. **FILTRADO DE TRÁFICO VOIP, PEER-TO-PEER Y MENSAJERÍA INSTANTÁNEA** • Soporte a aplicaciones multimedia tales como: SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).						

920000

						• Deberá contar con técnicas de detección y filtrado de programas P2P, Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa y Skype. • En el caso de los programas para compartir archivos (peer-to-peer) deberá limitar el ancho de banda utilizado. • La solución deberá contar con un ALG (Application Layer Gateway) de SIP. • Deberá poder hacer inspección de encabezados de SIP. • Deberá poder limitar la cantidad de peticiones SIP por segundo. Esto deberá poder definirse por cada método SIP. • La solución deberá soportar SIP HNT (Hosted NAT Transversal). **OPTIMIZACIÓN WAN Y WEB CACHING** • Deberá permitir la creación de perfiles para la aplicación de Optimización WAN e indicar bajo qué protocolos se ejecutará. • Deberá soportar la desfragmentación dinámica de paquetes para detectar fragmentos persistentes de distintos archivos dentro del tráfico. • Deberá ser capaz de generar y aplicar perfiles de Optimización WAN para los usuarios. • El dispositivo de seguridad podrá integrar contenido de inspección dentro de sus políticas de seguridad con Optimización WAN. • Integrará dentro de cada interfaz la capacidad de hacer túneles de Optimización WAN. • Deberá ser capaz de configurar Optimización WAN en modo Activo/Pasivo. • Deberá ser capaz de aplicar Web Caché a tráfico HTTP y HTTPS dentro de las políticas de seguridad incluyendo también Optimización WAN y Web Proxy Caché. • La solución podrá recibir el tráfico HTTPS en nombre del cliente, abrirá y extraerá el contenido del tráfico cifrado para inspeccionar y almacenar en cache para el envío al usuario final. • El dispositivo tendrá la opción de integrar un certificado SSL determinado para volver a cifrar el tráfico. • Deberá ser capaz de configurar el caché de tráfico HTTP y HTTPS bajo puertos distintos a los predeterminados (80 y 443). • Deberá ser capaz de habilitar opciones para depurar la funcionalidad de Web Caché a determinadas URLs. **ALTA DISPONIBILIDAD** • El dispositivo deberá soportar alta disponibilidad transparente, es decir, sin pérdida de conexiones en caso de falla tanto en IPV4 como IPV6. • Funcionamiento en modo Activo-Pasivo.							

						• Funcionamiento en modo Activo-Activo. • Posibilidad de definir al menos dos interfaces para sincronía. • Será posible definir interfaces de gestión independientes para cada miembro en un clúster. **CARACTERÍSTICAS DE ADMINISTRACIÓN** • Interfaz gráfica de usuario (GUI) vía Web por HTTP y HTTPS para administración de las políticas de seguridad, formando parte de la arquitectura nativa de la solución para administrar la solución localmente. por seguridad la interface debe soportar SSL sobre HTTP (HTTPS). • La interface gráfica de usuario (GUI) vía web deberá poder estar en español y en inglés, configurable por el usuario. • Interfaz basada en línea de comando (CLI) para administración de la solución. • Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto. • Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH o Telnet). • El administrador del sistema podrá autenticarse vía usuario/contraseña o certificados digitales. • Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo. • El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, HTTP o HTTPS. • El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un navegador (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional. • Soporte de SNMP versión 2 y 3. • Soporte de al menos 3 servidores syslog para envío de bitácoras a servidores de syslog remotos. • Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL. • Soporte de Control de Acceso basado en roles, con capacidad de al menos 6 perfiles para administración y monitoreo del Firewall. • Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red. • Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, log y gestión.						

520000

						• Permitir que el administrador pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica. • Contar con facilidades de administración a través de la interfaz gráfica como listas de edición a través de clic derecho. • Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard). • Contar con la posibilidad de agregar una barra superior (top bar) cuando los usuarios estén navegando con información como el id de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas definidas. • Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto top de sesiones por origen, top de sesiones por destino, y top de sesiones por aplicación. **VIRTUALIZACIÓN** • Deberá virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains" • La instancia virtual deberá soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus. • Se deberá incluir la licencia para al menos diez instancias virtuales. • Cada instancia virtual podrá tener un administrador independiente. • La configuración de cada instancia virtual podrá estar aislada de manera lógica del resto de las instancias virtuales. • Cada instancia virtual podrá estar en modo gateway o en modo transparente a la red. • Deberá ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual. • Deberá definir distintos servidores syslog para cada instancia virtual. • Deberá definir enlaces de comunicación entre los sistemas virtuales sin que el tráfico deba salir de la solución por medio de enlaces o conexiones virtuales. Estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y modo Transparente. **ACTUALIZACIONES DE PLATAFORMA** • La solución contara con el servicio de actualización de firmas para dispositivos sobre BYOD • El dispositivo tendrá la opción de conectarse a los servidores NTP de los Laboratorios de Investigación y Actualización propietarios del fabricante para actualización del horario de sistema local. • Será capaz de hacer consultas a servidores DNS de los Laboratorios de Investigación y Actualización del fabricante para resolución y						

