UNIVERSIDAD DE GUADALAJARA

Red Universitaria de Jalisco

CARATULA CONTRATO COMPRAVENTA

LAS PARTES

LA UNIVERSIDAD		EL VENDEDOR	
Nombre, denominación o razón social	Universidad de Guadalajara	**Nombre, denominación o razón social**	INITEL S.A. de C.V.
Representante	Dra. Carmen Enedina Rodríguez Armenta	**Acta Constitutiva**	Escritura Pública No. 50,136 de fecha 27 de Diciembre de 2002, ante el Lic. Jorge Robles Farías, Notario Público Titular No. 12, Guadalajara, Jalisco.
Título	Apoderada	**Representante**	Ing. Teobaldo Leal Arriaga
		Título	Administrador General Único
Documento que acredita las facultades	Escritura Pública No. 6,931 de fecha 18 de abril de 2013, otorgada ante la fe del Lic. Juan José Serratos Cervantes, Notario Público No. 116 de Guadalajara, Jalisco	**Documento que acredita las facultades**	Acta Constitutiva
		R.F.C.	[redacted] 1
Domicilio	Avenida Juárez número 976, Zona Centro, Código Postal 44100, en Guadalajara, Jalisco	**Clave Patronal I.M.S.S.**	[redacted] 2
		Domicilio	[redacted] 3

OBJETO E IMPORTE

Denominación	Adquisición de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de... (ver acta de fallo)		
Clave	LI-SEMS-040-2017	**Procedimiento de Adjudicación**	Licitación
Dependencia responsable del seguimiento	Sistema de Educación Media Superior	**Dependencia o comité que adjudicó**	Comité de Compras y Adquisiciones del Sistema de Educación Media Superior
Cantidad a pagar	$11'654,366.40 Incluye IVA	**Partidas**	1 y 2
		Tipo de Recurso	☐ Estatal ☒ Federal
Forma de pago (periodicidad)	15 días posteriores a la entrega de la totalidad de los bienes a entera satisfacción de la Universidad	**Fondo**	Programa CONECTIC

PLAZO DE ENTREGA		INSTALACIÓN
Plazo de entrega	6 semanas	☐ SI incluye instalación
A partir de	La firma del presente	☒ NO incluye instalación

FIANZAS

☐	a) Fianza para garantizar la correcta aplicación de los recursos del anticipo, por el importe total de éste, la cual deberá ser cancelada solo con el consentimiento por escrito de LA UNIVERSIDAD, y que deberá ser entregada previo a la entrega de dicho anticipo.
☒	b) Fianza para garantizar el cabal cumplimiento de todas las obligaciones contenidas en el presente contrato, misma que se contratará por el 10% (diez por ciento) del valor total del presente, y que deberá ser entregada dentro de los tres días naturales siguientes a la firma del presente.
☐	c) Fianza para garantizar los defectos o vicios ocultos, la cual se contratará por la cantidad de 10% (diez por ciento) del valor total del presente contrato, la que contará con una duración de 1 (un) año a partir de la fecha en que LA UNIVERSIDAD reciba los bienes por escrito, y deberá ser cancelada solo con el consentimiento por escrito de LA UNIVERSIDAD, a la entrega del acta de recepción expedida por LA UNIVERSIDAD, y una vez entregada esta fianza, se procederá a la cancelación de las establecidas en los incisos a) y b), mediante el escrito que para tal efecto emita LA UNIVERSIDAD.
☐	d) No aplica

FIRMAS

Enteradas las partes del contenido y alcance, lo ratifican y firman en triplicado, de conformidad ante los testigos.

En la ciudad de Guadalajara, Jalisco		**Fecha**	21 de noviembre de 2017
LA UNIVERSIDAD		EL VENDEDOR	
		[redacted] 4	
Representante	Dra. Carmen Enedina Rodríguez Armenta	**Representante**	Teobaldo Leal Arriaga
Título	Apoderada	**Título**	Administrador General Único
TESTIGOS			
Nombre	Ing. Fernando Calvillo Vargas	**Nombre**	Mtra. Adriana Lorena Fierros Lara
Cargo	Coordinador de Servicios Generales del Sistema de Educación Media Superior	**Cargo**	Secretario Administrativo del Sistema de Educación Media Superior

CONTRATO DE COMPRAVENTA QUE CELEBRAN POR UNA PARTE **LA UNIVERSIDAD DE GUADALAJARA,** A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ **LA UNIVERSIDAD,** Y POR LA OTRA PARTE, LA PERSONA CUYA DENOMINACIÓN APARECE EN LA CARATULA DEL PRESENTE CONTRATO, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ **EL VENDEDOR,** DE ACUERDO A LAS SIGUIENTES:

DECLARACIONES:

Declara **LA UNIVERSIDAD**:

I. Que es un organismo público descentralizado del gobierno del Estado de Jalisco con autonomía, personalidad jurídica y patrimonio propios de conformidad con lo dispuesto en el artículo primero de su Ley Orgánica publicada por el Ejecutivo Estatal el día 15 de enero de 1994, en ejecución del Decreto número 15,319 del H. Congreso del Estado de Jalisco.
II. Que es atribución de la Universidad de Guadalajara, conforme a la fracción XI del artículo 6 de la Ley Orgánica, administrar su patrimonio.
III. Que el Rector General es la máxima autoridad ejecutiva de la Universidad, representante legal de la misma, de conformidad con el artículo 32 de la ley Orgánica de la Universidad.
IV. Que su representante cuenta con las facultades necesarias para suscribir el presente contrato, mismas que manifiesta no le han sido revocadas, modificadas o restringidas en sentido alguno.

Declara **EL VENDEDOR** bajo protesta de decir verdad:

I. Que tiene la capacidad jurídica para contratar y obligarse a suministrar los bienes adjudicados por **LA UNIVERSIDAD**.
II. Que conoce el contenido y los alcances del artículo29 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, y en su caso del artículo 50 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y que no se encuentra en alguno de los supuestos establecidos por el mismo.

Declaran las partes que han convenido celebrar el presente contrato, para lo cual se sujetan a lo establecido en las siguientes:

CLÁUSULAS:

PRIMERA.- Las partes acuerdan que el objeto del presente contrato es que **EL VENDEDOR** realice a favor de **LA UNIVERSIDAD** el suministro cuya denominación aparece en la carátula del mismo, y que se detalla en el documento que como Anexo "A" se acompaña al presente.

Al respecto **EL VENDEDOR** se sujetará conforme a las indicaciones que le dé **LA UNIVERSIDAD** y a lo establecido en el presente instrumento.

Todo aquello que **EL VENDEDOR** necesitará para lograr el cumplimiento de lo establecido en el presente, incluidos los costos de transportación de los bienes, será a su cargo exclusivamente, liberando en consecuencia a **LA UNIVERSIDAD** de cualquier reclamación que se intente en su contra por alguno de los conceptos antes señalados.

SEGUNDA.- LA UNIVERSIDAD se obliga a pagar a **EL VENDEDOR** por los conceptos amparados en el presente, la cantidad establecida en la carátula del presente.

LA UNIVERSIDAD pagará a **EL VENDEDOR** dicha cantidad conforme a lo establecido en la carátula del presente.

Por su parte **EL VENDEDOR** se compromete a entregar la factura correspondiente con los requisitos que las leyes fiscales establecen, y a su vez, asume cualquier obligación fiscal que se derive del presente contrato, sacando en paz y a salvo a **LA UNIVERSIDAD** de cualquier reclamación que al respecto se pudiera originar.

Adicionalmente las partes acuerdan que en el supuesto de que **EL VENDEDOR** no cumpla con alguna de sus obligaciones en los tiempos pactados o conforme a las características establecidas, el pago se verá retrasado en la misma proporción. Lo anterior independientemente de que **LA UNIVERSIDAD** decida continuar con el contrato o darlo por rescindido.

Así mismo, las partes acuerdan que el presente contrato quedará sujeto a la disponibilidad presupuestal, por lo que sus efectos estarán condicionados a la existencia de los recursos financieros correspondientes, sin que la no realización del mismo por esta causa origine responsabilidad para **LA UNIVERSIDAD**.

TERCERA.- EL VENDEDOR se obliga a realizar todas las gestiones necesarias y a tramitar a su cargo, todas las licencias, permisos, avisos, seguros aplicables, importaciones y demás autorizaciones en general que sean obligatorias y/o que se requieran, a fin de cumplir con lo establecido en el presente contrato.

EL VENDEDOR deberá pagar todas las multas debido a infracciones contempladas en las Leyes y/o Reglamentos aplicables al objeto del presente contrato, aún cuando no haya habido dolo o negligencia, liberando de cualquier responsabilidad a **LA UNIVERSIDAD**.

De igual forma **EL VENDEDOR** se obliga a tomar un seguro a su cargo y a favor de **LA UNIVERSIDAD**, para cubrir los riesgos derivados entre ellos los de responsabilidad civil, daños a terceros en sus bienes o personas etc., el cual deberá de estar vigente hasta el cumplimi sus obligaciones plasmadas a su cargo en el presente, acordándose que en caso de no contar con dicho seguro, **EL VENDEDOR** será responsable por dichos conceptos.

[redacted]

OFICINA DEL
ABOGADO GENERAL

CUARTA.- EL VENDEDOR se compromete ante **LA UNIVERSIDAD** a entregar, y en su caso instalar, los bienes objeto del presente dentro del plazo señalado en la caratula del presente contrato, en la dependencia que **LA UNIVERSIDAD** designe. Al respecto queda establecido que **EL VENDEDOR** no podrá realizar entregas parciales y el plazo concedido es para realizar la entrega total de los bienes o servicios contratados.

En caso de retraso en el cumplimiento de lo establecido en el presente, por causas imputables a **EL VENDEDOR**, éste pagará a **LA UNIVERSIDAD** por concepto de pena el 1.5% de los bienes no entregados o instalados y de los servicios no realizados. Dicha cantidad se podrá deducir por **LA UNIVERSIDAD** de los pagos pendientes a su cargo y a favor de **EL VENDEDOR**.

Independientemente de la aplicación de la pena antes señalada **LA UNIVERSIDAD** podrá optar entre exigir el cumplimiento forzoso de las obligaciones del presente contrato, o darlo por rescindido.

Por causas justificadas y debidamente acreditadas a **LA UNIVERSIDAD**, la misma podrá, si lo considera conveniente, ampliar previa petición por escrito de **EL VENDEDOR**, el plazo de entrega contemplado en la presente cláusula y en cuyo caso deberá suscribirse un convenio modificatorio y deberá actualizarse la fianza correspondiente por parte de **EL VENDEDOR**, misma que se entregará a **LA UNIVERSIDAD** a la firma del convenio modificatorio.

QUINTA.- EL VENDEDOR queda obligado a realizar todo lo establecido en el presente de acuerdo a lo estipulado por las partes, para lo cual se responsabiliza hasta el cumplimiento de todas sus obligaciones.

SEXTA.- EL VENDEDOR dará aviso por escrito a **LA UNIVERSIDAD** cuando concluya con las obligaciones pactadas a su cargo en el presente, para que ésta última proceda a levantar un acta de entrega recepción por conducto de quien la misma señale.

SÉPTIMA.- Las partes acuerdan que **EL VENDEDOR** tiene prohibido:

a) Encomendar o subcontratar con otra persona la entrega o instalación de los bienes objeto del presente contrato, así como la cesión total o parcial de los derechos y obligaciones del mismo.
b) En su caso, hacer cambios estructurales en la o las instalaciones en donde se colocarán los bienes objeto del presente, sin la previa autorización por escrito de **LA UNIVERSIDAD**, estableciendo que en caso de no respetar lo antes señalado, **EL VENDEDOR** será responsable de los daños y perjuicios y la responsabilidad civil que dicho incumplimiento cause, lo anterior independientemente de la rescisión o cumplimiento forzoso del contrato.

OCTAVA.- EL VENDEDOR en tanto no se levante el acta de entrega recepción correspondiente, reconoce que **LA UNIVERSIDAD** no será responsable de la perdida (total o parcial), deterioro o maltrato de los bienes, materiales, herramientas o cualquier otro bien relacionado con el objeto del presente, ni aun en el supuesto de caso fortuito o fuerza mayor, ya que los mismos son responsabilidad directa de **EL VENDEDOR**, liberando a **LA UNIVERSIDAD** de cualquier responsabilidad que se pudiera derivar del presente concepto.

NOVENA.- Los servicios de entrega o, en su caso, de instalación de los bienes materia del presente contrato se ejecutarán durante días y horas hábiles de la o las dependencias universitarias en las cuales se entregarán los bienes materia del presente, acordando las partes que en caso de ser necesario realizar trabajos durante horas y días inhábiles, los mismos podrán llevarse a cabo, previa autorización por escrito que al efecto expida **LA UNIVERSIDAD**.

DÉCIMA.- La supervisión de lo establecido en el presente, estará a cargo de la Coordinación de Servicios Generales de la dependencia responsable o de la persona o las personas que esta última designe, quienes podrán inspeccionar en todo tiempo todo lo relacionado con los bienes, pudiendo en su caso, rechazar por escrito lo que no se ajuste a lo estipulado en el contrato y su Anexo "A".

Al respecto **EL VENDEDOR** se compromete a entregar los bienes nuevos y de primera calidad, según se establece en las especificaciones técnicas, siendo responsable de los daños y perjuicios, y la responsabilidad civil, que cause debido a la mala calidad de los mismos.

De existir inconformidad respecto a lo contemplado en esta cláusula, **LA UNIVERSIDAD** solicitará a **EL VENDEDOR** reemplazar a costa de esta última, los bienes defectuosos o no adecuados.

DÉCIMA PRIMERA.- EL VENDEDOR además de observar el cumplimiento de este contrato, estará obligado a lo siguiente:

a) Vigilar que el objeto del presente contrato sea de acuerdo a lo aprobado, y a las características especificaciones requeridas.
b) En su caso hacer la revisión detallada de la instalación de los bienes, rindiendo el informe correspondiente.
c) Tener en todo momento personal técnico capacitado para la dirección, supervisión e instalación y demás actividades relacionadas con el objeto materia de este contrato.
d) Estar al corriente de todas las contribuciones que se originen por el desempeño de su actividad.
e) Responder de la perdida, daño, robo o extravío de los bienes, hasta el momento en que se realice el acta de entrega recepción correspondiente, aún en el supuesto de que dichos bienes se encuentren en las instalaciones de **LA UNIVERSIDAD.**
f) Cumplir con todas las obligaciones derivadas de la ley, del presente y su Anexo "A".

DÉCIMA SEGUNDA.- LA UNIVERSIDAD podrá dar por terminado anticipadamente en cualquier momento el presente contrato, circunstancias imprevistas o razones de interés general, previa notificación por escrito a **EL VENDEDOR** con cuando menos 5 (cinco anticipación.

Adicionalmente, acuerdan las partes que **LA UNIVERSIDAD** podrá suspender los trabajos y/o pagos objeto del presente, en presente alguno de los supuestos que a continuación se mencionan de manera enunciativa mas no limitativa:

4

[redacted]

a) En su caso cuando existan bienes y/o trabajos defectuosos o no adecuados, que no se reemplacen o corrijan, dentro de los 30 (treinta) días siguientes a la fecha en que **LA UNIVERSIDAD** lo haga del conocimiento de **EL VENDEDOR**.
b) Incumplimiento de **EL VENDEDOR** por no estar al corriente en el pago de las contribuciones que se generen por su operación o el pago de sus obligaciones directas e indirectas con su personal.
c) Por presentación de reclamación de cualquier naturaleza, si se llegara a formalizar, en contra de **LA UNIVERSIDAD** derivada del objeto del presente contrato.
d) Si **EL VENDEDOR** no entrega las fianzas a que se hace referencia en el presente contrato, dentro de los términos establecidos para tal efecto.
e) Si **EL VENDEDOR** cayera en insolvencia o se declara en concurso mercantil.
f) Por muerte o disolución de **EL VENDEDOR**, según corresponda.
g) En general por cualquier incumplimiento por parte de **EL VENDEDOR** a cualquiera de las obligaciones derivadas del presente contrato, su anexo o la ley.

A juicio de **LA UNIVERSIDAD** y una vez que se subsanen los problemas a que se refieren los incisos anteriores, se podrán reanudar los efectos y/o pagos o rescindir el presente contrato.

DÉCIMA TERCERA.- En caso de que se presente algún defecto o vicio oculto relacionado con el objeto del presente contrato, **EL VENDEDOR** será la responsable ante **LA UNIVERSIDAD** por los mismos.

DÉCIMA CUARTA.- La entrega, y en su caso instalación, de los bienes detallados en el presente contrato y su Anexo "A" deberá quedar terminada en el plazo que se consigna en la carátula del presente.

El plazo de terminación del presente instrumento solo podrá ser ampliado en caso de que haya modificaciones en lo establecido en el objeto del presente contrato, en caso fortuito o de fuerza mayor de conformidad a la ley o por mutuo acuerdo.

Para que el objeto del presente instrumento se pueda considerar como satisfecho se deberá haber cumplido con lo establecido en el contrato y su Anexo "A".

DÉCIMA QUINTA.- Las partes convienen en que **EL VENDEDOR** se compromete a cumplir con todas y cada una de las obligaciones derivadas de la relación laboral que imponen la Ley Federal del Trabajo, y demás ordenamientos legales aplicables a los patrones; por lo tanto **EL VENDEDOR** será el único responsable y obligado para con los trabajadores, ante todo tipo de autoridades ya sean administrativas o judiciales, Federales, Estatales o Municipales.

En consecuencia, **EL VENDEDOR** asume todas las responsabilidades como patrón con relación a los trabajadores que emplee, liberando de posibles indemnizaciones, demandas o cualquier reclamación que éstos iniciaran en contra de **LA UNIVERSIDAD**.

LA UNIVERSIDAD, no será responsable por ninguna reclamación que en contra de **EL VENDEDOR** presenten sus empleados o colaboradores, obligándose ésta última a sacar en paz y a salvo a **LA UNIVERSIDAD** de cualquier reclamación de esta naturaleza, ya sea laboral, administrativa, civil o penal, incluyéndose los accidentes de trabajo.

Asimismo, será obligación de **EL VENDEDOR** hacer la retención y entero de las contribuciones correspondientes de los trabajadores que emplee con motivo del presente contrato.

DÉCIMA SEXTA.- EL VENDEDOR otorgará a favor de **LA UNIVERSIDAD** las fianzas descritas en la carátula del presente contrato, expedidas por una compañía legalmente constituida y registrada, con oficinas en la ciudad de Guadalajara, Jalisco, y que se sujeten a la jurisdicción de los tribunales competentes de esta ciudad.

Adicionalmente **EL VENDEDOR** manifiesta expresamente lo siguiente:

(A) Su conformidad para que la fianza de cumplimiento se pague independientemente de que se interponga cualquier tipo de recurso ante instancias del orden administrativo o no judicial.
(B) Su conformidad para que la fianza que garantiza el cumplimiento del contrato, permanezca vigente durante la substanciación de todos los procedimientos judiciales o arbítrales y los respectivos recursos que se interpongan con relación al presente contrato, hasta que sea dictada resolución definitiva que cause ejecutoria por parte de la autoridad o tribunal competente.
(C) Su aceptación para que la fianza de cumplimiento permanezca vigente hasta que las obligaciones garantizadas hayan sido cumplidas en su totalidad a satisfacción de **LA UNIVERSIDAD**.

DÉCIMA SÉPTIMA.- Además de las causas previstas por la Ley, las partes convienen en que el presente contrato podrá ser rescindido por **LA UNIVERSIDAD** cuando **EL VENDEDOR** no haya cumplido con todas o alguna de las obligaciones que a su cargo se derivan de éste contrato, en especial si la entrega o instalación no cumple con las características pactadas.

Serán causas de rescisión del presente contrato las que a continuación se mencionan enunciativamente más no limitativamente

a) Si **EL VENDEDOR,** por causas imputables a ella o a sus dependientes, no entrega los bienes, según lo acordado anexo.
b) Si **EL VENDEDOR,** en su caso, no entrega los trabajos contratados totalmente terminados dentro del plazo seña contrato y su anexo.

[redacted]

OFICINA DEL
ABOGADO GENERAL

c) Si **EL VENDEDOR,** en su caso, suspende injustificadamente los trabajos objeto del presente o se niega a reparar o responder alguno que hubiere sido rechazado por **LA UNIVERSIDAD,** en un término de 30 (treinta) días.
d) Si **EL VENDEDOR** cayera en insolvencia o se declara en concurso mercantil.
e) Por muerte o disolución de **EL VENDEDOR**, según sea el caso.
f) En general por cualquier incumplimiento por parte de **EL VENDEDOR** a cualquiera de las obligaciones derivadas del presente contrato, su anexo o la ley.

En caso de incumplimiento por parte de **EL VENDEDOR** en cualquiera de las obligaciones previstas en este contrato **LA UNIVERSIDAD** podrá rescindir el contrato o exigir el cumplimiento del mismo.

Si **LA UNIVERSIDAD** opta por rescindir el contrato por causa imputable a **EL VENDEDOR,** está última, quedará obligada a cubrir los daños y perjuicios que por tal motivo ocasione a **LA UNIVERSIDAD,** los cuales no podrán ser inferiores al 20% (veinte por ciento) del monto total del presente instrumento.

DÉCIMA OCTAVA.- Acuerdan las partes que en caso de que el presente contrato incluya mantenimiento preventivo, mantenimiento correctivo y/o capacitación, las actividades relacionadas con los mismos se realizarán conforme lo determinen las partes.

DÉCIMA NOVENA.- Queda establecido que **EL VENDEDOR** no podrá ceder o transferir parcial o totalmente los derechos y las obligaciones derivadas del presente instrumento, sin el previo consentimiento por escrito de **LA UNIVERSIDAD,** siendo responsable de los daños y perjuicios que tal incumplimiento cause.

VIGÉSIMA.- Nada de lo previsto en este contrato ni de las acciones que se deriven de su suscripción, podrá considerarse o interpretarse para constituir o considerar a las partes y al personal de las mismas que colabore en la ejecución de este contrato como socios, agentes, representantes o empleados uno del otro, y ninguna de las disposiciones de este contrato será interpretada para forzar a la otra parte a asumir cualquier obligación o a actuar o pretender actuar como representante de la otra.

VIGÉSIMA PRIMERA.- El presente contrato, podrá ser modificado previo acuerdo por escrito entre las partes y durante la vigencia del mismo, apegándose a la normatividad aplicable, y a través de los instrumentos jurídicos correspondientes, obligándose las partes a las nuevas estipulaciones, a partir de la fecha de su firma.

VIGÉSIMA SEGUNDA.- Si alguna de las disposiciones contenidas en el presente contrato, llegara a declararse nula por alguna autoridad, tal situación no afectará la validez y exigibilidad del resto de las disposiciones establecidas en este contrato. Al respecto las partes negociarán de buena fe la sustitución o modificación mutuamente satisfactoria de la cláusula o cláusulas declaradas nulas o inválidas por otras en términos similares y eficaces.

En caso de que el presente contrato llegara a declararse nulo por la autoridad competente o el mismo se rescindiera por causa imputable a **EL VENDEDOR**, el mismo estará obligado a devolver a **LA UNIVERSIDAD** la o las cantidades que le hayan sido entregadas, más la actualización correspondiente conforme al Índice Nacional de Precios al Consumidor, tomando como base la fecha en que se realizó la primera entrega por parte de **LA UNIVERSIDAD** y la fecha en que sean devueltas las mismas, lo anterior independientemente de los daños y perjuicios que por tal motivo tenga derecho a reclamar a **LA UNIVERSIDAD**.

VIGÉSIMA TERCERA.- EL VENDEDOR se obliga a que los bienes serán nuevos y de la calidad señalada en las especificaciones del Anexo "A", y responderá por cualquier defecto en cualquiera de las partes de los bienes y accesorios objeto del presente, o por la instalación y puesta en marcha de los mismos.

La garantía está sujeta a que los bienes sean utilizados de acuerdo a las especificaciones y características de estos.

VIGÉSIMA CUARTA.- Ambas partes acuerdan que cualquier controversia relacionada con la interpretación, contenido o ejecución del presente contrato, se sujetará a lo establecido en el presente contrato y de manera supletoria a lo establecido en los documentos señalados a continuación y en el orden siguiente; en el anexo, las bases del procedimiento correspondiente, la propuesta presentada por **EL VENDEDOR**, la legislación federal, la universitaria y demás leyes aplicables.

En este sentido queda establecido que si existe alguna discrepancia en la información contenida en alguno de los documentos señalados en el párrafo anterior, siempre será aplicable la disposición que sea más favorable para **LA UNIVERSIDAD,** quedando sin efectos la disposición distinta.

VIGÉSIMA QUINTA.- Para todo lo relacionado con la interpretación y cumplimiento del presente contrato, las partes se someten voluntariamente a las leyes aplicables de la República Mexicana y a la jurisdicción y competencia de las autoridades de la ciudad de Guadalajara, Jalisco, renunciando a cualquier otro fuero o jurisdicción que pudiera corresponderles en virtud de su domicilio presente o futuro.

Las partes enteradas del contenido y alcance del presente contrato, manifiestan que en el mismo no existe mala fe, dolo o error y firman por triplicado en la carátula del mismo, en compañía de los testigos, en la ciudad de Guadalajara, Jalisco.

OFICINA DEL
ABOGADO GENERAL

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD		DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
1	39	FG-200E-BDL-900-36 **Mca. FORTINET**	SOLUCIONUTM/NGFW TIPO 1 (1 UNIDAD)	$ 117,278.61	$ 4,573,865.79

Throughput de por lo menos 9 Gbps con la funcionalidad de firewall habilitada para trafico 1Pv4 y 1Pv6, independiente del tamafio del paquete

Soporte a por lo menos 2M conexiones simultaneas
Soporte a por lo menos 135K nuevas conexiones por segundo
Throughput de al menos 9 Gbps de VPN IPSec
Estar licenciado para, o soportar sin necesidad de licencia, 2K tuneles de VPN

IPSec site-to-site simultaneos
Estar licenciado para, o soportar sin necesidad de licencia, lOK tuneles de

clientes VPN IPSec simultaneos
Throughput de al menos 900 Mbps de VPN SSL
Soportar al menos 300 clientes de VPN SSL simultaneos
Soportar al menos 6000 Mbps de throughput de IPS
Soportar al menos 1000 Mbps de throughput de Inspecci6n SSL
Throughput de al menos 1200 Mbps con las siguientes funcionalidades habilitadas simuttaneamente para todas las firmas que la solución de seguridad tenga debidamente activadas y operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado

multiples oumeros de desempefio para cualquier de las funcionalidades,

solamente el de valor mas pequefio sera aceptado.
Permitir gestionar al menos 64 Access Points
Tener al menos 14 interfaces 1 Gbps RJ45, 4 Gbps SFP, 2 Gbps para WAN
Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas

virtuales lógicos (Contextos) par appliance
Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) par appliance
Debe de incluir un token fisico para autenticaciónde doble factor para la gestión del appliance o para el acceso VPN que debe ser de la misma marca

propuesta
Debe de brindar soporte 36 meses del tipo 8x5, reemplazo siguiente dia habil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus,

Botnet IP/Domain, AntiSpam y Filtrado Web

.