						categorización de sitios web dentro de los perfiles para Filtrado Web. • Tendrá la capacidad de hacer consultas a servidores de los Laboratorios de investigación y Actualización del fabricante sobre reputación de direcciones IP. **TOLERANCIA A FALLAS** Los dispositivos de seguridad UTM deberá incluir fuente de poder redundante de corriente alterna (AC). Voltaje requerido 110-220 [V] en corriente alterna. Deberán incluir cables para cada una de las fuentes de energía, mismas que serán conectadas a un PDU NEMA C-13. **CARACTERÍSTICAS TÉCNICAS** La infraestructura ofertada deberá cubrir las características y funcionalidades mínimas descritas en el presente documento; así como también debe cubrir el servicio de instalación, configuración, puesta a punto de su operación. La instalación, configuración y puesta a punto de la infraestructura de seguridad debe garantizar que la solución es implementada bajo las mejores prácticas y asegurar la correcta operación de la solución, el proveedor deberá incluir dentro de su propuesta servicios profesionales por parte del fabricante Las funcionalidades descritas y requeridas por "la UAEM" para la totalidad de este documento se consideran mínimas y deben ser cubiertas al 100% por cada una de las soluciones propuestas por el proveedor, y debidamente respaldadas por documentación técnica del fabricante referenciada con catálogos, manuales y publicaciones en el sitio web del fabricante. El proveedor, deberá contar con un centro de atención permanente las 24 horas del día durante la vigencia del contrato, debiendo proporcionar el soporte técnico que corresponda a las garantías y pólizas de mantenimiento adquiridas para cada uno de los bienes objeto del presente documento, a través del cual "la UAEM" pueda levantar reportes para solicitar soporte en sitio en caso de falla así como recibir asesoría técnica telefónica (ilimitada e inmediata). El proveedor, deberá incluir todos los cables, accesorios y/o aditamentos hardware-software necesario para la correcta operación y funcionalidad de la infraestructura solicitada, así como los kits de montaje. Asimismo, deberá incluir todos los accesorios (fibras ópticas, conectores, rieles, cables, SFP, etc.) que estime convenientes para la correcta conectividad de los equipos solicitados.						

020024

						El proveedor deberá de considerar en su propuesta todas las actualizaciones (updates, upgrades y demás elementos en software sobre el mismo release o en release diferente) que realice el fabricante con respecto de los bienes a adquirir. La infraestructura ofertada deberá cumplir a cabalidad con los requisitos y funcionalidades mínimas descritas en la tabla "características técnicas del firewall" de la presente. La infraestructura deberá incluir la memoria suficiente (flash, dram, ram) para la adecuada operación del dispositivo para cumplir con las funcionalidades y requerimientos mínimos solicitados. La infraestructura deberá incluir el licenciamiento necesario para cumplir con las funcionalidades y requerimientos mínimos solicitados. El licenciamiento de la infraestructura deberá ser efectivo durante la vigencia del contrato. La infraestructura ofertada por el licitante deberá ser del tipo appliance rackeable; es decir, hardware y software adaptados perfectamente entre sí. La funcionalidad de firewall virtual requerida deberá permitir la asignación de recursos asignados por cada firewall virtual. Se deberá brindar esta funcionalidad a través del firewall virtual o de equipo físico instalado en cada sitio que sea necesario. Los recursos que podrán asignarse a un firewall virtual deben incluir como mínimo: • Número de conexiones y/o sesiones para un firewall virtual. • Interfaces virtuales para cada instancia de manera independiente. • Archivos de configuración en registros independientes por firewall virtual. • Distribución de firewalls virtuales por grupo para cada ambiente de alta disponibilidad activo/pasivo. **HARDWARE Y DESEMPEÑO** Los equipos solicitados por "la UAEM", descritos en el "Listado de sitios de equipo de seguridad, así como su clasificación por tipo y cantidad de equipamiento de seguridad" deberán cumplir con las características mínimas de la siguiente tabla, respetando la marca solicitada:						

	Tipo I	Tipo II
Interfaces 10/100/1000 RJ45	14	16
Interfaces 1G SFP	4	16
Interfaces 10G SFP+	2	8
Interfaces 40G (QSFP+)	0	0
Desempeño de Firewall	20 Gbps	60 Gbps
Desempeño de VPN IPSec	8 Gbps	40 Gbps
Desempeño de Antivirus	1.7 Gbps	10 Gbps
Desempeño de IPS	6 Gbps	10 Gbps
Desempeño VPN SSL	1.3 Gbps	2 Gbps
Sesiones Concurrentes	7 Millones	10,000,000
Nuevas sesiones / segundo	190,000	200,000
Políticas de firewall	100,0000	80,000
Túneles de VPN cliente a sitio	50000	40,000
Fuentes de Poder redundantes	Si	Si

Tabla. Características del Firewall

FUNCIONALIDADES Y CARACTERÍSTICAS DE LA CONSOLA DE ADMINISTRACIÓN CENTRALIZADA.
CARACTERÍSTICAS DE LA SOLUCIÓN REQUERIDA.

El appliance deberá administrar como mínimo 1 equipo centrales y 27 equipos remotos para la implementación del modelo red hibrido. La consola deberá de gestionar todas las políticas de seguridad y configuraciones de equipos así como el monitoreo y respaldo para garantizar la operación de los servicios que de ellos dependan.

Se deberán de tomar en cuenta el "Listado de sitios de equipo de seguridad, así como su clasificación por tipo y cantidad de equipamiento de seguridad" de este documento para el dimensionamiento adecuado del equipo.

FUNCIONALIDADES:

- La solución deberá permitir la gestión y control de manera centralizada, ofreciendo un esquema en el cual los equipos del "Listado de sitios de equipo de seguridad, así como su clasificación por tipo y cantidad de equipamiento de seguridad" en cada sitio puedan operar de forma remota.
- Funcionalidad para la administración de políticas de tipo firewall y ruteo estático y dinámico así como la NATs.
- Funcionalidad para configuración de la Protección y el Filtrado de contenido WEB.

						• Capacidad de configurar las actualizaciones de firmas de ataques y múltiples tipos del malware provenientes de Internet para cada equipo o todos en conjunto. • Funcionalidad para la administración y monitoreo VPNs SSL. • Por seguridad y eficiencia, debe ser un "appliance" de propósito específico para el gerenciamiento de la seguridad. No se aceptan plataformas basadas en sistemas operativos genéricos y/o hardware genérico. • Se incluye la administración de dispositivos "virtuales" que residen en una misma unidad física. Estos equipos virtuales pueden ser administrados como un dispositivo completamente independiente dentro de la consola, con su propia configuración y administración. Esta capacidad permite consolidar en el número menor posible de consolas, preferentemente una, la administración de las diversas funcionalidades de protección completa de contenido. • Creación, almacenamiento e implementación automatizada de configuraciones de dispositivos. • Permitir tener un solo repositorio de almacenamiento centralizado y administración de configuraciones, para simplificar las tareas de administración de una gran cantidad de dispositivos de seguridad con protección completa de contenido. • Las comunicaciones entre la consola de administración y los dispositivos administrados deben ser cifradas (Encriptadas) • La interface de administración es basada en Web Seguro (HTTPS) • Para un eficiente almacenamiento de las configuraciones, debe incluirse una base de datos relacional integrada compatible con la solución. • Administración basada en roles para permitir a los administradores delegar los derechos a dispositivos específicos con los privilegios adecuados de lectura/escritura. • Configuración basada en scripts para una mejor flexibilidad y control. Esta funcionalidad permite la automatización de tareas operativas, cuya implementación puede ser de forma masiva, con tiempos de aplicación mínimos a los dispositivos administrados • Se debe poder realizar automatización calendarizada de respaldos de la configuración y las bitácoras. • Se debe poder realizar operaciones sobre grupos de dispositivos, y añadir/cambiar/borrar dispositivos de esos grupos. • Permitir el hospedaje local de actualizaciones de firmas de AV / IPS y filtrado de contenido web y Antispam, de los dispositivos UTM. Esto permite el almacenamiento de forma local de las bases de datos de protección AV e IPS, además de Filtrado de Contenido y Anti-SPAM, con la finalidad de disminuir el tráfico de consultas de actualizaciones a Internet a lo mínimo, evitando el consumo innecesario de ancho de banda, permitiendo la utilización de este para los fines requeridos por los usuarios de red.						

						• Capacidad de crear, exportar y almacenar versiones de configuración de los dispositivos administrados, antes de aplicar cambios a un dispositivo. De esta forma, se disminuye la posibilidad de cometer un error no intencional al modificar una política y permite regresar a una configuración en un estado operacional después de haber aplicado una implementación con resultados no esperados. • Incluye un subsistema Monitoreo en Tiempo-Real. Esto permite al equipo de monitoreo y administración obtener el estado actual de la infraestructura de dispositivos administrados, y permitir actuar proactivamente a un evento de seguridad y operación de los dispositivos de seguridad administrados. • Posibilidad de administrar el firmware de los dispositivos de seguridad, permitiendo programar y aplicar actualizaciones de sistema operativo de forma desatendida a un equipo o grupo de equipos administrados por la consola, reduciendo tiempos de operación y administración del personal que administra los equipos de seguridad. • La consola de administración permite configuración en Alta Disponibilidad, de tal forma que en caso de falla pueda existir otro equipo en línea que tome las tareas del equipo dañado con una pérdida mínima en la disponibilidad del servicio. **DESEMPEÑO.** • Deberá contar con un sistema operativo estable de uso específico para las funciones descritas con anterioridad. • El equipo deberá contar con la suficiente memoria y tipo de memoria para soportar la operación y monitoreo diario de toda la infraestructura de equipos y obtención de reportes en tiempo real. • Interfaces incluidas en el equipo con 2 puertos cobre 10/100/1000. • 8TB de disco duro como mínimo. **Adicionales** •Se requiere el Aprovisionamiento de dos discos adicionales de 2TB para el equipo Marca Fortinet Modelo FortiAnalyzer FA-2000B propiedad del cliente. •Se requiere que la totalidad de los 27 equipos UTM cuenten con certificado PKI X.509 de 2048 bits emitido por una entidad certificadora para habilitar la inspección SSL, con validez durante la vigencia del contrato con un nivel de encriptación de 2048 bits.						