REQUISITOS MINIMOS DE FUNCIONALIDAD
Caracteristicas Generales
La solución debe consistir en una plataforma de protecciónde Red, basada

en un dispositivo con funcionalidades de Firewall de Próxima generación

(NGFW), asi coma consola de gestión y monitoreo. ;
Porfuncionalidades de NGFW se entienda: aplicaciones de reconocimiento,

prevenci6n de amenazas, identificación de usuarios y control granular de permisos;
Las funcionalidades de protecciónde red que conforman la plataforma de

seguridad, puede ejecutarse en multiples dispositivos siempre que cum plan

todos los requisites de esta especificaci6n;
La plataforma debe estar optimizada para aplicaciones de analisis de contenido en la capa 7;
Todo el equipo proporcionado debe ser adecuado para montaje en rack de

19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;

La gestión del equipo debe ser compatible con acceso a traves de SSH, consola, web (HTIPS) y API abierta;
La gestión del equipos debe ser compatible a traves de la interfaz de administraci6n Web en el mismo dispositivo de protecciónde la red
Los dispositivos de protecciónde red deben soportar 4094 VLANs Tags 802.lq;
Los dispositivos de protecciónda red deben soportar agregaci6n de enlaces

802.3ad y LACP;
Los dispositivos de protecciónde red deben soportar Policy based routing y

policy based forwarding;

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

inite

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017

"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Los dispositivos de protecciónde red deben soportar encaminamiento de multicast (PIM-SM y PIM-OM); Los dispositivos de protecciónde red deben soportar DHCP Relay; Los dispositivos de protecciónde red deben soportar DHCP Server; Los dispositivos de protecciónde red deben soportar sFlow Los dispositivos de protecciónde red deben soportar Jumbo Frames; Los dispositivos de protecciónde red deben soportar sub-interfaces Ethernet 16gicas Debe ser compatible con NAT dinamica (varios-a-1); Debe ser compatible con NAT dinarnica (muchos-a-muchos); Debe soportar NAT estatica (I-a-1); Debe admitir NAT estatica (muchos-a-muchos); Debe ser compatible con NAT estatico bidireccional 1-a-1; Debe ser compatible con la traducci6n de puertos (PAT); Debe ser compatible con NAT Origen; Debe ser compatible con NAT de destine; Debe soportar NAT de origen y NAT de destino de forma simultanea: Debe soportarTraducci6n de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asirnetrico: Debe ser compatible con NAT64 y NAT46; Debe implementar el protocolo ECMP; Debe soportar el balanceo de en lace hash por IP de origen; Debe soportar el balanceo de en lace hash por IP de origen y destine; Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de traftco que fluira a traves de cada uno de los en laces. Debe ser compatible con el balanceo en al menos tres en laces; Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran numero de sesiones, conexiones por segundo, cantidad de tuneles establecidos en la VPN, CPU, memoria, estado del cluster, ataques y estadfsticas de uso de las interfaces de red Enviar logs a sistemas de gestión externos simultaneamente: Debe tener la opción de envíar logs a los sistemas de control externo a traves de TCP y SSL; Debe soporta protecciónccontra la suplantaci6n de identidad (anti-spoofing); Implementar la optimizaci6n del trafico entre dos dispositivos; Para 1Pv4, soportar enrutamiento estatlco y dinarnico (RIPv2, OSPFv2 y BGP); Para 1Pv6, soportar enrutamiento estatlco y dinarnico (OSPFv3); Soportar OSPF graceful restart; Los dispositivos de protecciódeben tener la capacidad de operar simultaneamente en una unica instancia de servidor de seguridad, mediante el uso de sus interfaces ffsicas en los siguientes modos: modo sniffer (monitoreo y anallsis de trafico de red), capa 2 (L2) y capa 3 (L3); Debe ser compatible con el modo Sniffer para la inspección a traves del puerto espe]o del trafico de datos de la red; Debe soportar modo capa - 2 (L2) para la inspección de datos en linea y la visibilidad del trafico: Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en lfnea de trafico: Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces fisicas; Soportar la configuración de alta disponibilidad active I pasivo y activo I active: En modo transparente; Soportar la configuración de alta disponibilidad activo I pasivo y activo I activo: En capa 3; Soportar configuración de alta disponibilidad active I pasivo y activo I activo: En la capa 3 y con al menos 3 dispositivos en el cluster; La configuración de alta disponibilidad debe sincronizar: Sesiones; La configuración de alta disponibilidad debe sincronizar: configuración , incluyendo, pero no limitados poHticas de Firewalls, NAT, QoS y objetos de la red;		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

in elo

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN;
La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
En modo HA (Modo de alta disponibilidad) debe permitir la supervision de fallos de enlace;
Debe soportar la creación de sistemas virtuales en el mismo equipo;
Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribuci6n de la carga entre los diferentes contextos;
Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes equipos;
La solución de gestión debe ser compatible con el acceso a traves de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportaci6n de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
Debe aportar el control, la inspección y el descifrado de SSL para el trafico entrante (inbound) y la salida (outbound), y debe ser compatible con el control de certificados de forma individual dentro de cada sistema virtual, es decir, el aislamiento de la adición, eliminación y uso de los certificados directamente en cada sistema virtual (contextos);
• CONTROL POR POLITICA DE FIREWALL
Debe soportar controles de zona de seguridad
Debe contar con políticas de control por puerto y protocolo
Contar con políticas por aplicación, grupos estatrcos de aplicaciones, grupos dlnamtcos de aplicaciones (en base a las caracteristicas y comportamiento de las aplicaciones) y categorias de aplicaciones
Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad
Control de política por código de pais (por ejemplo: BR, USA., UK, RUS)
Control, inspección y des encriptación de SSL por polftica para el trafico entrante y la salida
Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada;
Debe descifrar las conexiones de entrada y salida de trafico negociadas con TLS 1.2;
Control de inspección y descifrado SSH por politica;
Debe permitir el bloqueo de archivos por su extension y permitir la identificación de archivo correcto por su tipo, incluso cuando se cambia el nombre de su extension;
Traffic shaping QoS basado en políticas (garantia de prioridad y maxima);
QoS basado en políticas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones;
Soporte para objetos y reglas IPV6;
Soporte objetos y reglas de multicast;
Debe ser compatible con al menos tres tipos de respuesta en las políticas de firewall: 'Drop' sin la notificaci6n de bloqueo del usuario, 'Drop' con la notificaci6n de bloqueo del usuario, Drop con opción de env[o ICMP inalcanzable por la maquina fuente de trafico, TCP Reset para el cliente, RESET de TCP con el servidor o en ambos lados de la conexión;
Soportar la calendarizaci6n de políticas con el fin de activar y desactivar las reglas en tiempos predefinidos de forma automatica:
• CONTROL DE APLICACION
Los dispositivos de protecciónde red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo
Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos
Reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no limitado a: el trafico relacionado peer-to-peer, redes sociales, acceso remote, actualizaci6n de software, protocolos de red, VoIP, audio, video,

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

Proxy, mensajería instantanea, compartici6n de archives, correo electr6nico;

Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype,

facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail,

youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp,
4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory,

kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc
over http, gotomeeting, webex, evernote, google-docs;
Debe inspeccionar la carga util (payload) del paquete de datos con el fin de

detectar las firmas de las aplicaciones conocidas por el fabricante
independiente de puerto y protocolo;
Debe detectar aplicaciones a traves del analisis del comportamiento del
trafico observado, incluyendo, pero no limitado a las aplicaciones de VoIP

que utilizan cifrado propietario y BitTorrent;
Identificar el uso de tacticas evasivas, es decir, debe tener la capacidad de

very controlar las aplicaciones y los ataques con tacticas evasivas a traves de

las comunicaciones cifradas, tales como Skype y la utilizaci6n de la red Tor

Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura

de payload para permitir la identificación de firmas de la aplicación
conocidas por el fabricante;
Debe hacer decodificación de protocolos con el fin de detectar aplicaciones

encapsuladas dentro del protocolo y validar que el trafico corresponde a la

especificaci6n del protocolo, incluyendo, pero no limitado a Yahoo Instant

Messenger utilizando HTIP. La decodificación de protocolo tambien debe

identificar las caractedsticas espedficas dentro de una aplicación,
incluyendo, pero no limitado al intercambio de ficheros dentro de Webex

identificar el uso de tacttcas evasivas a traves de las comunicaciones cifradas;

Actualizaci6n de la base de firmas de la aplicación de forma automatica:
Limitar el ancho de banda (carga i descarga) utilizado por las aplicaciones
traffic shaping), basado en IP de origen, usuarios y grupos;
Los dispositivos de protecciónde red deben tener la capacidad de identificar

al usuario de la red con la integración de Microsoft Active Directory sin
necesidad de instalaci6n del agente en el controlador de dominio, o en
estaciones de trabajo de usuario;
Debe ser posible afiadir multiples reglas de control de aplicaciones, es decir,

no debe limitar habilitar el control de aplicaciones de control solamente en

algunas reglas;
Debe ser compatible con multiples metodos de identificación y clasificaci6n

de las aplicaciones, al menos verificar firmas y protocolos de decodificación;

Para mantener la seguridad de red eficiente debe ser soportar el control de

las aplicaciones desconocidas y no solo en aplicaciones conocidas;
Permitir la creación de forma nativa de fir mas personalizadas para el
reconocimiento de aplicaciones propietarias en su propia interfaz grafica, sin

la necesidad de la acci6n del fabricante
La creación de firmas personalizadas debe permitir el uso de expresiones

regulares, el contexto (sesiones o transacciones), utilizando la posici6n en el

payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los

siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-
SQL, IMAP, DNS, LDAP, SSL y RTSP
El fabricante debe permitir solicitar la inclusion de aplicaciones en su base de

dates;
Debe alertar al usuario cuando sea bloqueada una aplicación;
Debe permitir la diferenciación de trafico Peer2Peer (Bittorrent, eMule, etc)

permitiendo granularidad de control/reglas para el mismo;

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Debe permitir la diferenciacion de trafico de mensajeria Instantanea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo; Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video; Debe permitir la diferenciacion de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo; Debe ser posible la creación de grupos dinamicos de aplicaciones, basado en las caracteristicas de las mismas, tales coma: Tecnologia utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc) Debe ser posible crear grupos dlnarntcos de aplicaciones basados en caracteristicas de las mismas, tales como: nivel de riesgo de la aplicacion Debe ser posible crear grupos estaticos de aplicaciones basadas en caracterfsticas de las mismas, tales como: Categoria de Aplicacion • PREVENCION DE AMENAZAS Para proteger el entorno contra las ataques, deben tener modulo IPS, antivirus y anti-spyware integrado en el propio equipo; Debe incluir firmas de prevenci6n de intrusiones (IPS) y el bloqueo de archives maliciosos (antivirus y anti-spyware); Las caracteristicas de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no existe un contrato de garantfa del software con el fabricante; Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad; Debe implementar los siguientes tipos de acciones a las amenazas detectadas par IPS: permitir, permitir y generar registro, bloque, bloque del IP del atacante durante un tiempo y enviar tcp-reset; Las firmas deben ser capaces de ser activadas o desactivadas, o activadas solo en el modo de monitoreo; Deben ser posible crear polltlcas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas; Debe soportar granularidad en las politicas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes politicas par zona de seguridad, dirección de origen, dirección de destina, servicio y la combinaci6n de todos estos elementos Deber permitir el bloqueo de vulnerabilidades Debe permitir el bloqueo de exploits conocidos Debe incluir la protecciónContra ataques de denegacion de servicio Debe tener los siguientes mecanismos de inspección IPS: Analisis de patrones de estado de las conexiones; Debe tener los siguientes mecanismos de inspeccion IPS: analisis de decodificación de protocolo; Debe tener los siguientes mecanismos de inspeccion IPS: analisis para detectar anomalfas de protocolo; Debe tener los siguientes mecanismos de inspección IPS: Analisis heuristico; Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP; Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP; Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formate incorrecto (malformed packets) Debe ser inmune y capaz de prevenir los ataques basicos, tales como inundaciones SYN, ICMP, UDP, etc; Detectar y bloquear los escaneos de puertos de origen; Bloquear ataques realizados por gusanos (worms) conocidos; Contar con firmas especfficas para la mitlgacion de ataques DoS y DDoS; Contar con firm as para bloquear ataques de desbordamiento de memoria		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V. 1
R.F.C.: [redacted]
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

intermedia (buffer overflow);
Debe poder crear firmas personalizadas en la interfaz grafica del producto;

Debe permitir utilizar operadores de negaci6n en la creacion de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración ;
Permitir bloqueo de virus y software espia en por lo menos los siguientes

protocolos: HTIP, FTP, SMB, SMTP y POP3;
Soportar el bloqueo de archives por tipo;
Identificar y bloquear la comunicaci6n con redes de bots;
Registrar en la consola de supervision la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la apltcacion, el usuario, el origen y destine de las comunicaciones, adernas de las medidas

adoptadas por el dispositivo;
Debe ser compatible con la captura de paquetes (PCAP), mediante la firma

de IPS o control de aplicación;
Debe permitir la captura de paquetes por tipo de firma IPS para definir el

numero de paquetes capturados o permitir la captura del paquete que dio

lugar a la descripci6n, asf como su contexto, facilitando el anallsis forense y

la identificación de falsos positives
Debe tener la funci6n de protecciónа traves de la resolución de direcciones

DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
Los eventos deben identificar el pais que origino la amenaza;
Debe incluir protecciónontra virus en contenido HTML y Java script, software espia (spyware) y gusanos (worms)
Tener protecciónontra descargas involuntarias mediante archives ejecutables maliciosos y HTIP
Debe permitir la configuración de diferentes politicas de control de amenazas y ataques basados en politicas de firewall considerando usuarios,

grupos de usuarios, origen, destine, zonas de seguridad, etc., es decir, cada

polftica de firewall puede tener una configuración diferente de IPS basada en

usuario, grupos de usuarios, origen, destine, zonas de seguridad
•
FILTRADO DE URL
Debe permitir especificar la politica por tiempo, es decir, la definición de

reglas para un tiempo o periodo determinado (dia, mes, afio, dfa de la semana y hara);
Debe ser posible crear polfticas para usuarios, IPs, redes, o zonas de seguridad
Debe tener la capacidad de crear politicas basadas en la visibilidad y el control de quien esta utilizando las URL esto mediante la integración con las

servicios de directorio Active Directory, y la base de datos local;
Debe tener la capacidad de crear politicas basadas en la visibilidad y el control de quien esta usando las URL que mediante la integración con las

servicios de directorio Active Directory, y la base de dates local, en modo de

proxy transparente y explicito;
Debe soportar la capacidad de crear politicas basadas en control por URL y

categorfa de URL
Debe tener la base de datos de URLs en cache en el equipo o en la nube del

fabricante, evitando retrasos de comunicaci6n I validaci6n de direcciones

URL;
Tener por lo menos 60 categorias de URL;
Debe tener la funcionalidad de exclusion de URLs por categoria
Permitir pagina de bloqueo personalizada;
Permitir el bloqueo y continuaci6n (que permite al usuario acceder a un sitio

bloqueado potencialmente Informandole en la pantalla de bloqueo y permitiendo el uso de un bot6n Continuar para que el usuario pueda seguir

teniendo acceso al sitio);
•

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

IDENTIFICACION DE USUARIOS
Se debe incluir la capacidad de crear politicas basadas en la visibilidad y el

control de quien esta usando dichas aplicaciones a traves de la integración

con los servicios de directorio, a traves de la autenticaciónLDAP, Active Directory, E-directorio y base de datos local;
Debe tener integración con Microsoft Active Directory para identificar a los

usuarios y grupos, permitiendo granularidad a las polfticas / control basados

en usuarios y grupos de usuarios;
Debe tener integración y soporte para Microsoft Active Directory para los

siguientes sistemas operatives: Windows Server 2003 R2, Windows Server

2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2;
Debe tener integración con Microsoft Active Directory para identificar a los

usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener lf mites licenciados de usuarios o cualquier restricci6n de uso como, pero no limitado a, utilizaci6n de sistemas virtuales,

segmentos de red, etc;
Debe tener integración con RADIUS para identificar a los usuarios y grupos

que permiten las politicas de granularidad / control basados en usuarios y

grupos de usuarios;
Debe tener la integración LDAP para la identificación de los usuarios y grupos

que permiten granularidad en la politicas/control basados en usuarios y grupos de usuarios;
Debe permitir el control sin necesidad de instalaci6n de software de cliente,

el equipo que solicita salida a Internet, antes de iniciar la navegaci6n, entre a

un portal de autentificaci6n residente en el equipo de seguridad (portal cautivo);
Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix
y Microsoft Terminal Server, lo que permite
una visibilidad y un control granular por usuario en el uso de las aplicaciones

que se encuentran en estos servicios;
Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos del LDAP I AD
Permitir la integración con tokens para la autenticaciónde usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.

Proporcionar al menos un token de forma nativa, lo que permite la autenticaciónde dos factores
•
QOS TRAFFIC SHAPING
Con el fin de controlar el trafico y aplicaciones cuyo con sumo puede ser excesivo (como YouTube, Ustream, etc.) y tienen un alto consume de ancho

de banda, se requiere de la solución que, ademas de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda

maxima cuando son solicitados por los diferentes usuarios o aplicaciones,

tanto de audio coma de video streaming;
Soportar la creación de politicas de QoS y Traffic Shaping par dirección de

origen;
Soportar la creación de politicas de QoS y Traffic Shaping por dirección de

destine;
Soportar la creación de polfticas de QoS y Traffic Shaping par usuario y grupo;
Soportar la creación de politicas de QoS y Traffic Shaping para aplicaciones

incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
Soportar la creación de polfticas de calidad de servicio y Traffic Shaping por

puerto;

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

QoS debe permitir la definición de trafico con ancho de banda garantizado;

QoS debe permitir la definición de trafico
con maxima ancho de banda;
QoS debe permitir la definición de cola de prioridad;
Soportar la priorización de protocolo en tiempo real de voz (VoIP) como
H.323, SIP, SCCP, MGCP y aplicaciones coma Skype;
Soportar marcación de paquetes DiffServ, incluso par aplicación;
Soportar la modificación de los valores de DSCP para Diffserv;
Soportar priorización de trafico utilizando información de Tipo de Servicio

(Type of Service)
Proporcionar estadisticas en tiempo real para clases de QoS y Traffic Sha pig;

Debe soportar QoS (traffic-shaping) en la interfaz agregada o redundantes;

•
FILTRO DE DATOS
Permite la creación de filtros para archivos y dates predefinidos;
Los archivos deben ser identificados por tamafio y tipo;
Permitir identificar y opcionalmente prevenir la transferencia de varios tipos

de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTIP, FTP,

SMTP, etc.);
Soportar la identificación de archivos comprimidos o la aplicación de politicas

sabre el contenido de este tipo de archivos;
Soportar la identificación de archives cifrados y la aplicación de polltcas
sabre el contenido de este tipo de archivos;
Permitir identificar y opcionalmente prevenir la transferencia de información

sensible, incluyendo, pero no limitado a, numero de tarjeta de credlto,
permitiendo la creación de nuevos tipos de datos a traves de expresiones

regulares;
•
GEO LOCALIZACION
Soportar la creación de poHticas por geo-localizaci6n, permitiendo bloquear

el trafico de cierto Pais/Parses;
Debe permitir la visualizacionde los pafses de origen y destino en los
registros de acceso;
Debe permitir la creación de zonas geograficas por medio de la interfaz
grafica de usuario y la creación de politicas usando las mismas.
•
VPN
Soporte VPN de sitio a sitio y cliente a sitio;
Soportar VPN IP Sec;
Soportar VPN SSL;
la VPN IPSec debe ser compatible con 3DES;
La VPN IPSec debe ser compatible con la autenticaciónMOS y SHA-1;
la VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2,
Grupo 5 y el Grupo 14;
La VPN IPSec debe ser compatible con Internet Key Exchange (IKEvl y v2);

la VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced
Encryption Standard);
La VPN IPSec debe ser compatible con la autenticacióna traves de
certificados IKE PKI
Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check

Point, Juniper, Palo Alto Networks, Forti net, SonicWall;
Soportar VPN para 1Pv4 e 1Pv6, asi como el trafico 1Pv4 dentro de tuneles

IPv6 IPSec
Debe permitir activar y desactivar tuneles IPSec VPN desde la interfaz grafica

de la solución, lo que facilita el proceso throubleshooting;
La VPN SSL debe soportar que el usuario pueda realizar la conexión a traves

de cliente instalado en el sistema operativo de su rnaquina o a traves de la

interfaz web;
Las caracteristicas de VPN SSL se deben cumplir con o sin el uso de agentes;

Debe permitir que todo el trafico de los usuarios VPN remotos fluya hacia el

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

tunel VPN, previniendo la comunicaci6n directa con dispositivos locales
coma un proxy;
Asignaci6n de DNS en la VPN de cliente remoto;
Debe permitir la creación de polfticas de control de aplicaciones, IPS,
antivirus, filtrado da URL y AntiSpyware para el trafico de clientes remotos

conectados a la VPN SSL;
Suportar autenticaciónvia AD/LDAP, Secure id, certificado y base de usuarios

local;
Suportar lectura y revision de CRL (lista de revocaci6n de certificados);
Permitir la aplicación de poHticas de seguridad y visibilidad para las
aplicaciones que circulan dentro de tuneles SSL;
Debe permitir que la conexión a la VPN se establece de la siguiente manera:

Antes de que el usuario se autentique en su estaci6n
Deberfa permitir la conexión a la VPN se establece de la siguiente manera:

Oespues de la autenticaciónde usuario en la estaci6n;
Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo

demanda de los usuarios;
Debera mantener una conexión segura con el portal durante la sesi6n;
El agente de VPN SSL o IPSEC cliente a sitio debe ser compatible con al
menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y

64 bits) y Mac OS X (vl0.10 o superior);
•
WIRELESS CONTROLLER
Debera gestionar de manera centralizada puntos de acceso del mismo
fabricante de la solución ofertada
Soportar servicio del servidor DHCP por SSID para proporcionar direcciones

IP a los clientes malarnbrtcos
Soporte 1Pv4 e 1Pv6 por SSID
Permitir elegir si el trafico de cada 5510 se enviara a la controladora o
directamente por la interfaz de punto de acceso en una VLAN dada
Permitir definir que redes se acceden a traves de la controladora y que redes

seran accedidas directamente por la interfaz del Access Point
Soportar monitoreo y supresi6n de puntos de acceso indebidos
Proporcionar autenticaciónа la red inalambrica a traves de bases de datos

externas, tales como LDAP o RADIUS
Permitir autenticar a los usuarios de la red inalambrica de manera
transparente en dominios Windows
Permitir la visualizaciónde los dispositivos inalambricos conectados por
usuario
Permitir la visualizaciónde los dispositivos inalambricos conectados por IP

Permitir la visualizaciónde los dispositivos inalarnbricos conectados por tipo

de autenticación
Permitir la visualizaciónde los dispositivos inalambricos conectados por
canal
Permitir la visualizaciónde los dispositivos inalarnbricos conectados por
ancho de banda usado
Permitir la visualizaciónde los dispositivos inalambricos conectados por
potencia de la sefial
Permitir la visualizaciónde los dispositivos inalarnbricos conectados por
tiempo de asociación
Debe soportar Fast Roaming en autenticacióncon portal cautivo
Debe soportar configuración de portal cautivo por SSID
Permitir bloqueo de trafico entre los clientes conectados a un SSID y AP
espedfico
Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID,
usando un algoritmo AES y lo TKIP.
Debe ser compatible con el protocolo 802.lx RADIUS
La controladora tnalarnbrica debera permitir configurar los para metros de

radio como banda y canal
La controladora debera permitir metodos de descubrimiento de puntos de

acceso de manera automatica
La controladora debera permitir metcdos de descubrimiento de puntos de

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

acceso por IP estatica
La controladora debera permitir metodos de descubrimiento de puntos de

acceso por DHCP
La controladora debera permitir metodos de descubrimiento de puntos de

acceso por dns
La controladora debera permitir metodos de descubrimiento de puntos de

acceso por broadcast
La controladora debera permitir metodos de descubrimiento de puntos de

acceso par multicast
La controladora Inalambrica debera suministrar una lista de Puntos de
Acceso autorizados y puntos de acceso indebidos (Rogue)
La controladora debera contar con proteccion contra ataques ARP Poisoning

en el controlador Inalambrico
La controladora debera contar con mecanismos de protecciónde tramas de

administraci6n de acuerdo a las especificaciones de la alianza Wi-Fi y
estandar 802.llac
La controladora inalambrtca debera tener de manera integrada sistema de

deteccion de intrusion inalambrica contra ataques tipo ASLEAP
La controladora inalambrica debera tener de manera integrada sistema de

deteccion de intrusion Inalambrica contra ataques tipo Association Frame

Flooding
La controladora inalarnbrica debera tener de manera integrada sistema de

deteccion de intrusion inalambrica contra ataques tipo Authentication Frame

Flooding
La controladora tnalarnbrtca debera tener de manera integrada sistema de

detección de intrusion inalambrica contra ataques tipo Broadcasting De-
authentication
la controladora inalambrica debera tener de manera integrada sistema de

detección de intrusion Inalambrica contra ataques tipo EAPOL Packet
flooding
La controladora Inalambrica debera tener de manera integrada sistema de

deteccion de intrusion inalambrica contra ataques tipo Invalid MAC OUI
La controladora Inatarnbrtca debera tener de manera integrada sistema de

deteccion de intrusion Inalambrtca contra ataques tipo Long Duration Attack

La controladora Inalambrica debera tener de manera integrada sistema de

deteccion de intrusion inalambrica contra ataques tipo Null SSID probe
response
La controladora inalambrtca debera tener de manera integrada sistema de

deteccion de intrusion tnalambrica contra ataques tipo Spoofed De-
authentication
La controladora Inalambrica debera tener de manera integrada sistema de

deteccion de intrusion inalambrtca contra ataques tipo Weak WEP IV
Detection
La controladora tnalambrica debera tener de manera integrada sistema de

detección de intrusion Inalambrica contra ataques tipo Wireless Bridge
Implementar canales de auto-aprovisionamiento de los puntos de acceso con

el fin de minimizar la interferencia entre ellas
Permitir seleccionar el dia y hara en que se producira la optimizaci6n de
aprovisionamiento automatics de canales en los puntos de acceso
La controladora Inalambrica debe permitir agendar horarios para determinar

en que memento la red inalarnbrica (SSID) se encuentra disponible
La controladora inalarnbrica debe ofrecer funcionalidad de Firewall integrado

UTM basado en la identidad del usuario
Permitir configurar el nurnero rnaxirno de clientes que pueden ser permitidos

par SSID
Permitir configurar el numero rnaxirno de clientes que pueden ser permitidos

SEMS
SECRETARÍA ADMINISTRATIVA

4
[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

par punto de acceso
Permitir configurar el numero maxi mo de clientes que pueden ser permitidos

par Radio
La controladora debe permitir crear, administrar y autorizar las redes inalarnbrlcas mesh
Ofrecer un mecanismo de creacion automatica y/o manual de usuarios visitantes y contrasefias, que puedan ser enviados par correo electronlco o

SMS a los usuarios, con ajuste de tiempo de expiraci6n de la contrasef\a
La comunicacion entre la controladora y el punto de acceso Inalambrlco pueda ser realizada de forma cifrada utilizando protocolo DTLS
Debe tener un mecanismo de ajuste autornatlco de potencia de la serial con

el fin de reducir la interferencia entre canales entre dos puntos de acceso

administrados
Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso
Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso
Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualizaci6n a traves de la interfaz grafica:

Permitir que sean deshabilitados clientes inalarnbricos que tengan baja tasa

de transmisi6n
Permitir ignorar a los clientes inalambrlcos que tienen serial debtl, estableciendo un umbral de serial a partir de la cual los clientes son ignorados
la controladora debe permitir configurar el valor de Short Guard Interval para 802.lln y 802.llac en 5 GHz
Debe permitir seleccionar individualmente para cada punto de acceso los

SSID que van a ser propagados
Debe permitir asociación dinarntcas
de VIANs a los usuarios autenticados en
un SSID especifico mediante protocolo RADIUS
Debe permitir asociación dinamlca de VIANs a los usuarios autenticados en

un SSID especifico mediante vlan pooling
Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalambnco
la controladora inalarnbrica debe permitir identificar los clientes WIFI que

presenten algun riesgo basado en aplicaciones
la controladora inalambrica debe permitir identificar los clientes WiFi que

presenten algun riesgo basado en dirección de destine
la controladora inalambrica debe permitir identificar los clientes WiFi que

presenten algun riesgo basado en amenaza
la controladora inalarnbrica debe permitir identificar los clientes WiFi que

presenten algun riesgo basado en sesiones
la controladora Inalambrica debe soportar una licencia que permita al menos

10000 firmas de aplicaciones para reconocimiento de trafico
El controlador inalambrico debe tener interface de administraci6n integrado

en el mismo equipo
El controlador inalambnco debe soportar la funcionalidad de Fast-roaming

para enlaces mesh entre el node secundario y nodes principales
la controladora Inalambrica debera soportar aceleraci6n de trafico del protocolo CAPWAP a traves de un procesador de red de prop6sito espedfico

la controladora inalambrica debera soportar aceleraci6n de tunnel de trafico

de puente tnalambnco a traves de un procesador de red de prop6sito espedfico
la controladora inalarnbrica debe soportar protocolo LLDP
Debe permitir tecnica de detección de APs intrusos On-wire a traves de dirección MAC exacta
Debe permitir tecnica de detección de APs intrusos On-wire a traves de dirección MAC Adyacente
Debe permitir la visualizacionde los usuarios conectados en forma de

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa:	INITEL S.A. DE C.V.
R.F.C.:	[redacted] 1
Dirección:	[redacted] 3
Teléfono:	[redacted] 5
web:	[redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD		DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
			topologia 16gica de red representando la cantidad de datos transmitidos y recibidos la controladora inalarnbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado La controladora malambrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas la controladora inalambrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada Debera soportar la conversion de Multicast a Unicast para mejorar el rendimiento del tiempo de aire		
2	28	FG-400D-BDL-900-36 **Mca. FORTINET**	SOLUCIONUTM/NGFW TIPO 1 (1 UNIDAD) Throughput de por lo menos 16 Gbps con la funcionalidad de firewall habilitada para trafico 1Pv4 y 1Pv6, independiente del tamafio del paquete Soporte a por lo menos 4M conexiones simultaneas Soporte a por lo menos 200K nuevas conexiones por segundo Throughput de al menos 14 Gbps de VPN IPSec Estar licenciado para, o soportar sin necesidad de licencia, 2K tuneles de VPN IPSec site-to-site simultaneos Estar licenciado para, o soportar sin necesidad de licencia, 50K tuneles de clientes VPN IPSec simultaneos Throughput de al menos 350 Mbps de VPN SSL Soportar al menos 500 clientes de VPN SSL simultaneos Soportar al menos 2800 Mbps de throughput de IPS Soportar al menos 1900 Mbps de throughput de inspecci6n SSL Throughput de al menos 1500 Mbps con las siguientes funcionalidades habilitadas simuttaneamente para todas las firmas que la solución de seguridad tenga debidamente activadas y operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado multiples oumeros de desempefio para cualquier de las funcionalidades, solamente el de valor mas pequefio sera aceptado. Permitir gestionar al menos 256 Access Points Tener al menos 8 interfaces 1 Gbps RJ45, 8 interfaces de 1 Gbps SFP, 2 interfaces Gbps para gestion Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales 16 logicos (Contextos) par appliance Soporte a por lo menos 10 sistemas virtuales logicos (Contextos) par appliance Debe de incluir un token fisico para autenticaciónde doble factor para la gestión del appliance o para el acceso VPN que debe ser de la misma marca propuesta Debe de brindar soporte 36 meses del tipo 8x5, reemplazo siguiente dia habil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus, Botnet IP/Domain, AntiSpam y Filtrado Web . REQUISITOS MINIMOS DE FUNCIONALIDAD Caracteristicas Generales La solución debe consistir en una plataforma de protecciónde Red, basada en un dispositivo con funcionalidades de Firewall de Próxima generación (NGFW), asi coma consola de gestión y monitoreo. ;	$ 195,464.35	$ 5,473,001.80

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Porfuncionalidades de NGFW se entiende: aplicaciones de reconocimiento, prevenci6n de amenazas, identificación de usuarios y control granular de permisos; Las funcionalidades de protecciónde red que conforman la plataforma de seguridad, puede ejecutarse en multiples dispositivos siempre que cum plan todos los requisites de esta especificaci6n; La plataforma debe estar optimizada para aplicaciones de analisis de contenido en la capa 7; Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación; La gestión del equipo debe ser compatible con acceso a traves de SSH, consola, web (HTIPS) y API abierta; La gestión del equipos debe ser compatible a traves de la interfaz de administraci6n Web en el mismo dispositivo de protecciónde la red Los dispositivos de protecciónde red deben soportar 4094 VLANs Tags 802.lq; Los dispositivos de protecciónde red deben soportar agregaci6n de enlaces 802.3ad y LACP; Los dispositivos de protecciónde red deben soportar Policy based routing y policy based forwarding; Los dispositivos de protecciónde red deben soportar encaminamiento de multicast (PIM-SM y PIM-OM); Los dispositivos de protecciónde red deben soportar DHCP Relay; Los dispositivos de protecciónde red deben soportar DHCP Server; Los dispositivos de protecciónde red deben soportar sFlow Los dispositivos de protecciónde red deben soportar Jumbo Frames; Los dispositivos de protecciónde red deben soportar sub-interfaces Ethernet 16gicas Debe ser compatible con NAT dinamica (varios-a-1); Debe ser compatible con NAT dinarnica (muchos-a-muchos); Debe soportar NAT estatica (l-a-1); Debe admitir NAT estatica (muchos-a-muchos); Debe ser compatible con NAT estatico bidireccional 1-a-1; Debe ser compatible con la traducci6n de puertos (PAT); Debe ser compatible con NAT Origen; Debe ser compatible con NAT de destine; Debe soportar NAT de origen y NAT de destino de forma simultanea: Debe soportarTraducci6n de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento aslrnetrlco: Debe ser compatible con NAT64 y NAT46; Debe implementar el protocolo ECMP; Debe soportar el balanceo de en lace hash por IP de origen; Debe soportar el balanceo de en lace hash por IP de origen y destine; Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de traftco que fluira a traves de cada uno de los en laces.		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Debe ser compatible con el balanceo en al menos tres en laces; Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran nurnero de sesiones, conexiones por segundo, cantidad de tuneles establecidos en la VPN, CPU, memoria, estado del cluster, ataques y estadfsticas de uso de las interfaces de red Enviar logs a sistemas de gestión externos simultaneamente: Debe tener la opción de enviar logs a los sistemas de control externo a traves de TCP y SSL; Debe soporta protecciónc ontra la suplantaci6n de identidad (anti-spoofing); Implementar la optimizaci6n del trafico entre dos dispositivos; Para 1Pv4, soportar enrutamiento estatico y dinarnico (RIPv2, OSPFv2 y BGP); Para 1Pv6, soportar enrutamiento estatico y dlnarnico (OSPFv3); Soportar OSPF graceful restart; Los dispositivos de protecciónd eben tener la capacidad de operar simultaneamente en una unica instancia de servidor de seguridad, mediante el uso de sus interfaces ffsicas en los siguientes modos: modo sniffer (monitoreo y anallsis de trafico de red), capa 2 (L2) y capa 3 (L3); Debe ser compatible con el modo Sniffer para la inspección a traves del puerto espe]o del trafico de datos de la red; Debe soportar modo capa - 2 (L2) para la inspección de datos en linea y la visibilidad del trafico: Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en lfnea de trafico: Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces fisicas; Soportar la configuración de alta disponibilidad active I pasivo y activo I active: En modo transparente; Soportar la configuración de alta disponibilidad activo I pasivo y activo I activo: En capa 3; Soportar configuración de alta disponibilidad active I pasivo y activo I activo: En la capa 3 y con al menos 3 dispositivos en el cluster; La configuración de alta disponibilidad debe sincronizar: Sesiones; La configuración de alta disponibilidad debe sincronizar: configuración , incluyendo, pero no limitados poHticas de Firewalls, NAT, QoS y objetos de la red; La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN; La configuración de alta disponibilidad debe sincronizar: Tablas FIB; En modo HA (Modo de alta disponibilidad) debe permitir la supervision de fallos de enlace;		

SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 2
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Debe ser compatible con el balanceo en al menos tres en laces; Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran nurnero de sesiones, conexiones por segundo, cantidad de tuneles establecidos en la VPN, CPU, memoria, estado del cluster, ataques y estadfsticas de uso de las interfaces de red Enviar logs a sistemas de gestión externos simultaneamente: Debe tener la opción de enviar logs a los sistemas de control externo a traves de TCP y SSL; Debe soporta protecciónconcontra la suplantaci6n de identidad (anti-spoofing); Implementar la optimizaci6n del trafico entre dos dispositivos; Para 1Pv4, soportar enrutamiento estatico y dinarnico (RIPv2, OSPFv2 y BGP); Para 1Pv6, soportar enrutamiento estatico y dinarnico (OSPFv3); Soportar OSPF graceful restart; Los dispositivos de protecciódeben tener la capacidad de operar simultaneamente en una unica instancia de servidor de seguridad, mediante el uso de sus interfaces ffsicas en los siguientes modos: modo sniffer (monitoreo y analisis de trafico de red), capa 2 (L2) y capa 3 (L3); Debe ser compatible con el modo Sniffer para la inspección a traves del puerto espe]o del trafico de datos de la red; Debe soportar modo capa - 2 (L2) para la inspección de datos en linea y la visibilidad del trafico: Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en lfnea de trafico: Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces fisicas; Soportar la configuración de alta disponibilidad active I pasivo y activo I active: En modo transparente; Soportar la configuración de alta disponibilidad activo I pasivo y activo I activo: En capa 3; Soportar configuración de alta disponibilidad active I pasivo y activo I activo: En la capa 3 y con al menos 3 dispositivos en el cluster; La configuración de alta disponibilidad debe sincronizar: Sesiones; La configuración de alta disponibilidad debe sincronizar: configuración , incluyendo, pero no limitados poHticas de Firewalls, NAT, QoS y objetos de la red; La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN; La configuración de alta disponibilidad debe sincronizar: Tablas FIB; En modo HA (Modo de alta disponibilidad) debe permitir la supervision de fallos de enlace;		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

Empresa:	INITEL S.A. DE C.V. 1
R.F.C.:	[redacted]
Dirección:	[redacted] 3
Teléfono:	[redacted] 5
web:	[redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Debe soportar la creación de sistemas virtuales en el mismo equipo; Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribuci6n de la carga entre los diferentes contextos; Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes equipos; La solución de gestión debe ser compatible con el acceso a traves de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportaci6n de configuración de sistemas virtuales (contextos) por ambos tipos de acceso; Debe aportar el control, la inspección y el descifrado de SSL para el trafico entrante (inbound) y la salida (outbound), y debe ser compatible con el control de certificados de forma individual dentro de cada sistema virtual, es decir, el aislamiento de la adición, eliminación y uso de los certificados directamente en cada sistema virtual (contextos); • CONTROL POR POLITICA DE FIREWALL Debe soportar controles de zona de seguridad Debe contar con politicas de control por puerto y protocolo Contar con politicas por aplicación, grupos estatrcos de aplicaciones, grupos dinamtcos de aplicaciones (en base a las caracteristicas y comportamiento de las aplicaciones) y categorias de aplicaciones Control de politicas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad Control de politica por código de pais (por ejemplo: BR, USA., UK, RUS) Control, inspección y des encriptación de SSL por polftica para el trafico entrante y la salida Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada; Debe descifrar las conexiones de entrada y salida de trafico negociadas con TLS 1.2; Control de inspección y descifrado SSH por politica; Debe permitir el bloqueo de archivos por su extension y permitir la identificación de archivo correcto por su tipo, incluso cuando se cambia el nombre de su extension; Traffic shaping QoS basado en politicas (garantia de prioridad y maxima); QoS basado en politicas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones; Soporte para objetos y reglas IPV6; Soporte objetos y reglas de multicast; Debe ser compatible con al menos tres tipos de respuesta en las politicas de firewall: 'Drop' sin la notificaci6n de bloqueo del usuario, 'Drop' con la notificaci6n de bloqueo del usuario, Drop con opción de env[o ICMP		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

inalcanzable por la maquina fuente de trafico, TCP Reset para el cliente,
RESET de TCP con el servidor o en ambos lados de la conexión;

Soportar la calendarizaci6n de politicas con el fin de activar y desactivar las
reglas en tiempos predefinidos de forma automatica:
• CONTROL DE APLICACION
Los dispositivos de protecciónde red deben tener la capacidad de reconocer
las aplicaciones, independientemente del puerto y protocolo

Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o
cerrar puertos y protocolos
Reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no
limitado a: el trafico relacionado peer-to-peer, redes sociales, acceso
remote, actualizaci6n de software, protocolos de red, VoIP, audio, video,
Proxy, mensajeria instantanea, compartici6n de archives, correo electr6nico;
Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype,
facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail,
youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp,
4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory,
kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc
over http, gotomeeting, webex, evernote, google-docs;
Debe inspeccionar la carga util (payload) del paquete de datos con el fin de
detectar las firmas de las aplicaciones conocidas por el fabricante
independiente de puerto y protocolo;
Debe detectar aplicaciones a traves del analisis del comportamiento del
trafico observado, incluyendo, pero no limitado a las aplicaciones de VoIP
que utilizan cifrado propietario y BitTorrent;
Identificar el uso de tacticas evasivas, es decir, debe tener la capacidad de
very controlar las aplicaciones y los ataques con tacticas evasivas a traves de
las comunicaciones cifradas, tales como Skype y la utilizaci6n de la red Tor
Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura
de payload para permitir la identificación de firmas de la aplicación
conocidas por el fabricante;
Debe hacer decodificación de protocolos con el fin de detectar aplicaciones
encapsuladas dentro del protocolo y validar que el trafico corresponde a la
especificaci6n del protocolo, incluyendo, pero no limitado a Yahoo Instant
Messenger utilizando HTIP. La decodificación de protocolo tambien debe
identificar las caractedsticas espedficas dentro de una aplicación,
incluyendo, pero no limitado al intercambio de ficheros dentro de Webex
Identificar el uso de tacttcas evasivas a traves de las comunicaciones cifradas;
Actualizaci6n de la base de firmas de la aplicación de forma autornatica:

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Limitar el ancho de banda (carga I descarga) utilizado por las aplicaciones traffic shaping), basado en IP de origen, usuarios y grupos; Los dispositivos de protecciónde red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalaci6n del agente en el controlador de dominio, o en estaciones de trabajo de usuario; Debe ser posible afiadir multiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas; Debe ser compatible con multiples metodos de identificación y clasificaci6n de las aplicaciones, al menos verificar firmas y protocolos de decodificación; Para mantener la seguridad de red eficiente debe ser soportar el control de las aplicaciones desconocidas y no solo en aplicaciones conocidas; Permitir la creación de forma nativa de fir mas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz grafica, sin la necesidad de la acci6n del fabricante La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posici6n en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS- SQL, IMAP, DNS, LDAP, SSL y RTSP El fabricante debe permitir solicitar la inclusion de aplicaciones en su base de dates; Debe alertar al usuario cuando sea bloqueada una aplicación; Debe permitir la diferenciación de trafico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo; Debe permitir la diferenciacion de trafico de mensajeria Instantanea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo; Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video; Debe permitir la diferenciacion de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo; Debe ser posible la creación de grupos dinamicos de aplicaciones, basado en las caracteristicas de las mismas, tales coma: Tecnologia utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc) Debe ser posible crear grupos dinarntcos de aplicaciones basados en caracteristicas de las mismas, tales como: nivel de riesgo de la aplicacion		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Debe ser posible crear grupos estaticos de aplicaciones basadas en caracterfsticas de las mismas, tales como: Categoria de Aplicacion • PREVENCION DE AMENAZAS Para proteger el entorno contra las ataques, deben tener modulo IPS, antivirus y anti-spyware integrado en el propio equipo; Debe incluir firmas de prevenci6n de intrusiones (IPS) y el bloqueo de archives maliciosos (antivirus y anti-spyware); Las caracteristicas de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no existe un contrato de garantfa del software con el fabricante; Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad; Debe implementar los siguientes tipos de acciones a las amenazas detectadas par IPS: permitir, permitir y generar registro, bloque, bloque del IP del atacante durante un tiempo y enviar tcp-reset; Las firmas deben ser capaces de ser activadas o desactivadas, o activadas solo en el modo de monitoreo; Deben ser posible crear politicas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas; Debe soportar granularidad en las politicas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes politicas par zona de seguridad, dirección de origen, dirección de destine, servicio y la combinaci6n de todos estos elementos Deber permitir el bloqueo de vulnerabilidades Debe permitir el bloqueo de exploits conocidos Debe incluir la protecciónccontra ataques de denegacion de servicio Debe tener los siguientes mecanismos de inspección IPS: Analisis de patrones de estado de las conexiones; Debe tener los siguientes mecanismos de inspeccion IPS: analisis de decodificación de protocolo; Debe tener los siguientes mecanismos de inspeccion IPS: analisis para detectar anomalfas de protocolo; Debe tener los siguientes mecanismos de inspección IPS: Analisis heuristico; Debe tener los siguientes mecanismos de inspección IPS: Desfragmentaci6n IP; Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP; Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formate incorrecto (malformed packets) Debe ser inmune y capaz de prevenir los ataques basicos, tales como inundaciones SYN, ICMP, UDP, etc; Detectar y bloquear los escaneos de puertos de origen;		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Bloquear ataques realizados por gusanos (worms) conocidos; Contar con firmas especfficas para la rnitlgacion de ataques DoS y DDoS; Contar con firm as para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow); Debe poder crear firmas personalizadas en la interfaz grafica del producto; Debe permitir utilizar operadores de negaci6n en la creacicn de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración ; Permitir bloqueo de virus y software espia en por lo menos los siguientes protocolos: HTIP, FTP, SMB, SMTP y POP3; Soportar el bloqueo de archives por tipo; Identificar y bloquear la comunicaci6n con redes de bots; Registrar en la consola de supervision la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la apitcacion, el usuario, el origen y destine de las comunicaciones, adernas de las medidas adoptadas por el dispositivo; Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación; Debe permitir la captura de paquetes por tipo de firma IPS para definir el nurnero de paquetes capturados o permitir la captura del paquete que dio lugar a la descripci6n, asf como su contexto, facilitando el analisis forense y la identificación de falsos positives Debe tener la funci6n de protecciónа traves de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos; Los eventos deben identificar el pais que origino la amenaza; Debe incluir proteccióncontra virus en contenido HTML y Java script, software espia (spyware) y gusanos (worms) Tener proteccióncontra descargas involuntarias mediante archives ejecutables maliciosos y HTIP Debe permitir la configuración de diferentes politicas de control de amenazas y ataques basados en politicas de firewall considerando usuarios, grupos de usuarios, origen, destine, zonas de seguridad, etc., es decir, cada polftica de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destine, zonas de seguridad • FILTRADO DE URL Debe permitir especificar la politica por tiempo, es decir, la definición de reglas para un tiempo o periodo determinado (dia, mes, afio, dfa de la semana y hara); Debe ser posible crear polfticas para usuarios, IPs, redes, o zonas de seguridad Debe tener la capacidad de crear politicas basadas en la visibilidad y el		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initelo

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

control de quien esta utilizando las URL esto mediante la integración con las
servicios de directorio Active Directory, y la base de datos local;

Debe tener la capacidad de crear politicas basadas en la visibilidad y el
control de quien esta usando las URL que mediante la integración con las
servicios de directorio Active Directory, y la base de dates local, en modo de
proxy transparente y explicito;
Debe soportar la capacidad de crear politicas basadas en control por URL y
categorfa de URL
Debe tener la base de datos de URLs en cache en el equipo o en la nube de!
fabricante, evitando retrasos de comunicaci6n I validaci6n de direcciones
URL;
Tener por lo menos 60 categorias de URL;
Debe tener la funcionalidad de exclusion de URLs por categoria

Permitir pagina de bloqueo personalizada;
Permitir el bloqueo y continuaci6n (que permite al usuario acceder a un sitio
bloqueado potencialmente Inforrnandole en la pantalla de bloqueo y
permitiendo el uso de un bot6n Continuar para que el usuario pueda seguir
teniendo acceso al sitio);
•
IDENTIFICACION DE USUARIOS
Se debe incluir la capacidad de crear politicas basadas en la visibilidad y el
control de quien esta usando dichas aplicaciones a traves de la integración
con los servicios de directorio, a traves de la autenticaciónLDAP, Active
Directory, E-directorio y base de datos local;
Debe tener integración con Microsoft Active Directory para identificar a los
usuarios y grupos, permitiendo granularidad a las polfticas / control basados
en usuarios y grupos de usuarios;
Debe tener integración y soporte para Microsoft Active Directory para los
siguientes sistemas operatives: Windows Server 2003 R2, Windows Server
2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server
2012 R2;
Debe tener integración con Microsoft Active Directory para identificar a los
usuarios y grupos que permita tener granularidad en las politicas/control
basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta
funcionalidad no debe tener lf mites licenciados de usuarios o cualquier
restricci6n de uso como, pero no limitado a, utilizaci6n de sistemas virtuales,
segmentos de red, etc;
Debe tener integración con RADIUS para identificar a los usuarios y grupos
que permiten las politicas de granularidad / control basados en usuarios y
grupos de usuarios;
Debe tener la integración LDAP para la identificación de los usuarios y grupos
que permiten granularidad en la politicas/control basados en usuarios y

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initelo

Empresa: INITEL S.A. DE C.V. 1
R.F.C.: [redacted]
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		grupos de usuarios; Debe permitir el control sin necesidad de instalaci6n de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegaci6n, entre a un portal de autentificaci6n residente en el equipo de seguridad (portal cautivo); Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios; Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos del LDAP I AD Permitir la integración con tokens para la autenticaciónde usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma. Proporcionar al menos un token de forma nativa, lo que permite la autenticaciónde dos factores • QOS TRAFFIC SHAPING Con el fin de controlar el trafico y aplicaciones cuyo con sumo puede ser excesivo (como YouTube, Ustream, etc.) y tienen un alto consume de ancho de banda, se requiere de la solución que, adernas de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda maxima cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio coma de video streaming; Soportar la creación de politicas de QoS y Traffic Shaping par dirección de origen; Soportar la creación de politicas de QoS y Traffic Shaping por dirección de destine; Soportar la creación de polfticas de QoS y Traffic Shaping par usuario y grupo; Soportar la creación de politicas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube; Soportar la creación de polfticas de calidad de servicio y Traffic Shaping por puerto; QoS debe permitir la definición de trafico con ancho de banda garantizado; QoS debe permitir la definición de trafico con maxima ancho de banda; QoS debe permitir la definición de cola de prioridad; Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones coma Skype; Soportar marcación de paquetes DiffServ, incluso par aplicación; Soportar la modificación de los valores de DSCP para Diffserv; Soportar priorización de trafico utilizando información de Tipo de Servicio (Type of Service) Proporcionar estadisticas en tiempo real para clases de QoS y Traffic Sha pig;		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

Debe soportar QoS (traffic-shaping) en la interfaz agregada o redundantes;
•
FILTRO DE DATOS
Permite la creación de filtros para archivos y dates predefinidos;

Los archivos deben ser identificados por tamafio y tipo;
Permitir identificar y opcionalmente prevenir la transferencia de varios tipos
de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTIP, FTP,
SMTP, etc.);
Soportar la identificación de archivos comprimidos o la aplicación de politicas
sobre el contenido de este tipo de archivos;
Soportar la identificación de archives cifrados y la aplicación de polittcas
sobre el contenido de este tipo de archivos;
Permitir identificar y opcionalmente prevenir la transferencia de información
sensible, incluyendo, pero no limitado a, nurnero de tarjeta de credlto,
permitiendo la creación de nuevos tipos de datos a traves de expresiones
regulares;
•
GEO LOCALIZACION
Soportar la creación de poHticas por geo-localizaci6n, permitiendo bloquear
el trafico de cierto Pais/Parses;
Debe permitir la visualizaciónde los pafses de origen y destino en los
registros de acceso;
Debe permitir la creación de zonas geograficas por medio de la interfaz
grafica de usuario y la creación de politicas usando las mismas.