220000

						OTRAS CONSIDERACIONES • Conectividad con interfaces ethernet 10/100/1000. • El equipo es montable en rack. Para todo el equipamiento se requiere instalación, soporte y mantenimiento y actualización de las licencias necesarias durante el periodo del contrato. El tiempo de atención a fallas es de 30 minutos máximo y en caso de requerirse asistencia en sitio es de 4 horas máximo, con 8 horas como máximo de solución de problemas. Para los equipos de seguridad deberá considerarse que: a) El dispositivo de seguridad UTM deberá contar con la versión más reciente estable del sistema operativo. La versión del sistema operativo no deberá estar en etapa de pruebas (versiones beta no aceptadas). b) La consola de administración centralizada y el módulo de reporteo deberán ser del mismo fabricante de la solución UTM, esto con el fin de que sean compatibles y cuenten con soporte de integración transparente. c) Con el fin de minimizar riesgos operativos y asegurar la continuidad de servicios, el dispositivo de seguridad UTM deberá poder administrarse sin necesidad de la consola de administración central y solo se aceptara que el equipo UTM tenga capacidad de entregar reportes simples, delegando esta tarea al módulo de reporteo externo. d) El licitante adjudicado será el responsable de la configuración de los dispositivos, incluyendo pero no limitándose a: políticas de seguridad, interfaces de administración e inspección de contenido, envío de reportes, SNMP versión 2 ó 3 para envío de traps, así como la configuración asociada con la consola de administración centralizada y el módulo externo de reporteo. e) Las propuestas técnicas presentadas por los licitantes participantes para su revisión, deberán incluir las fichas técnicas en español o inglés, las cuales deberán estar referenciadas a las características requeridas. f) Todas las ofertas deberán suministrar la información completa sobre marca, modelo, dimensiones y especificaciones técnicas del						

						dispositivo de seguridad UTM, consola de administración centralizada y el módulo de reporteo. g) El licitante adjudicado se comprometerá a realizar, conjuntamente con el personal de la UAEM, al menos una vez al año la actualización del software, durante la vigencia del contrato. En caso de requerirse limpieza interna y externa de los componentes, esta se programará en el horario y día que la UAEM establezca con el fin de impactar lo menos posible en el servicio. **Entrega del proyecto** El licitante adjudicado deberá entregar a la terminación de los trabajos de instalación y previo a la operación y puesta en producción de cada equipo lo siguiente: a) Propuesta técnica presentada durante la licitación. b) Memoria técnica de puesta en operación del dispositivo de seguridad UTM, consola de administración centralizada y módulo de reporteo, de acuerdo a los requerimientos de la UAEM. La memoria técnica debe incluir: • Instalación física. • Diagramas de conexión. • Configuración del dispositivo de seguridad UTM. • Configuración de la consola de administración central. • Configuración del módulo de reporteo. • Documentación de fibra óptica y cableado UTP utilizado. • Etiquetado de los cordones de fibra óptica y cableado UTP. c) Manuales de instalación, operación, mantenimiento y administración del dispositivo de seguridad UTM, La consola de administración y el módulo de reporteo instalados. El licitante adjudicado será responsable de la total instalación y puesta en operación los dispositivos de seguridad UTM en el nodo central, así como en cada uno de los campus especificados en el presente documento, de igual forma será responsable de la total instalación la consola de administración centralizada y el módulo de reporteo en el nodo central. Asimismo, deberá incluir todos los accesorios (fibras ópticas, conectores, rieles, cables, SFP, etc.) que estime convenientes para este propósito.						