•
VPN
Soporte VPN de sitio a sitio y cliente a sitio;
Soportar VPN IP Sec;
Soportar VPN SSL;
la VPN IPSec debe ser compatible con 3DES;
La VPN IPSec debe ser compatible con la autenticaciónMOS y SHA-1;
la VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2,
Grupo 5 y el Grupo 14;
La VPN IPSec debe ser compatible con Internet Key Exchange (IKEvl y v2);
la VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced
Encryption Standard);
La VPN IPSec debe ser compatible con la autenticacióna traves de
certificados IKE PKI
Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check
Point, Juniper, Palo Alto Networks, Forti net, SonicWall;
Soportar VPN para 1Pv4 e 1Pv6, asl como el trafico 1Pv4 dentro de tuneles
IPv6 IPSec
Debe permitir activar y desactivar tuneles IPSec VPN desde la interfaz grafica
de la solución, lo que facilita el proceso troubleshooting;
La VPN SSL debe soportar que el usuario pueda realizar la conexión a traves
de cliente instalado en el sistema operativo de su rnaquina o a traves de la
interfaz web;

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V. 1
R.F.C.: [redacted]
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Las caracteristicas de VPN SSL se deben cumplir con o sin el uso de agentes; Debe permitir que todo el trafico de los usuarios VPN remotos fluya hacia el tunel VPN, previniendo la comunicaci6n directa con dispositivos locales coma un proxy; Asignaci6n de DNS en la VPN de cliente remoto; Debe permitir la creación de polfticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el trafico de clientes remotos conectados a la VPN SSL; Suportar autenticaciónvia AD/LDAP, Secure id, certificado y base de usuarios local; Suportar lectura y revision de CRL (lista de revocaci6n de certificados); Permitir la aplicación de poHticas de seguridad y visibilidad para las aplicaciones que circulan dentro de tuneles SSL; Debe permitir que la conexión a la VPN se establece de la siguiente manera: Antes de que el usuario se autentique en su estaci6n Deberfa permitir la conexión a la VPN se establece de la siguiente manera: Oespues de la autenticaciónde usuario en la estaci6n; Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo demanda de los usuarios; Debera mantener una conexión segura con el portal durante la sesi6n; El agente de VPN SSL o IPSEC cliente a sitio debe ser compatible con al menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (vl0.10 o superior); • WIRELESS CONTROLLER Debera gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada Soportar servicio del servidor DHCP por SSID para proporcionar direcciones IP a los clientes malarnbrtcos Soporte 1Pv4 e 1Pv6 por SSID Permitir elegir si el trafico de cada 5510 se enviara a la controladora o directamente por la interfaz de punto de acceso en una VLAN dada Permitir definir que redes se acceden a traves de la controladora y que redes seran accedidas directamente por la interfaz del Access Point Soportar monitoreo y supresi6n de puntos de acceso indebidos Proporcionar autenticacióna la red inalambrica a traves de bases de datos externas, tales como LDAP o RADIUS Permitir autenticar a los usuarios de la red inalarnbrica de manera transparente en dominios Windows Permitir la visualizaciónde los dispositivos inalambricos conectados por usuario Permitir la visualizaciónde los dispositivos inalambricos conectados por IP Permitir la visualizaciónde los dispositivos inalarnbricos conectados por tipo de autenticación		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initelo

Empresa: INITEL S.A. DE C.V. 1
R.F.C.: [redacted]
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Permitir la visualizacióndelos dispositivos Inalambricos conectados por canal Permitir la visualizacióndelos dispositivos inalarnbricos conectados por ancho de banda usado Permitir la visualizacióndelos dispositivos Inalambricos conectados por potencia de la sefial Permitir la visualizacióndelos dispositivos inalarnbricos conectados por tiempo de asociación Debe soportar Fast Roaming en autenticacióncon portal cautivo Debe soportar configuración de portal cautivo por SSID Permitir bloqueo de trafico entre los clientes conectados a un SSID y AP espedfico Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y lo TKIP. Debe ser compatible con el protocolo 802.lx RADIUS La controladora tnalarnbrica debera permitir configurar los para metros de radio como banda y canal La controladora debera permitir rnetodos de descubrimiento de puntos de acceso de manera automatica La controladora debera permitir rnetcdos de descubrimiento de puntos de acceso por IP estatica La controladora debera permitir rnetodos de descubrimiento de puntos de acceso por DHCP La controladora debera permitir metodos de descubrimiento de puntos de acceso por dns La controladora debera permitir metodos de descubrimiento de puntos de acceso por broadcast La controladora debera permitir metodos de descubrimiento de puntos de acceso par multicast La controladora Inalambrica debera suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue) La controladora debera contar con proteccion contra ataques ARP Poisoning en el controlador Inalarnbrico La controladora debera contar con mecanismos de protecciónde tramas de administraci6n de acuerdo a las especificaciones de la alianza Wi-Fi y estandar 802.llac La controladora inalambrtca debera tener de manera integrada sistema de deteccion de intrusion inalarnbrica contra ataques tipo ASLEAP La controladora inalambrica debera tener de manera integrada sistema de deteccion de intrusion Inalarnbrica contra ataques tipo Association Frame Flooding La controladora inalarnbrica debera tener de manera integrada sistema de deteccion de intrusion inalambrica contra ataques tipo Authentication Frame Flooding La controladora tnalarnbrtca debera tener de manera integrada sistema de		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

inite

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		detección de intrusion inalarnbrica contra ataques tipo Broadcasting De- authentication la controladora inalambrica debera tener de manera integrada sistema de detección de intrusion inalarnbrica contra ataques tipo EAPOL Packet flooding La controladora inalambrica debera tener de manera integrada sistema de deteccion de intrusion inalarnbrica contra ataques tipo Invalid MAC OUI La controladora inatarnbrtca debera tener de manera integrada sistema de deteccion de intrusion inalambrtca contra ataques tipo Long Duration Attack La controladora inalambrica debera tener de manera integrada sistema de deteccion de intrusion inalarnbrica contra ataques tipo Null SSID probe response La controladora inalambrtca debera tener de manera integrada sistema de deteccion de intrusion tnalambrica contra ataques tipo Spoofed De- authentication La controladora inalambrica debera tener de manera integrada sistema de deteccion de intrusion inalarnbrtca contra ataques tipo Weak WEP IV Detection La controladora tnalambrica debera tener de manera integrada sistema de detección de intrusion inalarnbrica contra ataques tipo Wireless Bridge Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas Permitir seleccionar el dia y hara en que se producira la optimizaci6n de aprovisionamiento automatics de canales en los puntos de acceso la controladora inalambrica debe permitir agendar horarios para determinar en que memento la red inalarnbrica {SSID) se encuentra disponible La controladora inalarnbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario Permitir configurar el nurnero rnaxirno de clientes que pueden ser permitidos par SSID Permitir configurar el numero rnaxirno de clientes que pueden ser permitidos par punto de acceso Permitir configurar el numero maxi mo de clientes que pueden ser permitidos par Radio La controladora debe permitir crear, administrar y autorizar las redes inalarnbricas mesh Ofrecer un mecanismo de creacion autornatica y/o manual de usuarios visitantes y contrasefias, que puedan ser enviados par correo electronico o SMS a los usuarios, con ajuste de tiempo de expiraci6n de la contrasef\a La comunicacion entre la controladora y el punto de acceso inalarnbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

inite

Empresa: INITEL S.A. DE C.V. 1
R.F.C.: [redacted]
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Debe tener un mecanismo de ajuste automatico de potencia de la serial con el fin de reducir la interferencia entre canales entre dos puntos de acceso administrados Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualizaci6n a traves de la interfaz grafica: Permitir que sean deshabilitados clientes inalarnbricos que tengan baja tasa de transmisi6n Permitir ignorar a los clientes inalambricos que tienen serial debti, estableciendo un umbral de serial a partir de la cual los clientes son ignorados la controladora debe permitir configurar el valor de Short Guard Interval para 802.lln y 802.llac en 5 GHz Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados Debe permitir asociación dinarntcas de VIANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS Debe permitir asociación dinarnica de VIANs a los usuarios autenticados en un SSID especifico mediante vlan pooling Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalambnco la controladora inalarnbrica debe permitir identificar los clientes WiFi que presenten algun riesgo basado en aplicaciones la controladora inalambrica debe permitir identificar los clientes WiFi que presenten algun riesgo basado en dirección de destine la controladora inalambrica debe permitir identificar los clientes WiFi que presenten algun riesgo basado en amenaza la controladora inalarnbrica debe permitir identificar los clientes WiFi que presenten algun riesgo basado en sesiones la controladora Inalambrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de trafico El controlador inalambrico debe tener interface de administraci6n integrado en el mismo equipo El controlador inalambnco debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el node secundario y nodes principales la controladora Inalambrica debera soportar aceleraci6n de trafico de! protocolo CAPWAP a traves de un procesador de red de prop6sito espedfico la controladora inalambrica debera soportar aceleraci6n de tunnel de trafico de puente tnalambnco a traves de un procesador de red de prop6sito espedfico la controladora inalarnbrica debe soportar protocolo LLDP		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Debe permitir tecnica de detección de APs intrusos On-wire a traves de dirección MAC exacta Debe permitir tecnica de detección de APs intrusos On-wire a traves de dirección MAC Adyacente Debe permitir la visualizaciónde los usuarios conectados en forma de topologia 16gica de red representando la cantidad de dates transmitidos y recibidos la controladora inalarnbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado La controladora malarnbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas la controladora inalambrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada Debera soportar la conversion de Multicast a Unicast para mejorar el rendimiento del tiempo de aire		

SUBTOTAL	**$**	**10,046,867.59**
IVA	**$**	**1,607,498.81**
TOTAL	$	11,654,366.40

Condiciones Comerciales — **Total con Letra: Once Millones Seiscientos Cincuenta y Cuatro Mil Trescientos Sesenta y Seis Pesos 40/100 M.N**

Moneda: Precios expresados en Moneda Nacional.
Tiempo de Entrega: 4 a 6 semanas despues de confirmado el pedido
Vigencia: 30 días naturales apartir de la fecha de apertura del sobre
Forma de pago: Credito 15 días naturales
Garantía: 3 años
Notas: Los precios ofertados consideran el costo de flete para la entrega a cada dependencia beneficiada.

[redacted] 4

Teobaldo Leal Arriaga 7

[redacted] 6

[redacted] 5

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

PANORAMA

UNIVERSIDAD DE GUADALAJARA

Red Universitaria e Institución Benemérita de Jalisco

CONVOCATORIA NACIONAL

La Universidad de Guadalajara, a través del Sistema de Educación Media Superior, en cumplimiento a las disposiciones establecidas en el artículo 86 fracción III de la Ley Orgánica de la Universidad de Guadalajara y en los artículos 18 fracción I, 23 fracción I, 24, 25, 26, 27, 34, 36 y 54 del Reglamento de Obras y Servicios relacionados con las mismas y de los artículos 16, 19, 20, 44, 45 y 47, del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, mediante la Coordinación de Servicios Generales del Sistema de Educación Media Superior.

CONVOCA

A las personas físicas o morales nacionales debidamente constituidas en posibilidad de suministrar mobiliario y equipos, descritas a continuación y que deseen participar en las licitaciones para la adjudicación de los contratos correspondientes:

LICITACIONES DE ADQUISICIONES:

LICITACIÓN	DESCRIPCIÓN DE LOS BIENES Y/O SERVICIOS	FECHA LÍMITE DE INSCRIPCIÓN	JUNTA DE ACLARACIONES	PRESENTACIÓN Y APERTURA DE PROPUESTAS	ACTA DE LECTURA DE FALLO
LI-SEMS-038-FIP-2017	Adquisición de mobiliario escolar para bibliotecas de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo a proyecto ampliado FIP 2017.	17 de octubre de 2017	24 de octubre de 2017 14:00 horas	30 de octubre de 2017 13:00 horas	17 de noviembre de 2017 15:00 horas
LI-SEMS-039-FIP-2017	Adquisición de equipo de cómputo para Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo a proyecto ampliado FIP 2017.	17 de octubre de 2017	24 de octubre de 2017 15:30 horas	30 de octubre de 2017 15:00 horas	17 de noviembre de 2017 18:00 horas
LI-SEMS-040-2017	Adquisición de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria (CONECTIC).	17 de octubre de 2017	24 de octubre de 2017 17:00 horas	30 de octubre de 2017 17:00 horas	17 de noviembre de 2017 17:00 horas

LOS INTERESADOS A PARTICIPAR EN LA PRESENTE LICITACIÓN DEBERÁN:

unos cuantos.

A diferencia de ello, dijo, "yo elijo ponerme en manos de los ciudadanos, de millones de mexicanos que no se resignan a la corrupción, a la delincuencia, a la desigualdad", a través de un proyecto que depende de los ciudadanos y no del "dedazo del presidente ni de un arreglo cupular".

México necesita y se merece la participación de todos, aseguró, por lo que convocó a sus seguidores a juntar más de 866 mil firmas para validar la nueva alternativa de país: "Iremos por las firmas, que son un sí a un México honesto para acabar la desconfianza y la corrupción". *Agencias*

PIDEN RENUNCIA DE ANAYA EN CHANGE.ORG

CIUDAD DE MÉXICO.- Con la utilización de la plataforma Change.org, se promueven firmas para la renuncia de Ricardo Anaya de la dirigencia nacional del PAN ante su "autoritarismo" en su afán de ser el candidato presidencial para 2018 y dividir a esa fuerza política.

"Queremos que Ricardo Anaya renuncie a la dirigencia del PAN", plantea la propuesta que convoca a sumarse a Rebeldes del PAN.

Argumenta que el Partido Acción Nacional se encuentra sumido en una profunda crisis, la cual es consecuencia del autoritarismo de Anaya Cor-

Bases de la Licitación Pública LI-SEMS-040-2017

ADQUISICIÓN DE EQUIPOS DE SEGURIDAD DE SIGUIENTE GENERACIÓN PARA LA RED DE ESCUELAS PREPARATORIAS DEL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR, CON CARGO AL PROGRAMA DE MEJORAMIENTO A LA CONECTIVIDAD Y A LOS SERVICIOS DORSALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA RED UNIVERSITARIA (CONECTIC).

OCTUBRE 2017

ÍNDICE

SECCIÓN I
INSTRUCCIONES A LOS LICITANTES

A. Introducción

1. Fuente de los recursos

1.1 Los recursos corresponden a: Al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria (CONECTIC), proyectos 239737, 234888, 238485, 236427.

1.2 La presente licitación quedará sujeta a la disponibilidad presupuestal, por lo que sus efectos estarán condicionados a la existencia de los recursos financieros correspondientes, sin que la no realización de la presente origine responsabilidad para la contratante.

2. Licitantes elegibles

2.1 Esta convocatoria se hace a todas las personas físicas o morales nacionales, debidamente constituidas, con actividad empresarial, con domicilio en territorio nacional, que estén en posibilidad de suministrar **EQUIPOS DE SEGURIDAD EN LA CONECTIVIDAD Y A LOS SERVICIOS DORSALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.**

3. Costo de la licitación

3.1 El licitante sufragará todos los costos relacionados con la preparación y presentación de su propuesta y la Universidad de Guadalajara no será responsable, en ningún caso por dichos costos, cualquiera que sea la forma en que se realice la licitación o su resultado.

4. Restricciones

4.1 Las personas que se encuentren en alguno de los supuestos establecidos en el artículo 29 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, no podrán participar en la licitación.

B. Documentos de la Licitación

5. Información contenida en los documentos de la licitación

5.1 Las condiciones contractuales, además de la convocatoria, los documentos de la licitación incluyen:

I. Instrucciones a los licitantes,
II. Condiciones generales,
III. Catálogo de Conceptos,
IV. Carta de seriedad de la propuesta,
V. Carta compromiso.

5.2 El licitante deberá examinar todas las instrucciones, condiciones y especificaciones que figuren en los documentos de la licitación. Si el licitante "**no**" incluye toda la información requerida en la convocatoria y las bases de la licitación presenta una propuesta que no se ajusta sustancialmente y en todos sus aspectos a esos documentos, el resultado será el "**rechazo de su oferta"**.

6. Aclaración de las Bases de la Licitación.

6.1 Cualquier licitante inscrito puede solicitar aclaraciones sobre las bases de la licitación, para lo cual se llevará a cabo una **junta de aclaraciones, con carácter de obligatoria,** misma que se celebrará el día **24 de octubre de 2017, a las 17:00 horas**, en el Auditorio del Sistema de Educación Media Superior de la Universidad de Guadalajara situada en el 1er, (primer) piso ala derecha del edificio "Valentín Gómez Farías" del Sistema de Educación Media Superior de la Universidad de Guadalajara, ubicado en la calle Liceo No. 496, Colonia Centro, Guadalajara, Jalisco.

6.2 Para llevar a cabo esta reunión, los participantes deberán enviar sus preguntas por correo electrónico, en archivo de Word, a más tardar a las **14:00 horas del día 21 de octubre de 2017**, a las **2 (dos)** siguientes direcciones:

Rosaura.rodriguez@sems.udg.mx

fcalvillo@sems.udg.mx

6.3 Cualquier modificación a las bases de la licitación, derivada del resultado de la junta de aclaraciones, será considerada como parte integrante de las propias bases de la licitación.

6.4 Al participante que no asista a la junta de aclaraciones en la **fecha y hora exacta estipulada en las bases de la licitación**, por sí o su representante, no obstante haber adquirido las bases de la licitación, le será desechada su propuesta.

7. Modificación de los documentos de la Licitación

7.1 El Sistema de Educación Media Superior podrá, por cualquier causa y en cualquier momento, antes de que venza el plazo para la presentación de propuestas, modificar las bases de la licitación mediante enmienda, ya sea por iniciativa propia o en atención a una aclaración solicitada por un licitante interesado.

7.2 Las enmiendas serán notificadas por escrito a los licitantes registrados, pudiendo entregarse el aviso mediante correo electrónico y serán obligatorias para ellos.

7.3 El Sistema de Educación Media Superior podrá, a su discreción, prorrogar el plazo para la presentación de ofertas a fin de dar a los posibles licitantes tiempo razonable para tomar en cuenta en la preparación de sus ofertas por las enmiendas hechas a las bases de la licitación.

C. Preparación de las Propuestas

8. Idioma

8.1 La propuesta que prepare el licitante y toda la correspondencia y documentos relativos a ella que intercambien el licitante y el Sistema de Educación Media Superior, deberá redactarse en español; en todo caso, cualquier material impreso que proporcione el ofertante en otro idioma, deberá ser acompañado de una traducción al español de las partes pertinentes de dicho material impreso, la cual prevalecerá a los efectos de interpretación de la propuesta.

9. Descripción de los bienes a adquirir

9.1 El licitante elaborará su propuesta en papel membretado de la empresa, en la cual describirá los bienes a suministrar, de acuerdo con el catálogo de conceptos de la **Sección III** de las presentes bases.

9.2 Los bienes a adquirir se adjudicaran por partida, los licitantes podrán participar en una, varias o todas las partidas, ya que **la evaluación y la adjudicación de las propuestas se realizará por partida.**

10. Requisitos para el proveedor

10.1 Los licitantes deberán ser compañías legalmente establecidas en territorio nacional, que se dediquen preponderantemente a la venta de equipos de seguridad en la conectividad y a los servicios dorsales de tecnologías de información y comunicación.

10.2 Adicionalmente los licitantes presentarán documentación que describa las características, capacidad y cobertura de la infraestructura que le permite ofertar los bienes objeto de la presente licitación.

10.3 En caso de no apegarse a cualquiera de los requisitos solicitados en la convocatoria, las presentes bases y el acta de la junta de aclaraciones, **será motivo de descalificación de la propuesta.**

10.4 Cabe mencionar que en el contrato de compra que se suscriba entre las partes se incorporarán a los requisitos y demás condiciones planteadas en este documento.

10.5 El número de artículos a adquirir podrá variar en razón del monto de las propuestas que se presenten y de la disponibilidad presupuestal con que se cuenta.

11. Precios y vigencia

11.1 El licitante indicará los precios unitarios y totales de su propuesta de acuerdo al catálogo de conceptos de la presente licitación.

11.2 Precio fijo. Los precios cotizados por el ofertante serán fijos y no estarán sujetos a variación por ningún motivo. No se considerarán las ofertas presentadas con cotizaciones de precios variables por no ajustarse a los documentos de la licitación y en consecuencia, serán rechazadas.

11.3 La facturación de las partidas adjudicadas serán con cargo proyectos de la Coordinación de cómputo e Informática del Sistema de Educación Media Superior.

11.4 Las cantidades solicitadas **podrán disminuir o aumentar** de acuerdo al recurso disponible con el que cuenta la convocante para cada una de las partidas.

12. Moneda en la que se expresará la propuesta

12.1 El licitante deberá cotizar en moneda nacional.

13. Documentos que establezcan la elegibilidad y calificación del licitante.

13.1 El licitante presentará todos los documentos solicitados en convocatoria y en las presentes bases como acreditación que es elegible y calificable para participar en la licitación.

14. Garantías

14.1 La circunstancia de que el licitante adjudicado no cumpla con la suscripción del contrato o lo dispuesto en las cláusulas del mismo, constituirá causa suficiente para la anulación de la adjudicación, en cuyo caso el Sistema de Educación Media Superior podrá adjudicar el contrato al licitante cuya oferta fue la siguiente mejor evaluada, o convocar a una nueva Licitación.

14.2 El licitante deberá garantizar la seriedad de su propuesta, mediante carta original en papel membretado de la empresa, firmada por el representante legal, conforme al modelo que se adjunta en la Sección IV de estas bases, la cual deberá apegarse estrictamente al contenido de la misma.

14.3 El licitante adjudicado deberá contratar a favor de la Universidad de Guadalajara una fianza, correspondiente al 10% del monto total adjudicado en el contrato respectivo, para asegurar su debido cumplimiento, mismo que se establece en la sección V de las bases de la licitación.

14.4 El licitante deberá especificar claramente el tiempo de garantía en su propuesta económica de todos los bienes ofertados, misma que se deberá ofertar por el licitante participante.

14.5 El Sistema de Educación Media Superior **no otorgara anticipo**.

15. Período de validez de la propuesta

15.1 El participante deberá de especificar la vigencia o el periodo de validez de su propuesta. Se adjunta modelo de carta en la **Sección V** de estas bases, la cual se deberá apegar estrictamente al contenido de la misma y presentar original en papel membretado de la empresa, firmada por el representante legal.

16. Formato y firma de la propuesta

16.1 El paquete original de la propuesta deberá estar firmado con tinta indeleble, por el representante legal, en todas las hojas que lo integran, así como los documentos anexos al mismo y organizado en un recopilador, marcando cada sección con separadores de la siguiente manera:

A) Propuesta técnica:

A.1 Especificaciones técnicas, folletos, manuales, características de cada una de las partidas, capacidad y cobertura de la infraestructura que le permite al licitante suministrar los bienes o prestar los servicios requeridos.

A.2 Bases y anexos de la licitación completos, firmados en todas sus hojas por el representante legal de la empresa en señal de aceptación de las mismas, incluyendo el acta de la junta de aclaraciones.

B) Propuesta económica:

B.1 Propuesta económica firmada en todas sus hojas, con base en la descripción de los equipos a adquirir del punto 9.1.

B.2 Carta de seriedad de la propuesta.

B.3 Carta compromiso.

16.2 El licitante presentará un ejemplar original de la propuesta, la cual no deberá contener textos entre líneas, borrones, tachaduras ni enmendaduras.

D. Presentación de Propuestas

17. Sellado y marca de propuesta

17.1 La oferta será colocada dentro de un sobre que el licitante deberá cerrar y marcar respectivamente.

17.2 El sobre:

a) Estará rotulado con la siguiente dirección:

Sistema de Educación Media Superior de la Universidad de Guadalajara
Domicilio: Liceo 496 Esq. Juan Álvarez
Atención: Mtra. Adriana Lorena Fierros Lara
Secretario Ejecutivo del Comité de Compras y Adquisiciones del Sistema de Educación Media Superior

b) **Indicará:** Propuesta para la Licitación Pública **LI-SEMS-040-2017** denominada ADQUISICIÓN DE EQUIPOS DE SEGURIDAD DE SIGUIENTE GENERACIÓN PARA LA RED DE ESCUELAS PREPARATORIAS DEL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR, CON CARGO AL PROGRAMA DE MEJORAMIENTO A LA CONECTIVIDAD Y A LOS SERVICIOS DORSALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA RED UNIVERSITARIA (CONECTIC)., **fecha de la convocatoria y la frase "NO ABRIR ANTES DE LAS 17:00 HORAS DEL 30 DE OCTUBRE DE 2017".**

c) Si el sobre no fuese sellado y marcado siguiendo las instrucciones establecidas en estas bases, el Sistema de Educación Media Superior, no asumirá responsabilidad alguna en caso de que la oferta sea traspapelada o abierta prematuramente.

18. Plazo para la presentación de ofertas.

18.1 **Las ofertas deberán ser presentadas en** la Sala de Juntas anexa (ala derecha) al Auditorio del Sistema de Educación Media Superior de la Universidad de Guadalajara situada en el 1er, (primer) piso ala derecha del edificio "Valentín Gómez Farías" del Sistema de Educación Media Superior de la Universidad de Guadalajara, ubicado en la calle Liceo No. 496, Colonia Centro, Guadalajara, Jalisco; antes de las **17:00 HORAS DEL 30 DE OCTUBRE DE 2017".**

18.2 El Sistema de Educación Media Superior podrá, a su discreción, prorrogar el plazo para la presentación de propuestas, mediante la enmienda de los documentos de la licitación, en cuyo caso todos los derechos y obligaciones de la Universidad de Guadalajara y de los licitantes anteriormente sujetos a plazo original quedarán en adelante sujetos a los nuevos plazos que al efecto se establezcan.

19. Propuestas tardías

19.1 Toda propuesta que se presente después del plazo y hora exacta fijada para su recepción no será considerada y se devolverá sin abrir al licitante.

20. Modificación, sustitución y retiro de propuestas

20.1 Una vez presentadas las propuestas, ninguna de ellas, podrá ser modificada, sustituida, retirada o negociada.

20.2 Todos los documentos presentados dentro del sobre serán conservados por el Sistema de Educación Media Superior como constancia de su participación en la licitación.

E. Apertura y evaluación de propuestas

21. Apertura de propuestas

21.1 El Sistema de Educación Media Superior, abrirá las propuestas en sesión pública exactamente a las **17:00 HORAS DEL 30 DE OCTUBRE DE 2017.**, en el Sala de Juntas anexa (ala derecha) al Auditorio del Sistema de Educación Media Superior de la Universidad de Guadalajara situada en el 1er, (primer) piso del edificio "Valentín Gómez Farías" del Sistema de Educación Media Superior de la Universidad de Guadalajara, ubicado en la calle Liceo No. 496, Colonia Centro, Guadalajara, Jalisco.

21.2 El Sistema de Educación Media Superior, elaborará el acta de presentación y apertura de las propuestas, en la que se hará constar las ofertas recibidas, la falta de cualquier documento de la licitación, así como las que hubieren sido rechazadas y las causas que lo motivaron, la cual deberá ser firmada por los asistentes, entregándoles copia de la misma. La falta de firma de algún licitante no invalidará su contenido y efectos, poniéndose a partir de esa fecha a disposición de los que no hayan asistido, para efecto de su notificación.

22. Aclaración de propuestas

22.1 A fin de facilitar la revisión, evaluación y comparación de propuestas, el Sistema de Educación Media Superior podrá, a su discreción, solicitar a cualquier licitante las aclaraciones de su oferta.

23. Revisión, evaluación y comparación de las propuestas

23.1 El Sistema de Educación Media Superior examinará las propuestas para determinar si están completas, si contienen errores de cálculo, si los documentos han sido debidamente firmados y si, en general, las propuestas cumplen con los requisitos establecidos en las presentes bases y en la convocatoria de la licitación.

23.2 Los errores aritméticos serán ratificados de la siguiente manera: si existiera una discrepancia entre un precio unitario y el precio total que resulte de multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido. Si existiera una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras. Si el licitante no aceptara la corrección, su propuesta será rechazada.

23.3 La comparación de las propuestas, se hará tomando en cuenta el cumplimiento de la convocatoria, las bases, la junta de aclaraciones, los antecedentes del suministro de bienes o prestación de servicios anteriormente prestados, los tiempos de entrega, así como los precios propuestos por cada licitante, los cuales incluirán todos los costos, comisiones y los derechos e impuestos aplicables.

24. Comunicaciones con la Universidad de Guadalajara

24.1 Ningún licitante se comunicará con el Sistema de Educación Media Superior sobre ningún aspecto de su propuesta a partir del momento en el que se le entreguen las bases y hasta el momento de la adjudicación.

24.2 Cualquier intento, por parte de un licitante, de ejercer influencia sobre las decisiones del Comité de Compras y Adquisiciones del Sistema de Educación Media Superior, en la evaluación y comparación de ofertas, podrá dar lugar al rechazo de su propuesta. Los casos en que se considere que ha existido influencia estarán determinados por el criterio del Sistema de Educación Media Superior.

F. Adjudicación del Contrato

25. Criterios para la adjudicación.

25.1 El Sistema de Educación Media Superior, adjudicará la adquisición al licitante cuya oferta se ajuste sustancialmente a los documentos de la licitación y haya sido evaluada como la mejor, a condición que, además se haya determinado que esté calificado para cumplir satisfactoriamente con la adjudicación.

26. Derecho del Sistema de Educación Media Superior de aceptar cualquier propuesta y rechazar cualquiera (todas las) propuesta (s).

26.1 El Sistema de Educación Media Superior, se reserva el derecho de aceptar o rechazar cualquier propuesta, así como el de declarar desierta la licitación y rechazar todas las propuestas en cualquier momento, con anterioridad a la adjudicación, sin que por ello incurra en responsabilidad alguna respecto al licitante o los licitantes afectados por esta decisión y/o tenga la obligación de comunicar al licitante o los licitantes afectados los motivos de la acción del Sistema de Educación Media Superior.

26.2 Los acuerdos, disposiciones y decisiones tomadas por los miembros del Comité de Compras y Adquisiciones del Sistema de Educación Media Superior con respecto al resolutivo de la licitación, serán inapelables.

26.3 El Comité de Compras y Adquisiciones del Sistema de Educación Media Superior tendrá la facultad de decidir sobre cualquier controversia que pudiera presentarse durante el desarrollo de la licitación y de aplicar la normatividad de la Universidad de Guadalajara.

27. Notificación de la adjudicación

27.1 Antes de la expiración del período de validez de la oferta el Sistema de Educación Media Superior, notificará a los licitantes, a través del acta de lectura de fallo, el fallo emitido por el Comité de Compras y Adquisiciones del Sistema de Educación Media Superior.

27.2 El contrato se entenderá perfeccionado hasta el momento en que sea suscrito el mismo por los representantes legales de las partes.

27.3 A partir de la misma fecha del acta de lectura de fallo, la misma estará disponible en el Sistema de Educación Media Superior, para los licitantes que no hubieran asistido al acto de la lectura del fallo.

28. Firma del contrato

28.1 Desde el momento en que reciba el formulario de contrato, el licitante adjudicado tendrá **48 horas** después de su notificación para pasar a firmarlo al Sistema de Educación Media Superior.

G. Motivos por las que puede ser desechada la propuesta

29. Causas por las que puede ser desechada la propuesta

Se considerará como suficiente para desechar una propuesta, cualquiera de las siguientes causas:

A) El incumplimiento de alguno de los requisitos establecidos en las presentes Bases de la licitación y sus anexos.

B) Que se encuentre en cualquiera de los supuestos del Artículo 29 del Reglamento de Adquisiciones, Arrendamientos, y Contratación de Servicios de la Universidad de Guadalajara.

C) Que el concursante no presente su propuesta con tinta indeleble.

D) La falta de alguno de los requisitos o esté diferente a lo solicitado o incumpla lo acordado en el acta de la junta aclaratoria, en su caso.

E) La falta de la firma autógrafa con tinta indeleble del Representante Legal en alguna de las hojas de la propuesta.

F) Si presenta alguno de los documentos solicitados elaborados a lápiz o si lo presenta con tachaduras o enmendaduras.

G) Cuando no satisfagan cualquiera de los requisitos determinados en estas bases y sus anexos, y que no hayan sido detectados en el acto de presentación y apertura de propuestas.

H) Cuando los precios de los bienes ofertados por el licitante, se encuentren fuera de los precios de mercado o sean elevados de acuerdo al precio de referencia con los que cuente la convocante.

I) Si el licitante no especifica claramente el tiempo de garantía en su propuesta económica de todos los bienes ofertados, misma que se deberá ofertar por el licitante participante.

J) Si el licitante no especifica claramente dentro de la propuesta económica en el rubro de las condiciones de pago el tiempo de crédito que la empresa licitante ofrece en su propuesta.

K) Si el licitante solicita en su propuesta anticipo.

L) Si el licitante no especifica la marca y modelo del bien (es) cotizado (s) en su propuesta económica

M) Si el licitante establece su propuesta económica con un costo variable o negociable de los bienes ofertados.

N) Si el licitante no especifica claramente dentro de la propuesta económica el tiempo de entrega de los bienes ofertados.

O) Si el licitante no especifica claramente dentro de la propuesta la **vigencia de la cotización mínima requerida por la convocante** en la propuesta ofertada.

P) Si el licitante establece en su propuesta alguna de las condiciones generales de dos maneras diferentes.

Q) Si el licitante no se presenta al acto de junta aclaratoria en la fecha y hora exacta establecidas en la bases de la licitación.

R) Si el licitante no presenta su propuesta en el acto de presentación y apertura de propuestas en la fecha y hora exacta establecidas en la bases de la licitación.

S) Si el licitante no se apega estrictamente al contenido de la carta de seriedad de la propuesta, establecida en la **sección IV**, de las bases de la licitación.

T) Si el licitante no se apega estrictamente al contenido de la carta compromiso, establecida en la **sección V**, de las bases de la licitación.

Sección II.
CONDICIONES GENERALES

1. Entrega y documentos

1.1 El Licitante deberá de especificar claramente en su propuesta el tiempo de entrega.

1.2 El licitante **suministrará los bienes** de acuerdo a lo dispuesto por el Sistema de Educación Media Superior, en los siguientes lugares y con las cantidades que a continuación se indican:

Coordinación de Cómputo e Informática del Sistema de Educación Media Superior de la Universidad de Guadalajara, ubicada en:

Dirección: Liceo No. 496 esq. Juan Álvarez (piso 6)

1.3 El licitante que requiera parte o la totalidad de la información de carácter comercial presentada en virtud de este procedimiento se clasifique con carácter de confidencial, deberá de presentar la carta correspondiente en la que se especifique tal situación, de conformidad con la Ley de Información Pública del Estado de Jalisco y sus Municipios.

2. Pago

2.1 El licitante deberá de especificar en su propuesta en las condiciones de pago: crédito y deberá expresarlo en número días.

2.2 El pago al licitante se realizará posterior a la recepción a entera satisfacción de los bienes adjudicados, y este será en moneda nacional, contra la entrega de las facturas originales que cumplan todos los requisitos fiscales en vigor, de acuerdo a los tiempos establecidos en su propuesta.

2.3 El Sistema de Educación Media Superior **no otorgara ningún porcentaje de anticipo.**

2.4 El Sistema de Educación Media Superior **requiere el pago a crédito.**

3. Precios y vigencia

3.1 Los precios facturados por el licitante, no serán mayores a los que haya cotizado en su propuesta.

3.2 El Sistema de Educación Media Superior requiere una **vigencia mínima de cotización de 30 días**

4. Modificaciones al contrato

4.1 Toda variación o modificación de los términos del contrato deberá efectuarse mediante adendum o convenio modificatorio firmado por las partes.

5. Resolución por incumplimiento

5.1 El Sistema de Educación Media Superior podrá, sin perjuicio de los demás recursos que tenga en caso de incumplimiento del contrato por el licitante, terminar el contrato en todo o en parte mediante notificación escrita al licitante, si:

a) El licitante no entrega los bienes, de conformidad con el contrato.

b) Se considera incumplimiento si el licitante no cumple cualquier otra de sus obligaciones establecidas en el contrato.

c) En caso de incumplimiento por causa imputable al licitante, se obligará al pago de una pena del 1%, por cada día que transcurra, hasta el 10%, misma que se establecerá en el contrato respectivo.

5.2 El licitante será sancionado de acuerdo al Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara y a lo estipulado en el Código Civil vigente en el Estado de Jalisco, por incumplimiento del contrato, así como el pago de los daños y perjuicios que estos ocasionen al Sistema de Educación Media Superior.

6. Resolución por insolvencia

6.1 El Sistema de Educación Media Superior, podrá terminar anticipadamente el contrato con el licitante en cualquier momento mediante notificación por escrito, sin indemnización alguna a la misma, si ésta fuese declarada en concurso mercantil o insolvente siempre que dicha terminación no perjudique o afecte derecho alguno a acción o recurso, que tenga o pudiera tener la Universidad de Guadalajara.

7. Revocación por conveniencia

7.1 El Sistema de Educación Media Superior, podrá en cualquier momento terminar total o parcialmente el contrato por razones de conveniencia, mediante notificación escrita a la licitante. La notificación indicará que la terminación se debe a conveniencia de la Universidad de Guadalajara, el alcance del suministro que se haya completado y la fecha a partir de la cual la terminación entrará en vigor.

8. Idioma

8.1 El contrato se redactará en idioma español.

9. Leyes aplicables

9.1 La interpretación del contrato se hará de conformidad con las leyes vigentes del Estado de Jalisco.

10. Notificaciones

10.1 Toda notificación entre las partes, de conformidad con el contrato se harán por escrito a la dirección especificada para tal fin en las condiciones especiales del contrato, que en su caso se establezcan.

Contratante:
Secretario Ejecutivo del Comité de Compras y Adjudicaciones del Sistema de Educación Media Superior.
Liceo 496, Col centro, Guadalajara, Jalisco.

La notificación entrará en vigor en el momento de su entrega o en la fecha de entrada en vigor que se especifique en la notificación, si dicha fecha fuese posterior.

Sección III

CATÁLOGO DE CONCEPTOS

Descripción del Equipo requerido por el Sistema de Educación Media Superior, conforme a la siguiente tabla:

PARTIDA	CANTIDAD	ESPECIFICACIONES	P.U.	TOTAL
1	39	• **SOLUCIÓN UTM/NGFW TIPO 1 (1 UNIDAD)** Throughput de por lo menos 9 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete Soporte a por lo menos 2M conexiones simultaneas Soporte a por lo menos 135K nuevas conexiones por segundo Throughput de al menos 9 Gbps de VPN IPSec Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos Estar licenciado para, o soportar sin necesidad de licencia, 10K túneles de clientes VPN IPSec simultáneos Throughput de al menos 900 Mbps de VPN SSL Soportar al menos 300 clientes de VPN SSL simultáneos Soportar al menos 6000 Mbps de throughput de IPS Soportar al menos 1000 Mbps de throughput de Inspección SSL Throughput de al menos 1200 Mbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la solución de seguridad tenga debidamente activadas y operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado múltiples números de desempeño para cualquier de las funcionalidades, solamente el de valor más pequeño será aceptado. Permitir gestionar al menos 64 Access Points Tener al menos 14 interfaces 1 Gbps RJ45, 4 Gbps SFP, 2 Gbps para WAN Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance Debe de incluir un token físico para autenticación de doble factor para la gestión del appliance o para el acceso VPN que debe ser de la misma marca propuesta Debe de brindar soporte 36 meses del tipo 8x5, reemplazo siguiente día hábil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus, Botnet IP/Domain, AntiSpam y Filtrado Web • **REQUISITOS MÍNIMOS DE FUNCIONALIDAD** **Características Generales** La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo. ; Por funcionalidades de NGFW se entiende: aplicaciones de reconocimiento, prevención de amenazas, identificación de usuarios y control granular de permisos; Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación; La plataforma debe estar optimizada para aplicaciones de análisis de contenido en la capa 7; Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación; La gestión del equipo debe ser compatible con acceso a través de SSH, consola, web (HTTPS) y API abierta;		

		La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q; Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP; Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding; Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM); Los dispositivos de protección de red deben soportar DHCP Relay; Los dispositivos de protección de red deben soportar DHCP Server; Los dispositivos de protección de red deben soportar sFlow Los dispositivos de protección de red deben soportar Jumbo Frames; Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas Debe ser compatible con NAT dinámica (varios-a-1); Debe ser compatible con NAT dinámica (muchos-a-muchos); Debe soportar NAT estática (1-a-1); Debe admitir NAT estática (muchos-a-muchos); Debe ser compatible con NAT estático bidireccional 1-a-1; Debe ser compatible con la traducción de puertos (PAT); Debe ser compatible con NAT Origen; Debe ser compatible con NAT de destino; Debe soportar NAT de origen y NAT de destino de forma simultánea; Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico; Debe ser compatible con NAT64 y NAT46; Debe implementar el protocolo ECMP; Debe soportar el balanceo de enlace hash por IP de origen; Debe soportar el balanceo de enlace hash por IP de origen y destino; Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces; Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red Enviar logs a sistemas de gestión externos simultáneamente; Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL; Debe soporta protección contra la suplantación de identidad (anti-spoofing); Implementar la optimización del tráfico entre dos dispositivos; Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP); Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3); Soportar OSPF graceful restart; Los dispositivos de protección deben tener la capacidad de operar simultáneamente en una única instancia de servidor de seguridad, mediante el uso de sus interfaces físicas en los siguientes modos: modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3); Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red; Debe soportar modo capa - 2 (L2) para la inspección de datos en línea y la visibilidad del tráfico; Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en línea de tráfico; Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas; Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;		

		Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3; Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster; La configuración de alta disponibilidad debe sincronizar: Sesiones; La configuración de alta disponibilidad debe sincronizar: configuración, incluyendo, pero no limitados políticas de Firewalls, NAT, QoS y objetos de la red; La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN; La configuración de alta disponibilidad debe sincronizar: Tablas FIB; En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace; Debe soportar la creación de sistemas virtuales en el mismo equipo; Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos; Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes equipos; La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso; Debe aportar el control, la inspección y el descifrado de SSL para el tráfico entrante (inbound) y la salida (outbound), y debe ser compatible con el control de certificados de forma individual dentro de cada sistema virtual, es decir, el aislamiento de la adición, eliminación y uso de los certificados directamente en cada sistema virtual (contextos); • **CONTROL POR POLÍTICA DE FIREWALL** Debe soportar controles de zona de seguridad Debe contar con políticas de control por puerto y protocolo Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad Control de política por código de país (por ejemplo: BR, USA., UK, RUS) Control, inspección y des encriptación de SSL por política para el tráfico entrante y la salida Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada; Debe descifrar las conexiones de entrada y salida de tráfico negociadas con TLS 1.2; Control de inspección y descifrado SSH por política; Debe permitir el bloqueo de archivos por su extensión y permitir la identificación de archivo correcto por su tipo, incluso cuando se cambia el nombre de su extensión; Traffic shaping QoS basado en políticas (garantía de prioridad y máximo); QoS basado en políticas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones; Soporte para objetos y reglas IPV6; Soporte objetos y reglas de multicast; Debe ser compatible con al menos tres tipos de respuesta en las políticas de firewall: 'Drop' sin la notificación de bloqueo del usuario, 'Drop' con la notificación de bloqueo del usuario, Drop con opción de envío ICMP inalcanzable por la máquina fuente de tráfico, TCP Reset para el cliente , RESET de TCP con el servidor o en ambos lados de la conexión; Soportar la calendarización de políticas con el fin de activar y desactivar las reglas en tiempos predefinidos de forma automática;		

		• **CONTROL DE APLICACIÓN** Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos Reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no limitado a: el tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico; Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs; Debe inspeccionar la carga útil (payload) del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo; Debe detectar aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent; Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante; Debe hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el tráfico corresponde a la especificación del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTTP. La decodificación de protocolo también debe identificar las características específicas dentro de una aplicación, incluyendo, pero no limitado al intercambio de ficheros dentro de Webex Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas; Actualización de la base de firmas de la aplicación de forma automática; Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos; Los dispositivos de protección de red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario; Debe ser posible añadir múltiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas; Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación; Para mantener la seguridad de red eficiente debe ser soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas; Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos; Debe alertar al usuario cuando sea bloqueada una aplicación; Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;		

		Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo; Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video; Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo; Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc) Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: nivel de riesgo de la aplicación Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación • **PREVENCIÓN DE AMENAZAS** Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo; Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware); Las características de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no existe un contrato de garantía del software con el fabricante; Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad; Debe implementar los siguientes tipos de acciones a las amenazas detectadas por IPS: permitir, permitir y generar registro, bloque, bloque del IP del atacante durante un tiempo y enviar tcp-reset; Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo; Deben ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas; Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos Deber permitir el bloqueo de vulnerabilidades Debe permitir el bloqueo de exploits conocidos Debe incluir la protección contra ataques de denegación de servicio Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones; Debe tener los siguientes mecanismos de inspección IPS: análisis de decodificación de protocolo; Debe tener los siguientes mecanismos de inspección IPS: análisis para detectar anomalías de protocolo; Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico; Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP; Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP; Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets) Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones SYN, ICMP , UDP, etc; Detectar y bloquear los escaneos de puertos de origen; Bloquear ataques realizados por gusanos (worms) conocidos; Contar con firmas específicas para la mitigación de ataques DoS y DDoS; Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);		

		Debe poder crear firmas personalizadas en la interfaz gráfica del producto; Debe permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración; Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3; Soportar el bloqueo de archivos por tipo; Identificar y bloquear la comunicación con redes de bots; Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo; Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación; Debe permitir la captura de paquetes por tipo de firma IPS para definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la descripción, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos; Los eventos deben identificar el país que origino la amenaza; Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms) Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad • **FILTRADO DE URL** Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora); Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory, y la base de datos local; Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory, y la base de datos local, en modo de proxy transparente y explícito; Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL; Tener por lo menos 60 categorías de URL; Debe tener la funcionalidad de exclusión de URLs por categoría Permitir página de bloqueo personalizada; Permitir el bloqueo y continuación (que permite al usuario acceder a un sitio bloqueado potencialmente informándole en la pantalla de bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio); • **IDENTIFICACIÓN DE USUARIOS** Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración		

		con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local; Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios; Debe tener integración y soporte para Microsoft Active Directory para los siguientes sistemas operativos: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2; Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc; Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios; Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios; Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo); Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios; Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos del LDAP / AD Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma. Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores • **QOS TRAFFIC SHAPING** Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming; Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen; Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino; Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo; Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube; Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto; QoS debe permitir la definición de tráfico con ancho de banda garantizado; QoS debe permitir la definición de tráfico con máximo ancho de banda; QoS debe permitir la definición de cola de prioridad; Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype; Soportar marcación de paquetes DiffServ, incluso por aplicación;		

		Soportar la modificación de los valores de DSCP para Diffserv; Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service) Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shapig; Debe soportar QoS (traffic-shaping) en la interfaz agregada o redundantes; • **FILTRO DE DATOS** Permite la creación de filtros para archivos y datos predefinidos; Los archivos deben ser identificados por tamaño y tipo; Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.); Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos; Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos; Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares; • **GEO LOCALIZACIÓN** Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países; Debe permitir la visualización de los países de origen y destino en los registros de acceso; Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas. • **VPN** Soporte VPN de sitio a sitio y cliente a sitio; Soportar VPN IPSec; Soportar VPN SSL; La VPN IPSec debe ser compatible con 3DES; La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1; La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y el Grupo 14; La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2); La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard); La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall; Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting; La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web; Las características de VPN SSL se deben cumplir con o sin el uso de agentes; Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy; Asignación de DNS en la VPN de cliente remoto; Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;		

		Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local; Suportar lectura y revisión de CRL (lista de revocación de certificados); Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL; Debe permitir que la conexión a la VPN se establece de la siguiente manera: Antes de que el usuario se autentique en su estación Debería permitir la conexión a la VPN se establece de la siguiente manera: Después de la autenticación de usuario en la estación; Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo demanda de los usuarios; Deberá mantener una conexión segura con el portal durante la sesión; El agente de VPN SSL o IPSEC cliente a sitio debe ser compatible con al menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (v10.10 o superior); • **WIRELESS CONTROLLER** Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada Soportar servicio del servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos Soporte IPv4 e IPv6 por SSID Permitir elegir si el tráfico de cada SSID se enviará a la controladora o directamente por la interfaz de punto de acceso en una VLAN dada Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point Soportar monitoreo y supresión de puntos de acceso indebidos Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows Permitir la visualización de los dispositivos inalámbricos conectados por usuario Permitir la visualización de los dispositivos inalámbricos conectados por IP Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación Permitir la visualización de los dispositivos inalámbricos conectados por canal Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación Debe soportar Fast Roaming en autenticación con portal cautivo Debe soportar configuración de portal cautivo por SSID Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP. Debe ser compatible con el protocolo 802.1x RADIUS La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP La controladora deberá permitir métodos de descubrimiento de puntos de acceso por dns		

		La controladora deberá permitir métodos de descubrimiento de puntos de acceso por broadcast La controladora deberá permitir métodos de descubrimiento de puntos de acceso por multicast La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue) La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico La controladora deberá contar con mecanismos de protección de tramas de administración de acuerdo a las especificaciones de la alianza Wi-Fi y estándar 802.11ac La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh Ofrecer un mecanismo de creación automática y/o manual de usuarios visitantes y contraseñas, que puedan ser enviados por correo electrónico o SMS a los usuarios, con ajuste de tiempo de expiración de la contraseña La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS		

		Debe tener un mecanismo de ajuste automático de potencia de la señal con el fin de reducir la interferencia entre canales entre dos puntos de acceso administrados Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica; Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados Debe permitir asociación dinámicas de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico La controladora inalámbrica deberá soportar aceleración de tunnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico La controladora inalámbrica debe soportar protocolo LLDP Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC Adyacente Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada Deberá soportar la conversión de Multicast a Unicast para mejorar el rendimiento del tiempo de aire		

2	**28**	• **SOLUCIÓN UTM/NGFW TIPO 1 (1 UNIDAD)** Throughput de por lo menos 16 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete Soporte a por lo menos 4M conexiones simultaneas Soporte a por lo menos 200K nuevas conexiones por segundo Throughput de al menos 14 Gbps de VPN IPSec Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos Estar licenciado para, o soportar sin necesidad de licencia, 50K túneles de clientes VPN IPSec simultáneos Throughput de al menos 350 Mbps de VPN SSL Soportar al menos 500 clientes de VPN SSL simultáneos Soportar al menos 2800 Mbps de throughput de IPS Soportar al menos 1900 Mbps de throughput de Inspección SSL Throughput de al menos 1500 Mbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la solución de seguridad tenga debidamente activadas y operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado múltiples números de desempeño para cualquier de las funcionalidades, solamente el de valor más pequeño será aceptado. Permitir gestionar al menos 256 Access Points Tener al menos 8 interfaces 1 Gbps RJ45, 8 interfaces de 1 Gbps SFP, 2 interfaces 1 Gbps para Gestión Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance Debe de incluir un token físico para autenticación de doble factor para la gestión del appliance o para el acceso VPN que debe ser de la misma marca propuesta Debe de brindar soporte 36 meses del tipo 8x5, reemplazo siguiente día hábil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus, Botnet IP/Domain, AntiSpam y Filtrado Web • **REQUISITOS MÍNIMOS DE FUNCIONALIDAD** **CARACTERÍSTICAS GENERALES** La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo. Por funcionalidades de NGFW se entiende: aplicaciones de reconocimiento, prevención de amenazas, identificación de usuarios y control granular de permisos; Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación; La plataforma debe estar optimizada para aplicaciones de análisis de contenido en la capa 7; Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación; La gestión del equipo debe ser compatible con acceso a través de SSH, consola, web (HTTPS) y API abierta; La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q; Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP; Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding; Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);		

		Los dispositivos de protección de red deben soportar DHCP Relay; Los dispositivos de protección de red deben soportar DHCP Server; Los dispositivos de protección de red deben soportar sFlow Los dispositivos de protección de red deben soportar Jumbo Frames; Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas Debe ser compatible con NAT dinámica (varios-a-1); Debe ser compatible con NAT dinámica (muchos-a-muchos); Debe soportar NAT estática (1-a-1); Debe admitir NAT estática (muchos-a-muchos); Debe ser compatible con NAT estático bidireccional 1-a-1; Debe ser compatible con la traducción de puertos (PAT); Debe ser compatible con NAT Origen; Debe ser compatible con NAT de destino; Debe soportar NAT de origen y NAT de destino de forma simultánea; Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico; Debe ser compatible con NAT64 y NAT46; Debe implementar el protocolo ECMP; Debe soportar el balanceo de enlace hash por IP de origen; Debe soportar el balanceo de enlace hash por IP de origen y destino; Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces; Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red Enviar logs a sistemas de gestión externos simultáneamente; Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL; Debe soporta protección contra la suplantación de identidad (anti-spoofing); Implementar la optimización del tráfico entre dos dispositivos; Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP); Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3); Soportar OSPF graceful restart; Los dispositivos de protección deben tener la capacidad de operar simultáneamente en una única instancia de servidor de seguridad, mediante el uso de sus interfaces físicas en los siguientes modos: modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3); Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red; Debe soportar modo capa - 2 (L2) para la inspección de datos en línea y la visibilidad del tráfico; Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en línea de tráfico; Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas; Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente; Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3; Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster; La configuración de alta disponibilidad debe sincronizar: Sesiones; La configuración de alta disponibilidad debe sincronizar: configuración, incluyendo, pero no limitados políticas de Firewalls, NAT, QoS y objetos de la red; La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN; La configuración de alta disponibilidad debe sincronizar: Tablas FIB;		

		En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace; Debe soportar la creación de sistemas virtuales en el mismo equipo; Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos; Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes equipos; La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso; Debe aportar el control, la inspección y el descifrado de SSL para el tráfico entrante (inbound) y la salida (outbound), y debe ser compatible con el control de certificados de forma individual dentro de cada sistema virtual, es decir, el aislamiento de la adición, eliminación y uso de los certificados directamente en cada sistema virtual (contextos); • **CONTROL POR POLÍTICA DE FIREWALL** Debe soportar controles de zona de seguridad Debe contar con políticas de control por puerto y protocolo Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad Control de política por código de país (por ejemplo: BR, USA., UK, RUS) Control, inspección y des encriptación de SSL por política para el tráfico entrante y la salida Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada; Debe descifrar las conexiones de entrada y salida de tráfico negociadas con TLS 1.2; Control de inspección y descifrado SSH por política; Debe permitir el bloqueo de archivos por su extensión y permitir la identificación de archivo correcto por su tipo, incluso cuando se cambia el nombre de su extensión; Traffic shaping QoS basado en políticas (garantía de prioridad y máximo); QoS basado en políticas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones; Soporte para objetos y reglas IPV6; Soporte objetos y reglas de multicast; Debe ser compatible con al menos tres tipos de respuesta en las políticas de firewall: 'Drop' sin la notificación de bloqueo del usuario, 'Drop' con la notificación de bloqueo del usuario, Drop con opción de envío ICMP inaccesible por la máquina fuente de tráfico, TCP Reset para el cliente , RESET de TCP con el servidor o en ambos lados de la conexión; Soportar la calendarización de políticas con el fin de activar y desactivar las reglas en tiempos predefinidos de forma automática; • **CONTROL DE APLICACIÓN** Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos Reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no limitado a: el tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico; Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, **gmail,** youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp,		

		4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs; Debe inspeccionar la carga útil (payload) del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo; Debe detectar aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent; Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante; Debe hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el tráfico corresponde a la especificación del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTTP. La decodificación de protocolo también debe identificar las características específicas dentro de una aplicación, incluyendo, pero no limitado al intercambio de ficheros dentro de Webex Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas; Actualización de la base de firmas de la aplicación de forma automática; Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos; Los dispositivos de protección de red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario; Debe ser posible añadir múltiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas; Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación; Para mantener la seguridad de red eficiente debe ser soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas; Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos; Debe alertar al usuario cuando sea bloqueada una aplicación; Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo; Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo; Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video; Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo; Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc) Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: nivel de riesgo de la aplicación Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación		

		• **PREVENCIÓN DE AMENAZAS** Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo; Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware); Las características de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no existe un contrato de garantía del software con el fabricante; Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad; Debe implementar los siguientes tipos de acciones a las amenazas detectadas por IPS: permitir, permitir y generar registro, bloque, bloque del IP del atacante durante un tiempo y enviar tcp-reset; Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo; Deben ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas; Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos Deber permitir el bloqueo de vulnerabilidades Debe permitir el bloqueo de exploits conocidos Debe incluir la protección contra ataques de denegación de servicio Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones; Debe tener los siguientes mecanismos de inspección IPS: análisis de decodificación de protocolo; Debe tener los siguientes mecanismos de inspección IPS: análisis para detectar anomalías de protocolo; Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico; Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP; Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP; Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets) Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones SYN, ICMP , UDP, etc; Detectar y bloquear los escaneos de puertos de origen; Bloquear ataques realizados por gusanos (worms) conocidos; Contar con firmas específicas para la mitigación de ataques DoS y DDoS; Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow); Debe poder crear firmas personalizadas en la interfaz gráfica del producto; Debe permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración; Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3; Soportar el bloqueo de archivos por tipo; Identificar y bloquear la comunicación con redes de bots; Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo; Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;		