000021

						Licenciamiento y actualizaciones El licenciamiento de todas las funcionalidades del equipo UTM debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de las funcionalidades debe proveerse durante la vigencia del contrato. **Mantenimiento, soporte y garantía** Dentro de su propuesta, el licitante participante deberá especificar por escrito las condiciones de garantía y soporte técnico para la solución ofertada, con la finalidad de garantizar la disponibilidad de servicios requerida. Todo mantenimiento que requiera suspender el servicio, deberá ser acordado previamente con la UAEM. **Documentos** El licitante participante deberá presentar la siguiente documentación, misma que no tendrá antigüedad superior a 3 meses de su emisión: a) Carta en papel membretado firmada por el representante legal donde se compromete a instalar todos los equipos ofertados, que su solución cumple con todas las especificaciones técnicas indicadas en estas bases y que proporcionará todos los entregables para la terminación de los trabajos. b) Constancias o certificados vigentes emitidos por el fabricante de un ingeniero responsable de la instalación, configuración y puesta en operación de la solución propuesta. c) Carta en papel membretado firmada por el representante legal en donde se compromete a contar con al menos un ingeniero certificado en la solución propuesta como parte de su equipo de ingeniería, durante la vigencia del contrato. d) Carta en papel membretado firmada por el representante legal en donde indique que el dispositivo de seguridad UTM ofertado posee una vida útil de al menos 5 años, garantizándose con ello refacciones, actualización de versiones de sistema operativo, así como todo el software necesario para su adecuada operación. e) Carta en papel membretado firmada por el representante legal en donde el licitante participante se compromete a proporcionar las garantías como se solicitan en las bases, cumpliendo con la disponibilidad de servicio requerida.						

						f) Carta en papel membretado firmada por el representante legal en donde acepta la ejecución de las penalizaciones que se indican en estas bases en caso de incumplimiento a la oferta presentada. g) Carta en papel membretado firmada por el representante legal en donde indique que los servicios de ingeniería para la entrega e instalación en sitio se ajustarán a los horarios, días y el lugar de trabajo que la UAEM establezca. h) Carta en papel membretado del fabricante en donde declare que cuenta con al menos 10 años de experiencia en el mercado internacional. i) Carta en papel membretado del fabricante, en donde se especifique que el licitante participante es canal autorizado para la venta, distribución y soporte del dispositivo de seguridad UTM ofertado. Asimismo que respalda las especificaciones técnicas y garantías del dispositivo de seguridad UTM, Consola de administración centralizada y el módulo de reporteo externo. j) Carta en papel membretado del fabricante en donde especifique que cuenta con al menos un centro de investigación sobre vulnerabilidades y amenazas informáticas. k) Carta en papel membretado del fabricante en donde se indique que cuenta con un centro de soporte técnico regional ubicado en el área metropolitana de la Ciudad de México.					
1.3	DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES		FONDO DE OPERACIÓN GENÉRICO	ENLACE DEDICADO DE INTERNET CON REDUNDANCIA	ENLACE	El servicio de Internet tendrá una capacidad de 1 Gbps con redundancia al 100% y se deberá contar con una disponibilidad de 99.99%. Se requiere de un enlace a Internet Directo con Acceso Ethernet, en la modalidad que le permita a "la UAEM" conectarse a Internet haciendo uso de la tecnología Ethernet. La principal característica del servicio es que se deberán ofrecer velocidades en los rangos FastEthernet (FE) y GigaEthernet (GE), a través de una conexión dedicada. De tal forma que se establecen velocidades que van de 10Mb a 100Mb en FE o de 100Mb a 1000Mb en GE. El servicio deberá ser escalable, es decir, debe tener la flexibilidad, eficiencia y transparencia suficiente para que en el momento que sea necesario, se puedan ampliar los anchos de banda.		1	Servicio			

020000

						Estándares, en los que se deberán basar los servicios de Internet. • RFC 791 - Internet Protocol • RFC 826 - ARP • RFC 917 - Internet Subnets • RFC 1878 - Variable Length Subnet • RFC 1519 - Classless Inter Domain Routing • RFC 1918 - Address Allocation for Privates Internet • RFC 1541 – Dynamic Host Configuration Protocol • RFC 1631 – The IP Network Address Translator • RFC 1661 – The Point to Point Protocol • RFC 1334 – PPP Authentication Protocols • RFC 2153 - PPP Vendor Extensions • RFC 3271 - The Internet is for everyone • RFC 1771 – A Border Gateway Protocol 4 (BGP-4) • RFC 904 – Exterior Gateway Protocol Formal Specification • RFC 1930 – Guidelines for creation, selection and registration of an Autonomous System (AS) • RFC 2270 – Using a Dedicate AS for Sites Homed to a Single Provider • RFC 1700 – Assigned Numbers • RFC 1966 – Autonomous System Confederation for BGP • RFC 1264 - Internet Engineering Task Force Internet Routing Protocol Standardization Criteria • ISO 3166 - Country Codes Nota: los estándares pueden variar de acuerdo a la implementación de cada solución, apegados a la parte de seguridad y de los servicios administrados requeridos por "la UAEM". El servicio deberá ser entregado a través de un equipo de ruteo para el enlace principal y el de redundancia de la siguiente marca y modelo: CISCO 4451-X Con las siguientes características: Componentes mínimos: • Memoria de Control Plane de 4GB • Memoria de Data Plane de 2GB • Memoria Flash mínima de 8 GB • Fuente redundante. Conectividad: • Puertos de administración. • 4 Puertos Ethernet 10/100/1000 • 4 Puertos SFP • NIN Slots 3						