		Debe permitir la captura de paquetes por tipo de firma IPS para definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la descripción, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos; Los eventos deben identificar el país que origino la amenaza; Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms) Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad • **FILTRADO DE URL** Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora); Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory, y la base de datos local; Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory, y la base de datos local, en modo de proxy transparente y explícito; Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL; Tener por lo menos 60 categorías de URL; Debe tener la funcionalidad de exclusión de URLs por categoría Permitir página de bloqueo personalizada; Permitir el bloqueo y continuación (que permite al usuario acceder a un sitio bloqueado potencialmente informándole en la pantalla de bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio); • **IDENTIFICACIÓN DE USUARIOS** Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local; Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios; Debe tener integración y soporte para Microsoft Active Directory para los siguientes sistemas operativos: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2; Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier		

		restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc; Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios; Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios; Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo); Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios; Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos del LDAP / AD Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma. Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores • **QOS TRAFFIC SHAPING** Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming; Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen; Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino; Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo; Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube; Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto; QoS debe permitir la definición de tráfico con ancho de banda garantizado; QoS debe permitir la definición de tráfico con máximo ancho de banda; QoS debe permitir la definición de cola de prioridad; Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype; Soportar marcación de paquetes DiffServ, incluso por aplicación; Soportar la modificación de los valores de DSCP para Diffserv; Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service) Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping; Debe soportar QoS (traffic-shaping) en la interfaz agregada o redundantes; • **FILTRO DE DATOS** Permite la creación de filtros para archivos y datos predefinidos; Los archivos deben ser identificados por tamaño y tipo; Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);		

		Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos; Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos; Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares; • **GEO LOCALIZACIÓN** Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países; Debe permitir la visualización de los países de origen y destino en los registros de acceso; Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas. • **VPN** Soporte VPN de sitio a sitio y cliente a sitio; Soportar VPN IPSec; Soportar VPN SSL; La VPN IPSec debe ser compatible con 3DES; La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1; La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y el Grupo 14; La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2); La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard); La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall; Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting; La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web; Las características de VPN SSL se deben cumplir con o sin el uso de agentes; Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy; Asignación de DNS en la VPN de cliente remoto; Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL; Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local; Suportar lectura y revisión de CRL (lista de revocación de certificados); Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL; Debe permitir que la conexión a la VPN se establece de la siguiente manera: Antes de que el usuario se autentique en su estación Debería permitir la conexión a la VPN se establece de la siguiente manera: Después de la autenticación de usuario en la estación; Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo demanda de los usuarios; Deberá mantener una conexión segura con el portal durante la sesión;		

		El agente de VPN SSL o IPSEC cliente a sitio debe ser compatible con al menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (v10.10 o superior); • **WIRELESS CONTROLLER** Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada Soportar servicio del servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos Soporte IPv4 e IPv6 por SSID Permitir elegir si el tráfico de cada SSID se enviará a la controladora o directamente por la interfaz de punto de acceso en una VLAN dada Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point Soportar monitoreo y supresión de puntos de acceso indebidos Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows Permitir la visualización de los dispositivos inalámbricos conectados por usuario Permitir la visualización de los dispositivos inalámbricos conectados por IP Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación Permitir la visualización de los dispositivos inalámbricos conectados por canal Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación Debe soportar Fast Roaming en autenticación con portal cautivo Debe soportar configuración de portal cautivo por SSID Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP. Debe ser compatible con el protocolo 802.1x RADIUS La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP La controladora deberá permitir métodos de descubrimiento de puntos de acceso por dns La controladora deberá permitir métodos de descubrimiento de puntos de acceso por broadcast La controladora deberá permitir métodos de descubrimiento de puntos de acceso por multicast La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue) La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico La controladora deberá contar con mecanismos de protección de tramas de administración de acuerdo a las especificaciones de la alianza Wi-Fi y estándar 802.11ac La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP		

		La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh Ofrecer un mecanismo de creación automática y/o manual de usuarios visitantes y contraseñas, que puedan ser enviados por correo electrónico o SMS a los usuarios, con ajuste de tiempo de expiración de la contraseña La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS Debe tener un mecanismo de ajuste automático de potencia de la señal con el fin de reducir la interferencia entre canales entre dos puntos de acceso administrados Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica; Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados		

		La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados Debe permitir asociación dinámicas de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico La controladora inalámbrica deberá soportar aceleración de tunnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico La controladora inalámbrica debe soportar protocolo LLDP Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC Adyacente Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada Deberá soportar la conversión de Multicast a Unicast para mejorar el rendimiento del tiempo de aire		
SUBTOTAL				
I.V.A.				
TOTAL				

Condiciones de pago: (crédito expresado en No. de días)
Tiempo de garantía que otorga el licitante concursante de los bienes ofertados:
Tiempo de entrega:
Vigencia de la cotización:

Notas:

- **Los equipos ofertados de cada partida deberán ser de marca.**
- **Se deberá especificar la marca y modelo del equipo ofertado en cada partida.**
- **Se deberán especificar en su propuesta económica el tiempo de garantía de todas las partidas, misma que deberá ser ofertado por la empresa licitante cuando menos 1 (un) año en todas las partidas.**
- **En los precios ofertados deberá de considerarse el costo de flete para la entrega a cada dependencia beneficiada.**

SECCION IV

CARTA DE SERIEDAD DE LA PROPUESTA

Licitación Pública No. LI-SEMS-040-2017

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media Superior
Universidad de Guadalajara.
Presente.

En referencia a la convocatoria publicada el 13 de octubre 2017, mediante la cual se invita a participar en la Licitación Pública arriba indicada, relativa a la ADQUISICIÓN DE EQUIPOS DE SEGURIDAD DE SIGUIENTE GENERACIÓN PARA LA RED DE ESCUELAS PREPARATORIAS DEL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR, CON CARGO AL PROGRAMA DE MEJORAMIENTO A LA CONECTIVIDAD Y A LOS SERVICIOS DORSALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA RED UNIVERSITARIA (CONECTIC)., y como representante legal de la empresa _____, manifiesto a usted que se cumplió en tiempo y forma con el registro señalado en dicha convocatoria y se adquirieron las bases y los anexos relativos a la licitación mencionada. También le informo que estamos enterados del contenido de las bases y las hemos aceptado íntegramente. Para tal efecto he tomado la debida nota a que nos sujetamos y se devuelven debidamente firmados.

Por otra parte manifiesto a usted, que se han tomado en cuenta las aclaraciones a las dudas de los licitantes participantes y declaro que mi representada posee y conoce toda la información adicional proporcionada por el Sistema de Educación Media Superior como complemento de la documentación inicial que se recibió y que se anexa a nuestra proposición.

Igualmente le informo que la empresa a la que represento se compromete a acatar las instrucciones señaladas en las bases de la licitación y garantizamos respetar nuestra oferta hasta la fecha límite de vigencia.

A T E N T A M E N T E

_____, Jalisco; a _____de _____ 2017

_____
NOMBRE Y FIRMA
REPRESENTANTE LEGAL DE LA EMPRESA O PERSONA FÍSICA

Sección V

CARTA COMPROMISO

Licitación Publica No. LI-SEMS-040-2017

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media Superior
Universidad de Guadalajara.
Presente.

Luego de haber examinado los documentos de la licitación, de los cuales confirmamos recibo por la presente, los suscritos ofrecemos ADQUISICIÓN DE EQUIPOS DE SEGURIDAD DE SIGUIENTE GENERACIÓN PARA LA RED DE ESCUELAS PREPARATORIAS DEL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR, CON CARGO AL PROGRAMA DE MEJORAMIENTO A LA CONECTIVIDAD Y A LOS SERVICIOS DORSALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA RED UNIVERSITARIA (CONECTIC)., de conformidad con dichos documentos, por la suma de $ ---------- (monto total de la oferta en palabras), con I.V.A. incluido, de acuerdo a la propuesta económica que se adjunta a la presente oferta y que forma parte integrante de ella.

Si nuestra oferta es aceptada, contrataremos a favor de la Universidad de Guadalajara una fianza, correspondiente al 10% del monto total adjudicado en el contrato respectivo, para asegurar su debido cumplimiento.

Convenimos en mantener esta oferta por un período de ____ días naturales a partir de la fecha fijada para la apertura de las propuestas, la cual nos obligará y podrá ser aceptada en cualquier momento antes de que expire el período indicado. Ésta, junto con el acta de lectura de fallo de adjudicación, constituirá un contrato obligatorio hasta que se prepare y firme el Contrato formal.

Entendemos que ustedes no están obligados a aceptar la más baja, ni ninguna otra de las ofertas que reciban.

A T E N T A M E N T E
Guadalajara, Jalisco; a_____de_____de 2017

_____
NOMBRE Y FIRMA
REPRESENTANTE LEGAL DE LA EMPRESA O PERSONA FÍSICA

DICTAMEN TÉCNICO

Guadalajara, Jalisco a 01 de noviembre de 2017

LICITACION: LI-SEMS-040-2017
DEPENDENCIA: SISTEMA DE EDUCACION MEDIA SUPERIOR
NOMBRE: ADQUISICIÓN DE EQUIPOS DE SEGURIDAD DE SIGUIENTE GENERACIÓN PARA LA RED DE ESCUELAS PREPARATORIAS DEL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR, CON CARGO AL PROGRAMA DE MEJORAMIENTO A LA CONECTIVIDAD Y A LOS SERVICIOS DORSALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA RED UNIVERSITARIA (CONECTIC).

1.- Relación de las proposiciones declaradas solventes, porque cumplen con todos los requisitos solicitados:

EMPRESAS	IMPORTE INCLUYE I.V.A
INITEL, S.A. DE C.V.	**$11´654,366.40**

2.- Criterios utilizados para la evaluación de las propuestas:

La Coordinación de Servicios Generales del Sistema de Educación Media Superior, para hacer la evaluación de las propuestas, realizaron lo siguiente:

Se revisaron las propuestas, de conformidad con lo estipulado en el Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, en sus artículos 45 y 47, en las bases de la licitación entregadas a los participantes, como se refleja en los siguientes puntos:

I) Se tomaron en cuenta sus antecedentes, su especialidad, su capacidad operativa.

II) Se consideraron los criterios de precio, calidad, tiempo de entrega, cumplimiento de requisitos técnicos, oportunidad y demás condiciones favorables a la Universidad de Guadalajara.

a) Que las propuestas contemplen todas y cada una de los requisitos solicitados en las bases de la licitación.

b) Que las mismas incluyan la información, documentos y requisitos solicitados.

c) Se verificó que las operaciones aritméticas se hayan ejecutado correctamente, en caso de que una o más tengan errores, se efectuaron las correcciones correspondientes, el monto correcto es el que se considera para el análisis comparativo de las proposiciones.

III) Criterios para la evaluación de las propuestas:

Se consideró la revisión del cumplimiento documental de las propuestas, que consistieron en lo siguiente:

- Verificación del cumplimiento de las especificaciones técnicas requeridas mediante dictamen técnico emitido por Ing. Esmeralda Olmos De La Cruz Coordinadora de Cómputo e Informática del Sistema de Educación Media Superior.
- Cumplimiento de los requisitos documentales para el concursante.
- Condiciones de pago.
- Precio.
- Vigencia de la cotización.
- Garantías.
- Tiempo de entrega.

3.- De conformidad con la revisión y evaluación de las propuestas, la Coordinación de Servicios Generales de Sistema de Educación Media Superior sugiere la adjudicación de la siguiente manera:

Partidas: **1 y 2**
Empresa: **INITEL, S.A. DE C.V.**
Por un importe de **$ 11´654,366.40 (Once millones seiscientos cincuenta y cuatro mil trescientos sesenta y seis pesos 40/100 m.n.) I.V.A. Incluido.**

En virtud de haber reunido las condiciones legales, técnicas y económicas para garantizar satisfactoriamente el cumplimiento de las obligaciones respectivas y haber presentado la propuesta solvente más baja en cada una de las partidas, en apego a lo establecido en los artículos 45 Y 47., del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara.

ELABORÓ

MTRA. ROSAURA RODRIGUEZ RODRIGUEZ
JEFA DE LA UNIDAD DE ADQUISICIONES
DEL SEMS

AUTORIZÓ

ING. FERNANDO CALVILLO VARGAS
COORDINADOR DE SERVICIOS
GENERALES DEL SEMS

ACTA DE FALLO

LICITACION: LI-SEMS-040-2017
DEPENDENCIA: SISTEMA DE EDUCACION MEDIA SUPERIOR
NOMBRE: ADQUISICIÓN DE EQUIPOS DE SEGURIDAD DE SIGUIENTE GENERACIÓN PARA LA RED DE ESCUELAS PREPARATORIAS DEL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR, CON CARGO AL PROGRAMA DE MEJORAMIENTO A LA CONECTIVIDAD Y A LOS SERVICIOS DORSALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA RED UNIVERSITARIA (CONECTIC).

En la Ciudad de Guadalajara, Jalisco siendo las 19:20 horas del día 15 de noviembre de 2017, se reunieron en la sala de juntas de Dirección General del Sistema de Educación Media Superior, los integrantes del Comité de Adquisiciones para emitir el siguiente fallo.

El Lic. Eduardo Gómez Abreu, Presidente del Comité de Compras y Adquisiciones del Sistema de Educación Media Superior con base en las atribuciones del Comité, contempladas en el Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, se llevó a cabo el análisis de los documentos presentados por la Coordinación de Servicios Generales del SEMS, e hizo saber que la adjudicación por Licitación Pública, corresponde a:

Partidas: **1 y 2**
Empresa: **INITEL, S.A. DE C.V.**
Por un importe de **$ 11´654,366.40 (Once millones seiscientos cincuenta y cuatro mil trescientos sesenta y seis pesos 40/100 m.n.) I.V.A. Incluido.**

En virtud de haber reunido las condiciones legales, técnicas y económicas para garantizar satisfactoriamente el cumplimiento de las obligaciones respectivas y haber presentado la propuesta solvente más baja en cada una de las partidas, en apego a lo establecido en los artículos 45 Y 47., del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara.

Lic. Eduardo Gómez Abreu
Presidente del Comité de Compras
y Adquisiciones del SEMS

Mtra. Adriana Lorena Fierros Lara
Secretario Ejecutivo del Comité de Compras
y Adquisiciones SEMS

UNIVERSIDAD DE GUADALAJARA

Red Universitaria de Jalisco

CARATULA CONTRATO COMPRAVENTA

LAS PARTES

LA UNIVERSIDAD		EL VENDEDOR	
Nombre, denominación o razón social	Universidad de Guadalajara	**Nombre, denominación o razón social**	INITEL S.A. de C.V.
Representante	Dra. Carmen Enedina Rodríguez Armenta	**Acta Constitutiva**	Escritura Pública No. 50,136 de fecha 27 de Diciembre de 2002, ante el Lic. Jorge Robles Farías, Notario Público Titular No. 12, Guadalajara, Jalisco.
Título	Apoderada	**Representante**	Ing. Teobaldo Leal Arriaga
		Título	Administrador General Único
Documento que acredita las facultades	Escritura Pública No. 6,931 de fecha 18 de abril de 2013, otorgada ante la fe del Lic. Juan José Serratos Cervantes, Notario Público No. 116 de Guadalajara, Jalisco	**Documento que acredita las facultades**	Acta Constitutiva
		R.F.C.	[redacted] 1
		Clave Patronal I.M.S.S.	[redacted] 2
Domicilio	Avenida Juárez número 976, Zona Centro, Código Postal 44100, en Guadalajara, Jalisco	**Domicilio**	[redacted] 3

OBJETO E IMPORTE

Denominación	Adquisición de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de... (ver acta de fallo)		
Clave	LI-SEMS-040-2017	**Procedimiento de Adjudicación**	Licitación
Dependencia responsable del seguimiento	Sistema de Educación Media Superior	**Dependencia o comité que adjudicó**	Comité de Compras y Adquisiciones del Sistema de Educación Media Superior
Cantidad a pagar	$11´654,366.40 Incluye IVA	**Partidas**	1 y 2
		Tipo de Recurso	☐ Estatal ☒ Federal
Forma de pago (periodicidad)	15 días posteriores a la entrega de la totalidad de los bienes a entera satisfacción de la Universidad	**Fondo**	Programa CONECTIC
PLAZO DE ENTREGA		**INSTALACIÓN**	
Plazo de entrega	6 semanas	☐ SI incluye instalación	
A partir de	La firma del presente	☒ NO incluye instalación	

FIANZAS

☐	a) Fianza para garantizar la correcta aplicación de los recursos del anticipo, por el importe total de éste, la cual deberá ser cancelada solo con el consentimiento por escrito de LA UNIVERSIDAD, y que deberá ser entregada previo a la entrega de dicho anticipo.
☒	b) Fianza para garantizar el cabal cumplimiento de todas las obligaciones contenidas en el presente contrato, misma que se contratará por el 10% (diez por ciento) del valor total del presente, y que deberá ser entregada dentro de los tres días naturales siguientes a la firma del presente.
☐	c) Fianza para garantizar los defectos o vicios ocultos, la cual se contratará por la cantidad de 10% (diez por ciento) del valor total del presente contrato, la que contará con una duración de 1 (un) año a partir de la fecha en que LA UNIVERSIDAD reciba los bienes por escrito, y deberá ser cancelada solo con el consentimiento por escrito de LA UNIVERSIDAD, a la entrega del acta de recepción expedida por LA UNIVERSIDAD, y una vez entregada esta fianza, se procederá a la cancelación de las establecidas en los incisos a) y b), mediante el escrito que para tal efecto emita LA UNIVERSIDAD.
☐	d) No aplica

FIRMAS

Enteradas las partes del contenido y alcance, lo ratifican y firman en triplicado, de conformidad ante los testigos.

En la ciudad de Guadalajara, Jalisco		**Fecha**	21 de noviembre de 2017
LA UNIVERSIDAD		**EL VENDEDOR**	
		[redacted] 4	
Representante	Dra. Carmen Enedina Rodríguez Armenta	**Representante**	Ing. Teobaldo Leal Arriaga
Título	Apoderada	**Título**	Administrador General Único
TESTIGOS			
Nombre	Ing. Fernando Calvillo Vargas	**Nombre**	Mtra. Adriana Lorena Fierros Lara
Cargo	Coordinador de Servicios Generales del Sistema de Educación Media Superior	**Cargo**	Secretario Administrativo del Sistema de Educación Media Superior

CONTRATO DE COMPRAVENTA QUE CELEBRAN POR UNA PARTE **LA UNIVERSIDAD DE GUADALAJARA,** A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ **LA UNIVERSIDAD,** Y POR LA OTRA PARTE, LA PERSONA CUYA DENOMINACIÓN APARECE EN LA CARATULA DEL PRESENTE CONTRATO, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ **EL VENDEDOR,** DE ACUERDO A LAS SIGUIENTES:

DECLARACIONES:

Declara **LA UNIVERSIDAD**:

I. Que es un organismo público descentralizado del gobierno del Estado de Jalisco con autonomía, personalidad jurídica y patrimonio propios de conformidad con lo dispuesto en el artículo primero de su Ley Orgánica publicada por el Ejecutivo Estatal el día 15 de enero de 1994, en ejecución del Decreto número 15,319 del H. Congreso del Estado de Jalisco.
II. Que es atribución de la Universidad de Guadalajara, conforme a la fracción XI del artículo 6 de la Ley Orgánica, administrar su patrimonio.
III. Que el Rector General es la máxima autoridad ejecutiva de la Universidad, representante legal de la misma, de conformidad con el artículo 32 de la ley Orgánica de la Universidad.
IV. Que su representante cuenta con las facultades necesarias para suscribir el presente contrato, mismas que manifiesta no le han sido revocadas, modificadas o restringidas en sentido alguno.

Declara **EL VENDEDOR** bajo protesta de decir verdad:

I. Que tiene la capacidad jurídica para contratar y obligarse a suministrar los bienes adjudicados por **LA UNIVERSIDAD**.
II. Que conoce el contenido y los alcances del artículo29 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, y en su caso del artículo 50 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y que no se encuentra en alguno de los supuestos establecidos por el mismo.

Declaran las partes que han convenido celebrar el presente contrato, para lo cual se sujetan a lo establecido en las siguientes:

CLÁUSULAS:

PRIMERA.- Las partes acuerdan que el objeto del presente contrato es que **EL VENDEDOR** realice a favor de **LA UNIVERSIDAD** el suministro cuya denominación aparece en la carátula del mismo, y que se detalla en el documento que como Anexo "A" se acompaña al presente.

Al respecto **EL VENDEDOR** se sujetará conforme a las indicaciones que le dé **LA UNIVERSIDAD** y a lo establecido en el presente instrumento.

Todo aquello que **EL VENDEDOR** necesitará para lograr el cumplimiento de lo establecido en el presente, incluidos los costos de transportación de los bienes, será a su cargo exclusivamente, liberando en consecuencia a **LA UNIVERSIDAD** de cualquier reclamación que se intente en su contra por alguno de los conceptos antes señalados.

SEGUNDA.- LA UNIVERSIDAD se obliga a pagar a **EL VENDEDOR** por los conceptos amparados en el presente, la cantidad establecida en la carátula del presente.

LA UNIVERSIDAD pagará a **EL VENDEDOR** dicha cantidad conforme a lo establecido en la carátula del presente.

Por su parte **EL VENDEDOR** se compromete a entregar la factura correspondiente con los requisitos que las leyes fiscales establecen, y a su vez, asume cualquier obligación fiscal que se derive del presente contrato, sacando en paz y a salvo a **LA UNIVERSIDAD** de cualquier reclamación que al respecto se pudiera originar.

Adicionalmente las partes acuerdan que en el supuesto de que **EL VENDEDOR** no cumpla con alguna de sus obligaciones en los tiempos pactados o conforme a las características establecidas, el pago se verá retrasado en la misma proporción. Lo anterior independientemente de que **LA UNIVERSIDAD** decida continuar con el contrato o darlo por rescindido.

Así mismo, las partes acuerdan que el presente contrato quedará sujeto a la disponibilidad presupuestal, por lo que sus efectos estarán condicionados a la existencia de los recursos financieros correspondientes, sin que la no realización del mismo por esta causa origine responsabilidad para **LA UNIVERSIDAD**.

TERCERA.- EL VENDEDOR se obliga a realizar todas las gestiones necesarias y a tramitar a su cargo, todas las licencias, permisos, avisos, seguros aplicables, importaciones y demás autorizaciones en general que sean obligatorias y/o que se requieran, a fin de cumplir con lo establecido en el presente contrato.

EL VENDEDOR deberá pagar todas las multas debido a infracciones contempladas en las Leyes y/o Reglamentos aplicables al obj[redacted] contrato, aún cuando no haya habido dolo o negligencia, liberando de cualquier responsabilidad a **LA UNIVERSIDAD**.

De igual forma **EL VENDEDOR** se obliga a tomar un seguro a su cargo y a favor de **LA UNIVERSIDAD**, para cubrir los riesgos derivad[redacted] entre ellos los de responsabilidad civil, daños a terceros en sus bienes o personas etc., el cual deberá de estar vigente hasta el cump[redacted] sus obligaciones plasmadas a su cargo en el presente, acordándose que en caso de no contar con dicho seguro, **EL VENDEDOR** se[redacted] responsable por dichos conceptos.

4

CUARTA.- EL VENDEDOR se compromete ante **LA UNIVERSIDAD** a entregar, y en su caso instalar, los bienes objeto del presente dentro del plazo señalado en la caratula del presente contrato, en la dependencia que **LA UNIVERSIDAD** designe. Al respecto queda establecido que **EL VENDEDOR** no podrá realizar entregas parciales y el plazo concedido es para realizar la entrega total de los bienes o servicios contratados.

En caso de retraso en el cumplimiento de lo establecido en el presente, por causas imputables a **EL VENDEDOR**, éste pagará a **LA UNIVERSIDAD** por concepto de pena el 1.5% de los bienes no entregados o instalados y de los servicios no realizados. Dicha cantidad se podrá deducir por **LA UNIVERSIDAD** de los pagos pendientes a su cargo y a favor de **EL VENDEDOR**.

Independientemente de la aplicación de la pena antes señalada **LA UNIVERSIDAD** podrá optar entre exigir el cumplimiento forzoso de las obligaciones del presente contrato, o darlo por rescindido.

Por causas justificadas y debidamente acreditadas a **LA UNIVERSIDAD**, la misma podrá, si lo considera conveniente, ampliar previa petición por escrito de **EL VENDEDOR**, el plazo de entrega contemplado en la presente cláusula y en cuyo caso deberá suscribirse un convenio modificatorio y deberá actualizarse la fianza correspondiente por parte de **EL VENDEDOR**, misma que se entregará a **LA UNIVERSIDAD** a la firma del convenio modificatorio.

QUINTA.- EL VENDEDOR queda obligado a realizar todo lo establecido en el presente de acuerdo a lo estipulado por las partes, para lo cual se responsabiliza hasta el cumplimiento de todas sus obligaciones.

SEXTA.- EL VENDEDOR dará aviso por escrito a **LA UNIVERSIDAD** cuando concluya con las obligaciones pactadas a su cargo en el presente, para que ésta última proceda a levantar un acta de entrega recepción por conducto de quien la misma señale.

SÉPTIMA.- Las partes acuerdan que **EL VENDEDOR** tiene prohibido:

a) Encomendar o subcontratar con otra persona la entrega o instalación de los bienes objeto del presente contrato, así como la cesión total o parcial de los derechos y obligaciones del mismo.
b) En su caso, hacer cambios estructurales en la o las instalaciones en donde se colocarán los bienes objeto del presente, sin la previa autorización por escrito de **LA UNIVERSIDAD,** estableciendo que en caso de no respetar lo antes señalado, **EL VENDEDOR** será responsable de los daños y perjuicios y la responsabilidad civil que dicho incumplimiento cause, lo anterior independientemente de la rescisión o cumplimiento forzoso del contrato.

OCTAVA.- EL VENDEDOR en tanto no se levante el acta de entrega recepción correspondiente, reconoce que **LA UNIVERSIDAD** no será responsable de la perdida (total o parcial), deterioro o maltrato de los bienes, materiales, herramientas o cualquier otro bien relacionado con el objeto del presente, ni aun en el supuesto de caso fortuito o fuerza mayor, ya que los mismos son responsabilidad directa de **EL VENDEDOR**, liberando a **LA UNIVERSIDAD** de cualquier responsabilidad que se pudiera derivar del presente concepto.

NOVENA.- Los servicios de entrega o, en su caso, de instalación de los bienes materia del presente contrato se ejecutarán durante días y horas hábiles de la o las dependencias universitarias en las cuales se entregarán los bienes materia del presente, acordando las partes que en caso de ser necesario realizar trabajos durante horas y días inhábiles, los mismos podrán llevarse a cabo, previa autorización por escrito que al efecto expida **LA UNIVERSIDAD**.