						Las características generales que deberá cumplir el equipo CPE descrito anteriormente son las siguientes: Protocolos Soportados: • IPv4 • IPv6 • Static routes • Routing Information Protocol Versions 1 and 2 (RIP and RIPv2) • Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP) • Border Gateway Protocol (BGP) • BGP Router Reflector • Intermediate System-to-Intermediate System (IS-IS) • Multicast Internet Group Management Protocol Version 3 (IGMPv3) • Protocol Independent Multicast sparse mode (PIM SM) • PIM Source Specific Multicast (SSM) • Distance Vector Multicast Routing Protocol (DVMRP) • IPv4-to-IPv6 Multicast • MPLS • Layer 2 and Layer 3 VPN • Layer 2 Tunneling Protocol Version 3 (L2TPv3) • Bidirectional Forwarding Detection (BFD) • IEEE802.1ag • IEEE802.3ah Protocolos de Encapsulación: • Generic routing encapsulation (GRE) • Ethernet • 802.1q VLAN, • Point-to-Point Protocol (PPP) • Multilink Point-to-Point Protocol (MLPPP) • Frame Relay • Multilink Frame Relay (MLFR) (FR.15 and FR.16) • High-Level Data Link Control (HDLC) • Serial (RS-232, RS-449, X.21, V.35, and EIA-530) • PPP over Ethernet (PPPoE) Protocolos para Administración de Tráfico: • QoS • Class-Based Weighted Fair Queuing (CBWFQ) • Weighted Random Early Detection (WRED) • Hierarchical QoS, Policy-Based Routing (PBR) • Performance Routing, and NBAR.						

610019

						Características de Administración: • SNMP • Syslog • Netflow						
1.4	DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES		FONDO DE OPERACIÓN GENÉRICO	CENTRO DE OPERACIÓN DE RED (NOC) PARA MPLS	SERVICO	**CENTRO DE OPERACIÓN DE RED (NOC)** El proveedor deberá proporcionar a través de su centro de operación de red NOC los servicios de Administración de fallas, configuraciones y desempeño de la Red MPLS e Internet. El proveedor deberá realizar el servicio de Administración de fallas, de configuraciones, de desempeño de la Red a través del NOC dentro del marco de referencia del modelo ISO para la Administración de Redes, comprendiendo las siguientes tres actividades: a. Administración de Fallas (Fault Management): Para la detección y solución de las fallas que se presenten en la red. b. Administración de Configuraciones (Configuration Management): Para el manejo de la información relativa a las configuraciones de los equipos de red. c. Administración del Desempeño (Performance Management): Para la medición y determinación de los niveles de operación de la red, en general y por cada elemento de la misma. **ADMINISTRACIÓN DE FALLAS** El objetivo de la administración de fallas deberá detectar, registrar, notificar y solucionar los problemas que ocurran en la red, para mantenerla operando adecuadamente. La administración de fallas deberá involucrar la determinación de los síntomas y el aislamiento del problema, seguida de la reparación del problema con pruebas de la solución y, finalmente, el registro de toda la información obtenida durante el proceso. **FUNCIONES** Descubrimiento y mapeo topológico de los dispositivos de la red. Por medio de una herramienta de monitoreo, se deberá detectar la presencia de todos los dispositivos activos de la red y generar un mapa topológico, donde se indique gráficamente la interrelación de estos dispositivos. Monitoreo de los dispositivos de la red. Monitoreo continuo de la actividad de los dispositivos de la red, mediante una representación gráfica de la herramienta		1	Servicio			

						de monitoreo, donde se deberá indicar, por medio de diferentes colores, el estado operacional de cada dispositivo. Detección y administración de incidentes. Detección proactiva de incidentes en los elementos de red en base a la detección de alarmas. Los dispositivos de red deberán tener la capacidad de alertar al sistema de administración y monitoreo, mediante la generación de una alarma al enviar un "trap", cuando ocurra una falla en el sistema, de tal manera que se puedan tomar acciones correctivas. Solución de incidentes de falla. Una vez detectada una situación de falla, se deberá abrir un caso o ticket en la herramienta de administración de incidentes y se deberá iniciar el proceso de solución de la misma, el cual incluye soporte de primero, segundo y tercer nivel, de la siguiente manera: 1. Soporte de Primer Nivel: Se deberá proporcionar remotamente a través del centro de operaciones, el cual deberá contar con ingenieros especializados en los equipos incluidos en la solución. 2. Soporte de Segundo Nivel: Cuando la falla detectada no pueda ser resuelta remotamente, la falla deberá ser canalizada a un ingeniero de soporte que deberá acudir con las herramientas y refacciones necesarias a la localidad donde se suscitó la falla. 3. Soporte de Tercer Nivel: De ser necesario para la solución de la falla, el centro de operaciones deberá escalar el problema al fabricante del equipo en cuestión. **HERRAMIENTAS** Las herramientas que se deberán utilizar para la administración de fallas deben cumplir como mínimo con los siguientes requerimientos: Consola gráfica de monitoreo y detección de incidentes de falla. • Esta herramienta deberá consistir en una consola que realizará las funciones de descubrimiento y mapeo de los elementos y dispositivos de la red. Cada elemento o dispositivo deberá ser desplegado en forma gráfica en una pantalla, indicando, por medio de colores su estado operacional. Los dispositivos de la red deberán ser configurados para enviar notificaciones o traps SNMP a la consola en la ocurrencia de incidentes. • La herramienta de administración de incidentes o "trouble ticket" deberá permitir registrar los incidentes de falla y darles continuidad hasta su solución, indicando fecha y hora de apertura del caso, tiempo de atención y fecha y hora de cierre del caso. La UAEM deberá tener acceso a una aplicación que presente la siguiente información:						

810000018

						• Notificación automática de incidentes • Indicadores de salud del servicio • Reporte de cumplimiento de los SLA **ADMINISTRACIÓN DE CONFIGURACIONES** La administración de configuraciones deberá tener como fin el manejo y control de la información relativa a la configuración de los dispositivos de la red, de tal manera que los cambios de configuración y actualizaciones de versión de hardware y software no tengan impacto en la operación de la red. Cada elemento de red deberá tener una variedad de información, en diferentes versiones, asociada a éste. Un sistema de administración de configuraciones deberá almacenar toda esta información en una base de datos de fácil acceso, la cual deberá ser consultada en el momento en que ocurra un problema en la red, para ayudar a resolverlo. **FUNCIONES** Administración de la nomenclatura. Deberá contar con identificación por nombre de los elementos de la red (equipos, interfaces, direccionamiento IP, etc). Aseguramiento de la integridad de las configuraciones. Deberá resguardar y respaldar las configuraciones de los equipos de la red, en servidores o dispositivos de almacenamiento. Administración de inventarios. Deberá contar con la utilización de la funcionalidad de descubrimiento de elementos de red, para mantener una base de datos con información detallada de cada equipo de la red. **ADMINISTRACIÓN DE DESEMPEÑO** El objetivo de la administración del desempeño deberá ser la medición y recolección de información estadística relativa a diversos parámetros de operación de los diferentes elementos de red (dispositivos y enlaces) con objeto de determinar el nivel de desempeño de la red. Tales parámetros de operación deberán comprender el throughput de la red, tiempos de respuesta y utilización de enlaces. La administración del desempeño deberá incluir tres actividades. Primero, la información de desempeño deberá ser reunida por medio de una herramienta de monitoreo. Segundo, la información deberá ser analizada para determinar los niveles de operación de la red (baselinning). Por último, se deberán determinar y ajustar los umbrales de operación de los parámetros analizados, de tal manera						

						que al excederse estos umbrales se detecten de manera proactiva la ocurrencia de una situación anormal de operación. **FUNCIONES** Se deberá recolectar periódicamente diferentes valores de desempeño de la red mediante mecanismos de sondeo periódico (poleo) en cada dispositivo, para la medición de parámetros concernientes al comportamiento de dichos dispositivos (poleo cada 5 minutos), tales como: Mediciones de desempeño de equipo: • Deberá dar a conocer el nivel de funcionamiento interno de los dispositivos de red para determinar la necesidad de reemplazar o incrementar la capacidad de los mismos para atender suficientemente las demandas de la red. Mediciones de rendimiento: • Deberá permitir conocer el desempeño de la red para transmitir y/o recibir información y será la guía para la vigilancia del cumplimiento de los Niveles de Servicio acordados. (SLA's) Mediciones de tráfico y utilización de los medios: • Definirá las características bajo las cuales deberán estar trabajando los elementos que componen la red. Permitirán obtener parámetros para visualizar las tendencias de su comportamiento para planear y decidir sobre las estrategias de crecimiento y mantenimiento de la red. • Almacenamiento y representación gráfica de la información recolectada. Esta información deberá ser utilizada para la elaboración de reportes ejecutivos que describan el comportamiento de la red en un periodo de tiempo. **ALCANCES DEL SERVICIO** **CENTRO DE OPERACIÓN DE RED NOC** Funciones o actividades que se deberán proporcionar a través del NOC a "la UAEM": **COBERTURA DEL SERVICIO** Administración de fallas, configuraciones y desempeño con un horario de soporte 7x24x365 El centro de operación de red NOC se ubicara fuera de las instalaciones de "la UAEM". **PLATAFORMAS A SOPORTAR** La propuesta deberá considerar el monitoreo y administración de los equipos CPE routers que integran la red MPLS e Internet.						