DÉCIMA.- La supervisión de lo establecido en el presente, estará a cargo de la Coordinación de Servicios Generales de la dependencia responsable o de la persona o las personas que esta última designe, quienes podrán inspeccionar en todo tiempo todo lo relacionado con los bienes, pudiendo en su caso, rechazar por escrito lo que no se ajuste a lo estipulado en el contrato y su Anexo "A".

Al respecto **EL VENDEDOR** se compromete a entregar los bienes nuevos y de primera calidad, según se establece en las especificaciones técnicas, siendo responsable de los daños y perjuicios, y la responsabilidad civil, que cause debido a la mala calidad de los mismos.

De existir inconformidad respecto a lo contemplado en esta cláusula, **LA UNIVERSIDAD** solicitará a **EL VENDEDOR** reemplazar a costa de esta última, los bienes defectuosos o no adecuados.

DÉCIMA PRIMERA.- EL VENDEDOR además de observar el cumplimiento de este contrato, estará obligado a lo siguiente:

a) Vigilar que el objeto del presente contrato sea de acuerdo a lo aprobado, y a las características especificaciones requeridas.
b) En su caso hacer la revisión detallada de la instalación de los bienes, rindiendo el informe correspondiente.
c) Tener en todo momento personal técnico capacitado para la dirección, supervisión e instalación y demás actividades relacionadas con el objeto materia de este contrato.
d) Estar al corriente de todas las contribuciones que se originen por el desempeño de su actividad.
e) Responder de la perdida, daño, robo o extravío de los bienes, hasta el momento en que se realice el acta de entrega recepción correspondiente, aún en el supuesto de que dichos bienes se encuentren en las instalaciones de **LA UNIVERSIDAD**.
f) Cumplir con todas las obligaciones derivadas de la ley, del presente y su Anexo "A".

DÉCIMA SEGUNDA.- LA UNIVERSIDAD podrá dar por terminado anticipadamente en cualquier momento el presente contrato, c
circunstancias imprevistas o razones de interés general, previa notificación por escrito a **EL VENDEDOR** con cuando menos 5 (cinco)
anticipación.

Adicionalmente, acuerdan las partes que **LA UNIVERSIDAD** podrá suspender los trabajos y/o pagos objeto del presente, en
presente alguno de los supuestos que a continuación se mencionan de manera enunciativa mas no limitativa:

a) En su caso cuando existan bienes y/o trabajos defectuosos o no adecuados, que no se reemplacen o corrijan, dentro de los 30 (treinta) días siguientes a la fecha en que **LA UNIVERSIDAD** lo haga del conocimiento de **EL VENDEDOR**.
b) Incumplimiento de **EL VENDEDOR** por no estar al corriente en el pago de las contribuciones que se generen por su operación o el pago de sus obligaciones directas e indirectas con su personal.
c) Por presentación de reclamación de cualquier naturaleza, si se llegara a formalizar, en contra de **LA UNIVERSIDAD** derivada del objeto del presente contrato.
d) Si **EL VENDEDOR** no entrega las fianzas a que se hace referencia en el presente contrato, dentro de los términos establecidos para tal efecto.
e) Si **EL VENDEDOR** cayera en insolvencia o se declara en concurso mercantil.
f) Por muerte o disolución de **EL VENDEDOR**, según corresponda.
g) En general por cualquier incumplimiento por parte de **EL VENDEDOR** a cualquiera de las obligaciones derivadas del presente contrato, su anexo o la ley.

A juicio de **LA UNIVERSIDAD** y una vez que se subsanen los problemas a que se refieren los incisos anteriores, se podrán reanudar los efectos y/o pagos o rescindir el presente contrato.

DÉCIMA TERCERA.- En caso de que se presente algún defecto o vicio oculto relacionado con el objeto del presente contrato, **EL VENDEDOR** será la responsable ante **LA UNIVERSIDAD** por los mismos.

DÉCIMA CUARTA.- La entrega, y en su caso instalación, de los bienes detallados en el presente contrato y su Anexo "A" deberá quedar terminada en el plazo que se consigna en la carátula del presente.

El plazo de terminación del presente instrumento solo podrá ser ampliado en caso de que haya modificaciones en lo establecido en el objeto del presente contrato, en caso fortuito o de fuerza mayor de conformidad a la ley o por mutuo acuerdo.

Para que el objeto del presente instrumento se pueda considerar como satisfecho se deberá haber cumplido con lo establecido en el contrato y su Anexo "A".

DÉCIMA QUINTA.- Las partes convienen en que **EL VENDEDOR** se compromete a cumplir con todas y cada una de las obligaciones derivadas de la relación laboral que imponen la Ley Federal del Trabajo, y demás ordenamientos legales aplicables a los patrones; por lo tanto **EL VENDEDOR** será el único responsable y obligado para con los trabajadores, ante todo tipo de autoridades ya sean administrativas o judiciales, Federales, Estatales o Municipales.

En consecuencia, **EL VENDEDOR** asume todas las responsabilidades como patrón con relación a los trabajadores que emplee, liberando de posibles indemnizaciones, demandas o cualquier reclamación que éstos iniciaran en contra de **LA UNIVERSIDAD**.

LA UNIVERSIDAD, no será responsable por ninguna reclamación que en contra de **EL VENDEDOR** presenten sus empleados o colaboradores, obligándose ésta última a sacar en paz y a salvo a **LA UNIVERSIDAD** de cualquier reclamación de esta naturaleza, ya sea laboral, administrativa, civil o penal, incluyéndose los accidentes de trabajo.

Asimismo, será obligación de **EL VENDEDOR** hacer la retención y entero de las contribuciones correspondientes de los trabajadores que emplee con motivo del presente contrato.

DÉCIMA SEXTA.- EL VENDEDOR otorgará a favor de **LA UNIVERSIDAD** las fianzas descritas en la carátula del presente contrato, expedidas por una compañía legalmente constituida y registrada, con oficinas en la ciudad de Guadalajara, Jalisco, y que se sujeten a la jurisdicción de los tribunales competentes de esta ciudad.

Adicionalmente **EL VENDEDOR** manifiesta expresamente lo siguiente:

(A) Su conformidad para que la fianza de cumplimiento se pague independientemente de que se interponga cualquier tipo de recurso ante instancias del orden administrativo o no judicial.
(B) Su conformidad para que la fianza que garantiza el cumplimiento del contrato, permanezca vigente durante la substanciación de todos los procedimientos judiciales o arbitrales y los respectivos recursos que se interpongan con relación al presente contrato, hasta que sea dictada resolución definitiva que cause ejecutoria por parte de la autoridad o tribunal competente.
(C) Su aceptación para que la fianza de cumplimiento permanezca vigente hasta que las obligaciones garantizadas hayan sido cumplidas en su totalidad a satisfacción de **LA UNIVERSIDAD**.

DÉCIMA SÉPTIMA.- Además de las causas previstas por la Ley, las partes convienen en que el presente contrato podrá ser rescindido por **LA UNIVERSIDAD** cuando **EL VENDEDOR** no haya cumplido con todas o alguna de las obligaciones que a su cargo se derivan de éste contrato, en especial si la entrega o instalación no cumple con las características pactadas.

Serán causas de rescisión del presente contrato las que a continuación se mencionan enunciativamente más no limitativamente:

a) Si **EL VENDEDOR**, por causas imputables a ella o a sus dependientes, no entrega los bienes, según lo acorado en anexo.
b) Si **EL VENDEDOR**, en su caso, no entrega los trabajos contratados totalmente terminados dentro del plazo señalado contrato y su anexo.

[redacted]

c) Si **EL VENDEDOR,** en su caso, suspende injustificadamente los trabajos objeto del presente o se niega a reparar o responder alguno que hubiere sido rechazado por **LA UNIVERSIDAD,** en un término de 30 (treinta) días.
d) Si **EL VENDEDOR** cayera en insolvencia o se declara en concurso mercantil.
e) Por muerte o disolución de **EL VENDEDOR**, según sea el caso.
f) En general por cualquier incumplimiento por parte de **EL VENDEDOR** a cualquiera de las obligaciones derivadas del presente contrato, su anexo o la ley.

En caso de incumplimiento por parte de **EL VENDEDOR** en cualquiera de las obligaciones previstas en este contrato **LA UNIVERSIDAD** podrá rescindir el contrato o exigir el cumplimiento del mismo.

Si **LA UNIVERSIDAD** opta por rescindir el contrato por causa imputable a **EL VENDEDOR,** está última, quedará obligada a cubrir los daños y perjuicios que por tal motivo ocasione a **LA UNIVERSIDAD,** los cuales no podrán ser inferiores al 20% (veinte por ciento) del monto total del presente instrumento.

DÉCIMA OCTAVA.- Acuerdan las partes que en caso de que el presente contrato incluya mantenimiento preventivo, mantenimiento correctivo y/o capacitación, las actividades relacionadas con los mismos se realizarán conforme lo determinen las partes.

DÉCIMA NOVENA.- Queda establecido que **EL VENDEDOR** no podrá ceder o transferir parcial o totalmente los derechos y las obligaciones derivadas del presente instrumento, sin el previo consentimiento por escrito de **LA UNIVERSIDAD,** siendo responsable de los daños y perjuicios que tal incumplimiento cause.

VIGÉSIMA.- Nada de lo previsto en este contrato ni de las acciones que se deriven de su suscripción, podrá considerarse o interpretarse para constituir o considerar a las partes y al personal de las mismas que colabore en la ejecución de este contrato como socios, agentes, representantes o empleados uno del otro, y ninguna de las disposiciones de este contrato será interpretada para forzar a la otra parte a asumir cualquier obligación o a actuar o pretender actuar como representante de la otra.

VIGÉSIMA PRIMERA.- El presente contrato, podrá ser modificado previo acuerdo por escrito entre las partes y durante la vigencia del mismo, apegándose a la normatividad aplicable, y a través de los instrumentos jurídicos correspondientes, obligándose las partes a las nuevas estipulaciones, a partir de la fecha de su firma.

VIGÉSIMA SEGUNDA.- Si alguna de las disposiciones contenidas en el presente contrato, llegara a declararse nula por alguna autoridad, tal situación no afectará la validez y exigibilidad del resto de las disposiciones establecidas en este contrato. Al respecto las partes negociarán de buena fe la sustitución o modificación mutuamente satisfactoria de la cláusula o cláusulas declaradas nulas o inválidas por otras en términos similares y eficaces.

En caso de que el presente contrato llegara a declararse nulo por la autoridad competente o el mismo se rescindiera por causa imputable a **EL VENDEDOR**, el mismo estará obligado a devolver a **LA UNIVERSIDAD** la o las cantidades que le hayan sido entregadas, más la actualización correspondiente conforme al Índice Nacional de Precios al Consumidor, tomando como base la fecha en que se realizó la primera entrega por parte de **LA UNIVERSIDAD** y la fecha en que sean devueltas las mismas, lo anterior independientemente de los daños y perjuicios que por tal motivo tenga derecho a reclamar a **LA UNIVERSIDAD**.

VIGÉSIMA TERCERA.- EL VENDEDOR se obliga a que los bienes serán nuevos y de la calidad señalada en las especificaciones del Anexo "A", y responderá por cualquier defecto en cualquiera de las partes de los bienes y accesorios objeto del presente, o por la instalación y puesta en marcha de los mismos.

La garantía está sujeta a que los bienes sean utilizados de acuerdo a las especificaciones y características de estos.

VIGÉSIMA CUARTA.- Ambas partes acuerdan que cualquier controversia relacionada con la interpretación, contenido o ejecución del presente contrato, se sujetará a lo establecido en el presente contrato y de manera supletoria a lo establecido en los documentos señalados a continuación y en el orden siguiente; en el anexo, las bases del procedimiento correspondiente, la propuesta presentada por **EL VENDEDOR**, la legislación federal, la universitaria y demás leyes aplicables.

En este sentido queda establecido que si existe alguna discrepancia en la información contenida en alguno de los documentos señalados en el párrafo anterior, siempre será aplicable la disposición que sea más favorable para **LA UNIVERSIDAD,** quedando sin efectos la disposición distinta.

VIGÉSIMA QUINTA.- Para todo lo relacionado con la interpretación y cumplimiento del presente contrato, las partes se someten voluntariamente a las leyes aplicables de la República Mexicana y a la jurisdicción y competencia de las autoridades de la ciudad de Guadalajara, Jalisco, renunciando a cualquier otro fuero o jurisdicción que pudiera corresponderles en virtud de su domicilio presente o futuro.

4

Las partes enteradas del contenido y alcance del presente contrato, manifiestan que en el mismo no existe mala fe, dolo [redacted] triplicado en la carátula del mismo, en compañía de los testigos, en la ciudad de Guadalajara, Jalisco.

[redacted]

initel

ANEXO "A"

Empresa: INITEL S.A. DE C.V. 1
R.F.C.: [redacted]
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD		DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
1	39	FG-200E-BDL-900-36 **Mca. FORTINET**	SOLUCIONUTM/NGFW TIPO 1 (1 UNIDAD)	$ 117,278.61	$ 4,573,865.79

Throughput de por lo menos 9 Gbps con la funcionalidad de firewall habilitada para trafico IPv4 y IPv6, independiente del tamaño del paquete

Soporte a por lo menos 2M conexiones simultaneas
Soporte a por lo menos 135K nuevas conexiones por segundo
Throughput de al menos 9 Gbps de VPN IPSec
Estar licenciado para, o soportar sin necesidad de licencia, 2K tuneles de VPN IPSec site-to-site simultaneos
Estar licenciado para, o soportar sin necesidad de licencia, 10K tuneles de clientes VPN IPSec simultaneos
Throughput de al menos 900 Mbps de VPN SSL
Soportar al menos 300 clientes de VPN SSL simultaneos
Soportar al menos 6000 Mbps de throughput de IPS
Soportar al menos 1000 Mbps de throughput de Inspección SSL
Throughput de al menos 1200 Mbps con las siguientes funcionalidades habilitadas simuttaneamente para todas las firmas que la solución de seguridad tenga debidamente activadas y operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado multiples oumeros de desempeño para cualquier de las funcionalidades, solamente el de valor mas pequeño sera aceptado.
Permitir gestionar al menos 64 Access Points
Tener al menos 14 interfaces 1 Gbps RJ45, 4 Gbps SFP, 2 Gbps para WAN
Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) par appliance
Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) par appliance
Debe de incluir un token fisico para autenticaciónde doble factor para la gestión del appliance o para el acceso VPN que debe ser de la misma marca propuesta
Debe de brindar soporte 36 meses del tipo 8x5, reemplazo siguiente dia habil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus, Botnet IP/Domain, AntiSpam y Filtrado Web

REQUISITOS MINIMOS DE FUNCIONALIDAD
Caracteristicas Generales
La solución debe consistir en una plataforma de protecciónde Red, basada en un dispositivo con funcionalidades de Firewall de Próxima generación (NGFW), asi coma consola de gestión y monitoreo. ;
Porfuncionalidades de NGFW se entiende: aplicaciones de reconocimiento, prevención de amenazas, identificación de usuarios y control granular de permisos;
Las funcionalidades de protecciónde red que conforman la plataforma de seguridad, puede ejecutarse en multiples dispositivos siempre que cum plan todos los requisitos de esta especificación;
La plataforma debe estar optimizada para aplicaciones de analisis de contenido en la capa 7;
Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;
La gestión del equipo debe ser compatible con acceso a traves de SSH, consola, web (HTIPS) y API abierta;
La gestión del equipos debe ser compatible a traves de la interfaz de administración Web en el mismo dispositivo de protecciónde la red
Los dispositivos de protecciónde red deben soportar 4094 VLANs Tags 802.1q;
Los dispositivos de protecciónde red deben soportar agregación de enlaces 802.3ad y LACP;
Los dispositivos de protecciónde red deben soportar Policy based routing y policy based forwarding;

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

inteLa

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

Los dispositivos de protecciónde red deben soportar encaminamiento de

multicast (PIM-SM y PIM-DM);
Los dispositivos de protecciónde red deben soportar DHCP Relay;
Los dispositivos de protecciónde red deben soportar DHCP Server;
Los dispositivos de protecciónde red deben soportar sFlow
Los dispositivos de protecciónde red deben soportar Jumbo Frames;
Los dispositivos de protecciónde red deben soportar sub-interfaces Ethernet

16gicas
Debe ser compatible con NAT dinamica (varios-a-1);
Debe ser compatible con NAT dinamica (muchos-a-muchos);
Debe soportar NAT estatica (l-a-1);
Debe admitir NAT estatica (muchos-a-muchos);
Debe ser compatible con NAT estatico bidireccional 1-a-1;
Debe ser compatible con la traducci6n de puertos (PAT);
Debe ser compatible con NAT Origen;
Debe ser compatible con NAT de destine;
Debe soportar NAT de origen y NAT de destino de forma simultanea:
Debe soportarTraducci6n de Prefijos de Red (NPTv6) o NAT66, para evitar

problemas de enrutamiento asirnetrico:
Debe ser compatible con NAT64 y NAT46;
Debe implementar el protocolo ECMP;
Debe soportar el balanceo de en lace hash por IP de origen;
Debe soportar el balanceo de en lace hash por IP de origen y destino;
Debe soportar balanceo de enlace por peso. En esta opción debe ser posible

definir el porcentaje de trafico que fluira a traves de cada uno de los en laces

Debe ser compatible con el balanceo en al menos tres en laces;
Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso

de instancias virtuales
Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos

por gran numero de sesiones, conexiones por segundo, cantidad de tuneles

establecidos en la VPN, CPU, memoria, estado del cluster, ataques y
estadisticas de uso de las interfaces de red
Enviar logs a sistemas de gestión externos simultaneamente:
Debe tener la opción de enviar logs a los sistemas de control externo a traves

de TCP y SSL;
Debe soporta protecciónContra la suplantaci6n de identidad (anti-spoofing);

Implementar la optimizaci6n del trafico entre dos dispositivos;
Para 1Pv4, soportar enrutamiento estatico y dinamico (RIPV2, OSPFv2 y BGP);

Para 1Pv6, soportar enrutamiento estatico y dinamico (OSPFv3);
Soportar OSPF graceful restart;
Los dispositivos de protecciÓndeben tener la capacidad de operar
simultaneamente en una unica instancia de servidor de seguridad, mediante

el uso de sus interfaces ffsicas en los siguientes modos: modo sniffer
(monitoreo y analisis de trafico de red), capa 2 (L2) y capa 3 (L3);
Debe ser compatible con el modo Sniffer para la inspección a traves del
puerto espejo del trafico de datos de la red;
Debe soportar modo capa - 2 (L2) para la inspección de datos en linea y la
visibilidad del trafico:
Debe soportar modo capa - 3 (L3) para la inspección de los datos de la
visibilidad en lfnea de trafico:
Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces
fisicas;
Soportar la configuración de alta disponibilidad active I pasivo y activo I
activo: En modo transparente;
Soportar la configuración de alta disponibilidad activo I pasivo y activo I
activo: En capa 3;
Soportar configuración de alta disponibilidad active I pasivo y activo I activo:

En la capa 3 y con al menos 3 dispositivos en el cluster;
La configuración de alta disponibilidad debe sincronizar: Sesiones;
La configuración de alta disponibilidad debe sincronizar: configuración ,
incluyendo, pero no limitados poHticas de Firewalls, NAT, QoS y objetos de la

red;

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	SUBTOTAL

La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN;
La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
En modo HA (Modo de alta disponibilidad) debe permitir la supervision de fallos de enlace;
Debe soportar la creación de sistemas virtuales en el mismo equipo;
Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;
Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes equipos;
La solución de gestión debe ser compatible con el acceso a traves de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
Debe aportar el control, la inspección y el descifrado de SSL para el trafico entrante (inbound) y la salida (outbound), y debe ser compatible con el control de certificados de forma individual dentro de cada sistema virtual, es decir, el aislamiento de la adición, eliminación y uso de los certificados directamente en cada sistema virtual (contextos);
• CONTROL POR POLITICA DE FIREWALL
Debe soportar controles de zona de seguridad
Debe contar con politicas de control por puerto y protocolo
Contar con politicas por aplicación, grupos estatrcos de aplicaciones, grupos dinamtcos de aplicaciones (en base a las caracteristicas y comportamiento de las aplicaciones) y categorias de aplicaciones
Control de politicas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad
Control de politica por código de pais (por ejemplo: BR, USA., UK, RUS)
Control, inspección y des encriptación de SSL por politica para el trafico entrante y la salida
Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada;
Debe descifrar las conexiones de entrada y salida de trafico negociadas con TLS 1.2;
Control de inspección y descifrado SSH por politica;
Debe permitir el bloqueo de archivos por su extension y permitir la identificación de archivo correcto por su tipo, incluso cuando se cambia el nombre de su extension;
Traffic shaping QoS basado en politicas (garantia de prioridad y maxima);
QoS basado en politicas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones;
Soporte para objetos y reglas IPV6;
Soporta objetos y reglas de multicast;
Debe ser compatible con al menos tres tipos de respuesta en las politicas de firewall: 'Drop' sin la notificación de bloqueo del usuario, 'Drop' con la notificación de bloqueo del usuario, Drop con opción de envío ICMP inalcanzable por la maquina fuente de trafico, TCP Reset para el cliente, RESET de TCP con el servidor o en ambos lados de la conexión;
Soportar la calendarización de politicas con el fin de activar y desactivar las reglas en tiempos predefinidos de forma automatica;
• CONTROL DE APLICACION
Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo
Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos
Reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no limitado a: el trafico relacionado peer-to-peer, redes sociales, acceso remote, actualización de software, protocolos de red, VoIP, audio, video,

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	SUBTOTAL
		Proxy, mensajería instantanea, compartición de archives, correo electrónico; Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs; Debe inspeccionar la carga util (payload) del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo; Debe detectar aplicaciones a traves del analisis del comportamiento del trafico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent; Identificar el uso de tacticas evasivas, es decir, debe tener la capacidad de very controlar las aplicaciones y los ataques con tacticas evasivas a traves de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante; Debe hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el trafico corresponde a la especificación del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTIP. La decodificación de protocolo tambien debe identificar las caractedsticas espedficas dentro de una aplicación, incluyendo, pero no limitado al intercambio de ficheros dentro de Webex Identificar el uso de tacttcas evasivas a traves de las comunicaciones cifradas; Actualización de la base de firmas de la aplicación de forma automatica: Limitar el ancho de banda (carga I descarga) utilizado por las aplicaciones traffic shaping), basado en IP de origen, usuarios y grupos; Los dispositivos de protecciónde red deben tener la capacidad de identificar al usuario de la red con la Integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario; Debe ser posible añadir multiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas; Debe ser compatible con multiples metodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación; Para mantener la seguridad de red eficiente debe ser soportar el control de las aplicaciones desconocidas y no solo en aplicaciones conocidas; Permitir la creación de forma nativa de fir mas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz grafica, sin la necesidad de la acción del fabricante La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP El fabricante debe permitir solicitar la inclusion de aplicaciones en su base de datos; Debe alertar al usuario cuando sea bloqueada una aplicación; Debe permitir la diferenciación de trafico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;		

SEMS
SECRETARÍA ADMINISTRATIVA

4 [redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

Debe permitir la diferenciacion de trafico de mensajeria instantanea (AIM,

Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas

para el mismo;
Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;
Debe permitir la diferenciacion de aplicaciones Proxies (psiphon, Freegate,

etc.) permitiendo granularidad de control/reglas para el mismo;
Debe ser posible la creación de grupos dinamicos de aplicaciones, basado en

las caracteristicas de las mismas, tales coma: Tecnologia utilizaca en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc)
Debe ser posible crear grupos dinarntcos de aplicaciones basados en caracteristicas de las mismas, tales como: nivel de riesgo de la aplicacion
Debe ser posible crear grupos estaticos de aplicaciones basadas en caracterfsticas de las mismas, tales como: Categoria de Aplicacion
•
PREVENCION DE AMENAZAS
Para proteger el entorno contra las ataques, deben tener modulo IPS, antivirus y anti-spyware integrado en el propio equipo;
Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archives maliciosos (antivirus y anti-spyware);
Las caracteristicas de IPS, antivirus y anti-spyware deben funcionar de forma

permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el

derecho a recibir actualizaciones o no existe un contrato de garantía del software con el fabricante;
Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad;
Debe implementar los siguientes tipos de acciones a las amenazas detectadas par IPS: permitir, permitir y generar registro, bloque, bloque del

IP del atacante durante un tiempo y enviar tcp-reset;
Las firmas deben ser capaces de ser activadas o desactivadas, o activadas solo en el modo de monitoreo;
Deben ser posible crear politicas para usuarios, grupos de usuarios, IP, redes

o zonas de seguridad
Excepciones por IP de origen o destino deben ser posibles en las reglas o en

cada una de las firmas;
Debe soportar granularidad en las politicas de IPS, Antivirus y Anti-Spyware,

permitiendo la creación de diferentes politicas par zona de seguridad, dirección de origen, dirección de destine, servicio y la combinación de todos

estos elementos
Debor permitir el bloqueo de vulnerabilidades
Debe permitir el bloqueo de exploits conocidos
Debe incluir la protecciónscontra ataques de denegacion de servicio
Debe tener los siguientes mecanismos de inspección IPS: Analisis de patrones

de estado de las conexiones;
Debe tener los siguientes mecanismos de inspeccion IPS: analisis de decodificación de protocolo;
Debe tener los siguientes mecanismos de inspeccion IPS: analisis para detectar anomalfas de protocolo;
Debe tener los siguientes mecanismos de inspección IPS: Analisis heuristico;

Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación

IP;
Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de

paquetes TCP;
Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formate incorrecto (malformed packets)
Debe ser inmune y capaz de prevenir los ataques basicos, tales como inundaciones SYN, ICMP, UDP, etc;
Detectar y bloquear los escaneos de puertos de origen;
Bloquear ataques realizados por gusanos (worms) conocidos;
Contar con firmas especfficas para la mitigacion de ataques DoS y DDoS;
Contar con firm as para bloquear ataques de desbordamiento de memoria

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

intermedia (buffer overflow);
Debe poder crear firmas personalizadas en la interfaz grafica del producto;

Debe permitir utilizar operadores de negación en la creacion de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración ;
Permitir bloqueo de virus y software espia en por lo menos los siguientes

protocolos: HTIP, FTP, SMB, SMTP y POP3;
Soportar el bloqueo de archives por tipo;
Identificar y bloquear la comunicación con redes de bots;
Registrar en la consola de supervision la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la apltcacion, el usuario, el origen y destine de las comunicaciones, ademas de las medidas

adoptadas por el dispositivo;
Debe ser compatible con la captura de paquetes (PCAP), mediante la firma

de IPS o control de aplicación;
Debe permitir la captura de paquetes por tipo de firma IPS para definir el

numero de paquetes capturados o permitir la captura del paquete que dio

lugar a la descripci6n, asf como su contexto, facilitando el anallsis forense y

la identificación de falsos positives
Debe tener la funci6n de protecciona traves de la resolución de direcciones

DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
Los eventos deben identificar el pais que origino la amenaza;
Debe incluir protecciónContra virus en contenido HTML y Java script, software espia (spyware) y gusanos (worms)
Tener protecciónContra descargas involuntarias mediante archives ejecutables maliciosos y HTIP
Debe permitir la configuración de diferentes politicas de control de amenazas y ataques basados en politicas de firewall considerando usuarios,

grupos de usuarios, origen, destine, zonas de seguridad, etc., es decir, cada

polftica de firewall puede tener una configuración diferente de IPS basada en

usuario, grupos de usuarios, origen, destine, zonas de seguridad
•
FILTRADO DE URL
Debe permitir especificar la politica por tiempo, es decir, la definición de

reglas para un tiempo o periodo determinado (dia, mes, afio, dfa de la semana y hara);
Debe ser posible crear polfticas para usuarios, IPs, redes, o zonas de seguridad
Debe tener la capacidad de crear politicas basadas en la visibilidad y el control de quien esta utilizando las URL esto mediante la integración con las

servicios de directorio Active Directory, y la base de datos local;
Debe tener la capacidad de crear politicas basadas en la visibilidad y el control de quien esta usando las URL que mediante la integración con las

servicios de directorio Active Directory, y la base de dates local, en modo de

proxy transparente y explicito;
Debe soportar la capacidad de crear politicas basadas en control por URL y

categorfa de URL
Debe tener la base de datos de URLs en cache en el equipo o en la nube del

fabricante, evitando retrasos de comunicación I validación de direcciones

URL;
Tener por lo menos 60 categorias de URL;
Debe tener la funcionalidad de exclusion de URLs por categoria
Permitir pagina de bloqueo personalizada;
Permitir el bloqueo y continuación que permite al usuario acceder a un sitio

bloqueado potencialmente informandole en la pantalla de bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir

teniendo acceso al sitio);
•

SEMS
SECRETARÍA ADMINISTRATIVA

4

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

IDENTIFICACION DE USUARIOS
Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quien esta usando dichas aplicaciones a traves de la integración con los servicios de directorio, a traves de la autenticaciónLDAP, Active Directory, E-directorio y base de datos local;
Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las polfticas / control basados en usuarios y grupos de usuarios;
Debe tener integración y soporte para Microsoft Active Directory para los siguientes sistemas operatives: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2;
Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las politicas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener lf mites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;
Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la politicas/control basados en usuarios y grupos de usuarios;
Debe permitir el control sin necesidad de instalación de software de cliente, al equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);
Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix
y Microsoft Terminal Server, lo que permite
una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos del LDAP I AD
Permitir la integración con tokens para la autenticaciónde usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.