410000

						MONITOREO DE RED Y ATENCIÓN A FALLAS El centro de operación de Red NOC deberá realizar las siguientes actividades: a) Monitoreo de red b) Monitorear en forma remota los siguientes componentes: • Medios de Comunicación de la Red MPLS e Internet • Dispositivos de conectividad, equipos y puertos respectivos de la Red MPLS e Internet. • Operación y administración del funcionamiento, disponibilidad, y rendimiento de los enlaces a través de los equipos • Detección proactiva de fallas en la red MPLS e Internet mediante la generación de alarmas. • Notificación automática de alarmas para escalamiento de la falla • Estas alarmas deberán ser notificadas al personal que "la UAEM" designe vía correo electrónico o bien a través del NOC. • Administración de Capacidades a través de Reportes y Estadísticos • Respaldo y Prueba periódicas de las configuraciones de los equipos a Monitorear a través de la Herramienta de Gestión • La Herramienta de Monitoreo deberá proporcionar las siguientes características: o Visualización del estado de la red (equipos y enlaces) a través de alarmas o Administración vía WEB http o Acceso vía WEB (http) para lectura de reportes o Reportes o Elementos para la generación de alarmas, alertas y traps SNMP o Gráficas con la utilización de ancho de banda de los enlaces que conformen la red y porcentajes de utilización de CPU de los equipos principales **ALCANCES DE LA ADMINISTRACIÓN DE FALLAS:** • Operación y administración del funcionamiento, disponibilidad, rendimiento y eficiencia de los equipos y enlaces • El NOC deberá contar con un número telefónico único para la recepción de los reportes y requerimientos por parte del personal asignado por "la UAEM". • Recibir, registrar, analizar, resolver y canalizar los reportes de incidencias o fallas, dar seguimiento y solución a los reportes, generar un registro histórico con consulta en línea para "la UAEM" a través del protocolo http sobre el tipo de fallas presentadas y su solución. • El sistema de mesa de ayuda del NOC deberá incluir acceso vía http en línea para 3 usuarios concurrentes de "la UAEM". • Soporte y coordinación a los reportes de fallas. • Administración de Incidentes a través del registro (Tickets)						

- Diagnóstico de falla, escalamiento, coordinación, seguimiento de los Reportes de falla hasta su solución
- Coordinar el envío de la refacción a sitio.
- Atención Telefónica de reportes de Falla a la mesa de ayuda del proveedor y seguimiento hasta la solución. "la UAEM" asignará a un grupo responsable para interactuar y/o canalizar los reportes de falla y solicitudes a la mesa de ayuda del NOC. Este grupo será el filtro entre el usuario final y la mesa de ayuda del NOC.
- Soporte y diagnóstico remoto de falla y cuando no pueda resolverse por esta vía se deberá coordinar el envío de un ingeniero a sitio
- Coordinación, solicitud y seguimiento de mantenimientos preventivos
- Soporte de tercer nivel del fabricante de los equipos soportados

ADMINISTRACIÓN DE CONFIGURACIONES Y REGISTRO DE INVENTARIOS

ALCANCES:

- Altas, bajas y cambios, vía acceso remoto, a los equipos de la red MPLS e Internet.
- Control y administración de bitácoras de los equipos de la red
- Control, mantenimiento y actualización de la memoria técnica de la red
- Control, mantenimiento y actualización de inventarios
- Administración de los Niveles de Servicio y control de cambios
- Administración, mantenimiento, actualización y respaldo de configuraciones de los equipos
- Pruebas semestrales de funcionamiento de respaldos

ADMINISTRACIÓN DEL DESEMPEÑO

- Generación y entrega mensual de los siguientes reportes de Monitoreo :

De desempeño de los equipos de la red MPLS e Internet
% Utilización de CPU y Memoria.
Volumen de Tráfico transmitido por puerto WAN.
Consumo de ancho de banda Principal (Entrada, Salida y Promedio).
Consumo de ancho de banda Respaldo (Entrada, Salida y Promedio).
Consumo de ancho de banda por QoS
Paquetes enviados / recibidos.
Paquetes perdidos por errores y descartes
Disponibilidad por enlace a la red MPLS e Internet

000016

- Generación y entrega mensual de los siguientes reportes de Administración de fallas:

Administración de fallas
Clasificación de reportes por tipo de falla
Frecuencia y tipo de fallas
Identificación de problemas
Plan de acción para corregir desviaciones en los niveles de servicio
Tiempo promedio de solución y respuesta
Casos abiertos y cerrados
Proactividad: casos proactivos, casos reactivos (en porcentaje y gráfica)

NIVELES DE SERVICIO
VENTANA DESERVICIO DE RED ADMINISTRADA

Servicio	Cobertura
Administración de fallas	7 x 24 x 365
Administración del desempeño	7 x 24 x 365
Centro de operación de red NOC	7 x 24 x 365

TIEMPOS DE RESPUESTA EN ATENCIÓN A REPORTES DE FALLA EN LOS SERVICIOS DE COMUCACIONES Y EQUIPOS DE SEGURIDAD

CONCEPTO	DESCRIPCIÓN	NIVEL DE SERVICIO
Tiempo de apertura de reporte.	Tiempo máximo para detectar y levantar un reporte de falla y comunicarlo a "la UAEM".	15 min
Tiempo de atención de reporte.	Tiempo para la atención del reporte de falla detectado.	30 min
Tiempo de solución de reporte de falla.	Tiempo máximo para solución del reporte, en caso de que la falla pueda resolverse vía remota.	4 horas + Tiempo de Traslado