Proporcionar al menos un token de forma nativa, lo que permite la autenticaciónde dos factores
•
QOS TRAFFIC SHAPING
Con el fin de controlar el trafico y aplicaciones cuyo con sumo puede ser excesivo (como YouTube, Ustream, etc.) y tienen un alto consume de ancho de banda, se requiere de la solución que, ademas de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda maxima cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio coma de video streaming;
Soportar la creación de políticas de QoS y Traffic Shaping par dirección de origen;
Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
Soportar la creación de polfticas de QoS y Traffic Shaping par usuario y grupo;
Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
Soportar la creación de polfticas de calidad de servicio y Traffic Shaping por puerto;

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa:	INITEL S.A. DE C.V.
R.F.C.:	[redacted] 1
Dirección:	[redacted] 3
Teléfono:	[redacted] 5
web:	[redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	SUBTOTAL

QoS debe permitir la definición de trafico con ancho de banda garantizado;

QoS debe permitir la definición de trafico
con maxima ancho de banda;
QoS debe permitir la definición de cola de prioridad;
Soportar la priorización de protocolo en tiempo real de voz (VoIP) como
H.323, SIP, SCCP, MGCP y aplicaciones coma Skype;
Soportar marcación de paquetes DiffServ, incluso por aplicación;
Soportar la modificación de los valores de DSCP para Diffserv;
Soportar priorización de trafico utilizando información de Tipo de Servicio

(Type of Service)
Proporcionar estadisticas en tiempo real para clases de QoS y Traffic Sha pig;

Debe soportar QoS (traffic-shaping) en la interfaz agregada o redundantes;

•
FILTRO DE DATOS
Permite la creación de filtros para archivos y dates predefinidos;
Los archivos deben ser identificados por tamafio y tipo;
Permitir identificar y opcionalmente prevenir la transferencia de varios tipos

de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTIP, FTP,

SMTP, etc.);
Soportar la identificación de archivos comprimidos o la aplicación de politicas

sabre el contenido de este tipo de archivos;
Soportar la identificación de archives cifrados y la aplicación de polittcas
sabre el contenido de este tipo de archivos;
Permitir identificar y opcionalmente prevenir la transferencia de información

sensible, incluyendo, pero no limitado a, numero de tarjeta de credito,
permitiendo la creación de nuevos tipos de datos a traves de expresiones

regulares;
•
GEO LOCALIZACION
Soportar la creación de politticas por geo-localización, permitiendo bloquear

el trafico de cierto Pais/Parses;
Debe permitir la visualizaciónde los pafses de origen y destino en los
registros de acceso;
Debe permitir la creación de zonas geograficas por medio de la interfaz
grafica de usuario y la creación de politicas usando las mismas.
•
VPN
Soporte VPN de sitio a sitio y cliente a sitio;
Soportar VPN IP Sec;
Soportar VPN SSL;
la VPN IPSec debe ser compatible con 3DES;
La VPN IPSec debe ser compatible con la autenticaciónMOS y SHA-1;
la VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2,
Grupo 5 y el Grupo 14;
La VPN IPSec debe ser compatible con Internet Key Exchange (IKEvl y v2);

la VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced
Encryption Standard);
La VPN IPSec debe ser compatible con la autenticación a traves de
certificados IKE PKI
Debe tener interoperablilidad con los siguientes fabricantes: Cisco, Check

Point, Juniper, Palo Alto Networks, Forti net, SonicWall;
Soportar VPN para 1Pv4 e 1Pv6, asi como el trafico 1Pv4 dentro de tuneles

IPv6 IPSec
Debe permitir activar y desactivar tuneles IPSec VPN desde la interfaz grafica

de la solución, lo que facilita el proceso troubleshooting;
La VPN SSL debe soportar que el usuario pueda realizar la conexión a traves

de cliente instalado en el sistema operativo de su maquina o a traves de la

interfaz web;
Las caracteristicas de VPN SSL se deben cumplir con o sin el uso de agentes;

Debe permitir que todo el trafico de los usuarios VPN remotos fluya hacia el

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

tunel VPN, previniendo la comunicación directa con dispositivos locales
coma un proxy;
Asignación de DNS en la VPN de cliente remoto;
Debe permitir la creación de políticas de control de aplicaciones, IPS,
antivirus, filtrado de URL y AntiSpyware para el trafico de clientes remotos

conectados a la VPN SSL;
Suportar autenticaciónvia AD/LDAP, Secure id, certificado y base de usuarios

local;
Suportar lectura y revision de CRL (lista de revocación de certificados);
Permitir la aplicación de poHticas de seguridad y visibilidad para las
aplicaciones que circulan dentro de tuneles SSL;
Debe permitir que la conexión a la VPN se establece de la siguiente manera:

Antes de que el usuario se autentique en su estación
Deberfa permitir la conexión a la VPN se establece de la siguiente manera:

Oespues de la autenticaciónde usuario en la estación;
Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo

demanda de los usuarios;
Debera mantener una conexión segura con el portal durante la sesión;
El agente de VPN SSL o IPSEC cliente a sitio debe ser compatible con al
menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y

64 bits) y Mac OS X (v10.10 o superior);
•
WIRELESS CONTROLLER
Debera gestionar de manera centralizada puntos de acceso del mismo
fabricante de la solución ofertada
Soportar servicio del servidor DHCP por SSID para proporcionar direcciones

IP a los clientes malambrtcos
Soporte 1Pv4 e 1Pv6 por SSID
Permitir elegir si el trafico de cada SS10 se enviara a la controladora o
directamente por la interfaz de punto de acceso en una VLAN dada
Permitir definir que redes se accaden a traves de la controladora y que redes

seran accedidas directamente por la interfaz del Access Point
Soportar monitoreo y supresión de puntos de acceso indebidos
Proporcionar autenticaciónа la red inalambrica a traves de bases de datos

externas, tales como LDAP o RADIUS
Permitir autenticar a los usuarios de la red inalambrica de manera
transparente en dominios Windows
Pérmitir la visualizaciónde los dispositivos inalambricos conectados por
usuario
Permitir la visualizaciónde los dispositivos inalambricos conectados por IP

Permitir la visualizaciónde los dispositivos inalarnbricos conectados por tipo

de autenticación
Permitir la visualizaciónde los dispositivos inalambricos conectados por
canal
Permitir la visualizaciónde los dispositivos inalarnbricos conectados por
ancho de banda usado
Permitir la visualizaciónde los dispositivos inalambricos conectados por
potencia de la señal
Permitir la visualizaciónde los dispositivos inalarnbricos conectados por
tiempo de asociación
Debe soportar Fast Roaming en autenticacióncon portal cautivo
Debe soportar configuración de portal cautivo por SSID
Permitir bloqueo de trafico entre los clientes conectados a un SSID y AP
espedfico
Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID,
usando un algoritmo AES y lo TKIP.
Debe ser compatible con el protocolo 802.lx RADIUS
La controladora tnalarnbrica debera permitir configurar los para metros de

radio como banda y canal
La controladora debera perrnitir metodos de descubrimiento de puntos de

acceso de manera automatica
La controladora debera permitir rnetcdos de descubrimiento de puntos de

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

acceso por IP estatica
La controladora debera permitir metodos de descubrimiento de puntos de

acceso por DHCP
La controladora debera permitir metodos de descubrimiento de puntos de

acceso por dns
La controladora debera permitir metodos de descubrimiento de puntos de

acceso por broadcast
La controladora debera permitir metodos de descubrimiento de puntos de

acceso par multicast
La controladora inalambrica debera suministrar una lista de Puntos de
Acceso autorizados y puntos de acceso indebidos (Rogue)
La controladora debera contar con proteccion contra ataques ARP Poisoning

en el controlador Inalarnbrico
La controladora debera contar con mecanismos de protecciónde tramas de

administración de acuerdo a las especificaciones de la alianza Wi-Fi y
estandar 802.llac
La controladora inalambrtca debera tener de manera integrada sistema de

deteccion de intrusion inalambrica contra ataques tipo ASLEAP
La controladora inalambrica debera tener de manera integrada sistama de

deteccion de intrusion inalambrica contra ataques tipo Association Frame

Flooding
La controladora inalarnbrica debera tener de manera integrada sistema de

deteccion de intrusion inalambrica contra ataques tipo Authentication Frame

Flooding
La controladora tnalarnbrtca debera tener de manera integrada sistema de

detección de intrusion inalambrica contra ataques tipo Broadcasting De-
authentication
la controladora inalambrica debera tener de.manera integrada sistema de

detección de intrusion inalambrica contra ataques tipo EAPOL Packet
flooding
La controladora inalambrica debera tener de manera integrada sistema de

deteccion de intrusion inalambrica contra ataques tipo Invalid MAC OUI
La controladora inatarnbrtca debera tener de manera integrada sistema de

deteccion de intrusion Inalambrtca contra ataques tipo Long Duration Attack

La controladora inalambrica debera tener de manera integrada sistema de

deteccion de intrusion inalambrica contra ataques tipo Null SSID probe
response
La controladora inalambrtca debera tener de manera integrada sistema de

deteccion de intrusion tnalambrica contra ataques tipo Spoofed De-
authentication
La controladora inalambrica debera tener de manera integrada sistema de

deteccion de intrusion inalambrtca contra ataques tipo Weak WEP IV
Detection
La controladora tnalambrica debera tener de manera integrada sistema de

detección de intrusion inalambrica contra ataques tipo Wireless Bridge
Implementar canales de auto-aprovisionamiento de los puntos de acceso con

el fin de minimizar la interferencia entre ellas
Permitir seleccionar el dia y hara en que se producira la optimización de
aprovisionamiento automatics de canales en los puntos de acceso
La controladora inalambrica debe permitir agendar horarios para determinar

en que memento la red inalambrica (SSID) se encuentra disponible
La controladora inalarnbrica debe ofrecer funcionalidad de Firewall integrado

UTM basado en la identidad del usuario
Permitir configurar el numero maximo de clientes que pueden ser permitidos

par SSID
Permitir configurar el numero maximo de clientes que pueden ser permitidos

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initela

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	SUBTOTAL

par punto de acceso
Permitir configurar el numero maxi mo de clientes qua pueden ser permitidos

par Radio
La controladora debe permitir crear, administrar y autorizar las redes
inalarnbricas mesh
Ofrecer un mecanismo de creacion automatica y/o manual de usuarios
visitantes y contrasefias, que puedan ser enviados par correo electronico o

SMS a los usuarios, con ajuste de tiempo de expiraci6n de la contrasef\a
La comunicacion entre la controladora y el punto de acceso inalarnbrico
pueda ser realizada de forma cifrada utilizando protocolo DTLS
Debe tener un mecanismo de ajuste autornatlco de potencia de la serial con

el fin de reducir la interferencia entre canales entre dos puntos de acceso

administrados
Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de
acceso
Proporcionar un mecanismo de balanceo de trafico/usuarios entre
frecuencias y/o radios de los Puntos de Acceso
Debe permitir la identificación del firmware utilizado por cada punto de
acceso gestionado y permitir la actualizaci6n a traves de la interfaz grafica.

Permitir que sean deshabilitados clientes inalarnbricos que tengan baja tasa

de transmisi6n
Permitir ignorar a los clientes inalambricos que tienen serial debti,
estableciendo un umbral de serial a partir de la cual los clientes son
ignorados
la controladora debe permitir configurar el valor de Short Guard Interval
para 802.lln y 802.llac en 5 GHz
Debe permitir seleccionar individualmente para cada punto de acceso los

SSID que van a ser propagados
Debe permitir asociación dinamtcas
de VIANs a los usuarios autenticados en
un SSID especifico mediante protocolo RADIUS
Debe permitir asociación dinamica de VIANs a los usuarios autenticados en

un SSID especifico mediante vian pooling
Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo
inalambnco
la controladora inalarnbrica debe permitir identificar los clientes WIFI que

presenten algun riesgo basado en aplicaciones
la controladora inalambrica debe permitir identificar los clientes WiFi que

presenten algun riesgo basado en dirección de destino
la controladora inalambrica debe permitir identificar los clientes WIFI que

presenten algun riesgo basado en amenaza
la controladora inalarnbrica debe permitir identificar los clientes WIFI que

presenten algun riesgo basado en sesiones
la controladora inalambrica debe soportar una licencia que permita al menos

10000 firmas de aplicaciones para reconocimiento de trafico
El controlador inalambrico debe tener interface de administraci6n integrado

en el mismo equipo
El controlador inalambnco debe soportar la funcionalidad de Fast-roaming

para enlaces mesh entre el node secundario y nodes principales
la controladora inalambrica debera soportar aceleraci6n de trafico del
protocolo CAPWAP a traves de un procesador de red de propósito espedfico

la controladora inalambrica debera soportar aceleraci6n de tunnel de trafico

de puente tnalambnco a traves de un procesador de red de propósito
espedfico
la controladora inalarnbrica debe soportar protocolo LLDP
Debe permitir tecnica de detección de APs intrusos On-wire a traves de
dirección MAC exacta
Debe permitir tecnica de detección de APs intrusos On-wire a traves de
dirección MAC Adyacente
Debe permitir la visualizaciónde los usuarios conectados an forma de

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initelo

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD		DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
			topologia 16gica de red representando la cantidad de dates transmitidos y recibidos la controladora inalarnbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado La controladora malambrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas la controladora inalambrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada Debera soportar la conversion de Multicast a Unicast para mejorar el rendimiento del tiempo de aire		
2	28	FG-400D-BDL-900-36 **Mca. FORTINET**	SOLUCIONUTM/NGFW TIPO 1 (1 UNIDAD) Throughput de por lo menos 16 Gbps con la funcionalidad de firewall habilitada para trafico 1Pv4 y 1Pv6, independiente del tamafio del paquete Soporte a por lo menos 4M conexiones simultaneas Soporte a por lo menos 200K nuevas conexiones por segundo Throughput de al menos 14 Gbps de VPN IPSec Estar licenciado para, o soportar sin necesidad de licencia, 2K tuneles de VPN IPSec site-to-site simultaneos Estar licenciado para, o soportar sin necesidad de licencia, 50K tuneles de clientes VPN IPSec simultaneos Throughput de al menos 350 Mbps de VPN SSL Soportar al menos 500 clientes de VPN SSL simultaneos Soportar al menos 2800 Mbps de throughput de IPS Soportar al menos 1900 Mbps de throughput de Inspecci6n SSL Throughput de al menos 1500 Mbps con las siguientes funcionalidades habilitadas simuttaneamente para todas las firmas que la solución de seguridad tenga debidamente activadas y operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado multiples oumeros de desempefio para cualquier de las funcionalidades, solamente el de valor mas pequefio sera aceptado. Permitir gestionar al menos 256 Access Points Tener al menos 8 interfaces 1 Gbps RJ45, 8 interfaces de 1 Gbps SFP, 2 interfaces Gbps para gestion Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales 16 logicos (Contextos) par appliance Soporte a por lo menos 10 sistemas virtuales logicos (Contextos) par appliance Debe de incluir un token fisico para autenticaciónde doble factor para la gestión del appliance o para el acceso VPN que debe ser de la misma marca propuesta Debe de brindar soporte 36 meses del tipo 8x5, reemplazo siguiente dia habil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus, Botnet IP/Domain, AntiSpam y Filtrado Web REQUISITOS MINIMOS DE FUNCIONALIDAD Caracteristicas Generales La solución debe consistir en una plataforma de protecciónde Red, basada en un dispositivo con funcionalidades de Firewall de Próxima generación (NGFW), asi coma consola de gestión y monitoreo. ;	$ 195,464.35	$ 5,473,001.80

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Porfuncionalidades de NGFW se entiende: aplicaciones de reconocimiento, prevenci6n de amenazas, identificación de usuarios y control granular de permisos; Las funcionalidades de protecciónde red que conforman la plataforma de seguridad, puede ejecutarse en multiples dispositivos siempre que cum plan todos los requisites de esta especificaci6n; La plataforma debe estar optimizada para aplicaciones de analisis de contenido en la capa 7; Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación; La gestión del equipo debe ser compatible con acceso a traves de SSH, consola, web (HTIPS) y API abierta; La gestión del equipos debe ser compatible a traves de la interfaz de administraci6n Web en el mismo dispositivo de protecciónde la red Los dispositivos de protecciónde red deben soportar 4094 VLANs Tags 802.lq; Los dispositivos de protecciónde red deben soportar agregaci6n de enlaces 802.3ad y LACP; Los dispositivos de protecciónde red deben soportar Policy based routing y policy based forwarding; Los dispositivos de protecciónde red deben soportar encaminamiento de multicast (PIM-SM y PIM-OM); Los dispositivos de protecciónde red deben soportar DHCP Relay; Los dispositivos de protecciónde red deben soportar DHCP Server; Los dispositivos de protecciónde red deben soportar sFlow Los dispositivos de protecciónde red deben soportar Jumbo Frames; Los dispositivos de protecciónde red deben soportar sub-interfaces Ethernet 16gicas Debe ser compatible con NAT dinamica (varios-a-1); Debe ser compatible con NAT dinamica (muchos-a-muchos); Debe soportar NAT estatica (l-a-1); Debe admitir NAT estatica (muchos-a-muchos); Debe ser compatible con NAT estatico bidireccional 1-a-1; Debe ser compatible con la traducci6n de puertos (PAT); Debe ser compatible con NAT Origen; Debe ser compatible con NAT de destine; Debe soportar NAT de origen y NAT de destino de forma simultanea: Debe soportarTraducci6n de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimetrico: Debe ser compatible con NAT64 y NAT46; Debe implementar el protocolo ECMP; Debe soportar el balanceo de en lace hash por IP de origen; Debe soportar el balanceo de en lace hash por IP de origen y destine; Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de trafico que fluira a traves de cada uno de los en laces.		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initelo

Empresa:	INITEL S.A. DE C.V.
R.F.C.:	[redacted] 1
Dirección:	[redacted] 3
Teléfono:	[redacted] 5
web:	[redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Debe ser compatible con el balanceo en al menos tres enlaces;		
		Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales		
		Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran numero de sesiones, conexiones por segundo, cantidad de tuneles establecidos en la VPN, CPU, memoria, estado del cluster, ataques y estadfsticas de uso de las interfaces de red		
		Enviar logs a sistemas de gestión externos simultaneamente:		
		Debe tener la opción de enviar logs a los sistemas de control externo a traves de TCP y SSL;		
		Debe soporta protecciónContra la suplantaci6n de identidad (anti-spoofing);		
		Implementar la optimizaci6n del trafico entre dos dispositivos;		
		Para 1Pv4, soportar enrutamiento estatico y dinarnico (RIPv2, OSPFv2 y BGP);		
		Para 1Pv6, soportar enrutamiento estatico y dinarnico (OSPFv3);		
		Soportar OSPF graceful restart;		
		Los dispositivos de protecciódeben tener la capacidad de operar simultaneamente en una unica instancia de servidor de seguridad, mediante el uso de sus interfaces ffsicas en los siguientes modos: modo sniffer (monitoreo y anallsis de trafico de red), capa 2 (L2) y capa 3 (L3);		
		Debe ser compatible con el modo Sniffer para la inspección a traves del puerto espe]o del trafico de datos de la red;		
		Debe soportar modo capa -2 (L2) para la inspección de datos en linea y la visibilidad del trafico:		
		Debe soportar modo capa -3 (L3) para la inspección de los datos de la visibilidad en lfnea de trafico:		
		Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces fisicas;		
		Soportar la configuración de alta disponibilidad active l pasivo y activo l active: En modo transparente;		
		Soportar la configuración de alta disponibilidad activo l pasivo y activo l activo: En capa 3;		
		Soportar configuración de alta disponibilidad active l pasivo y activo l activo: En la capa 3 y con al menos 3 dispositivos en el cluster;		
		La configuración de alta disponibilidad debe sincronizar: Sesiones;		
		La configuración de alta disponibilidad debe sincronizar: configuración, Incluyendo, pero no limitados poHticas de Firewalls, NAT, QoS y objetos de la red;		
		La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN;		
		La configuración de alta disponibilidad debe sincronizar: Tablas FIB;		
		En modo HA (Modo de alta disponibilidad) debe permitir la supervision de fallos de enlace;		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa:	INITEL S.A. DE C.V.
R.F.C.:	[redacted] 1
Dirección:	[redacted] 3
Teléfono:	[redacted] 5
web:	[redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	SUBTOTAL
		Debe ser compatible con el balanceo en al menos tres en laces; Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran numero de sesiones, conexiones por segundo, cantidad de tuneles establecidos en la VPN, CPU, memoria, estado del cluster, ataques y estadfsticas de uso de las interfaces de red Enviar logs a sistemas de gestión externos simultaneamente: Debe tener la opción de enviar logs a los sistemas de control externo a traves de TCP y SSL; Debe soporta protecciónContra la suplantaci6n de identidad (anti-spoofing); Implementar la optimizaci6n del trafico entre dos dispositivos; Para 1Pv4, soportar enrutamiento estatico y dinarnico (RIPv2, OSPFv2 y BGP); Para 1Pv6, soportar enrutamiento estatico y dinarnico (OSPFv3); Soportar OSPF graceful restart; Los dispositivos de protecciódeben tener la capacidad de operar simultaneamente en una unica instancia de servidor de seguridad, mediante el uso de sus interfaces ffsicas en los siguientes modos: modo sniffer (monitoreo y anallsis de trafico de red), capa 2 (L2) y capa 3 (L3); Debe ser compatible con el modo Sniffer para la inspección a través del puerto espe]o del trafico de datos de la red; Debe soportar modo capa - 2 (L2) para la inspección de datos en linea y la visibilidad del trafico: Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en lfnea de trafico: Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces fisicas; Soportar la configuración de alta disponibilidad active l pasivo y activo l active: En modo transparente; Soportar la configuración de alta disponibilidad activo l pasivo y activo l activo: En capa 3; Soportar configuración de alta disponibilidad active l pasivo y activo l activo: En la capa 3 y con al menos 3 dispositivos en el cluster; La configuración de alta disponibilidad debe sincronizar: Sesiones; La configuración de alta disponibilidad debe sincronizar: configuración , Incluyendo, pero no limitados poHticas de Firewalls, NAT, QoS y objetos de la red; La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN; La configuración de alta disponibilidad debe sincronizar: Tablas FIB; En modo HA (Modo de alta disponibilidad) debe permitir la supervision de fallos de enlace;		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

inite

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	SUBTOTAL
		Debe soportar la creación de sistemas virtuales en el mismo equipo; Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribuci6n de la carga entre los diferentes contextos; Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes equipos; La solución de gestión debe ser compatible con el acceso a traves de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportaci6n de configuración de sistemas virtuales (contextos) por ambos tipos de acceso; Debe aportar el control, la inspección y el descifrado de SSL para el trafico entrante (inbound) y la salida (outbound), y debe ser compatible con el control de certificados de forma individual dentro de cada sistema virtual, es decir, el aislamiento de la adición, eliminación y uso de los certificados directamente en cada sistema virtual (contextos); • CONTROL POR POLITICA DE FIREWALL Debe soportar controles de zona de seguridad Debe contar con politicas de control por puerto y protocolo Contar con politicas por aplicación, grupos estatrcos de aplicaciones, grupos dlnamtcos de aplicaciones (en base a las caracteristicas y comportamiento de las aplicaciones) y categorias de aplicaciones Control de politicas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad Control de politica por código de pais (por ejemplo: BR, USA, UK, RUS) Control, inspección y des encriptación de SSL por polftica para el trafico entrante y la salida Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada; Debe descifrar las conexiones de entrada y salida de trafico negociadas con TLS 1.2; Control de inspección y descifrado SSH por politica; Debe permitir el bloqueo de archivos por su extensión y permitir la identificación de archivo correcto por su tipo, incluso cuando se cambia el nombre de su extension; Traffic shaping QoS basado en politicas (garantia de prioridad y maxima); QoS basado en politicas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones; Soporte para objetos y reglas IPV6; Soporte objetos y reglas de multicast; Debe ser compatible con al menos tres tipos de respuesta en las politicas de firewall: 'Drop' sin la notificaci6n de bloqueo del usuario, 'Drop' con la notificaci6n de bloqueo del usuario, Drop con opción de envlo ICMP		

SEMS
SECRETARÍA ADMINISTRATIVA

[redacted] 4

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		inalcanzable por la maquina fuente de trafico, TCP Reset para el cliente, RESET de TCP con el servidor o en ambos lados de la conexión; Soportar la calendarizaci6n de politicas con el fin de activar y desactivar las reglas en tiempos predefinidos de forma automatica: • CONTROL DE APLICACION Los dispositivos de protecciónde red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos Reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no limitado a: el trafico relacionado peer-to-peer, redes sociales, acceso remote, actualizaci6n de software, protocolos de red, VoIP, audio, video, Proxy, mensajeria instantanea, compartici6n de archives, correo electr6nico; Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs; Debe inspeccionar la carga util (payload) del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo; Debe detectar aplicaciones a traves del analisis del comportamiento del trafico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent; Identificar el uso de tacticas evasivas, es decir, debe tener la capacidad de very controlar las aplicaciones y los ataques con tacticas evasivas a traves de las comunicaciones cifradas, tales como Skype y la utilizaci6n de la red Tor Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante; Debe hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el trafico corresponde a la especificaci6n del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTIP. La decodificación de protocolo tambien debe identificar las caractedsticas espedficas dentro de una aplicación; Incluyendo, pero no limitado al intercambio de ficheros dentro de Webex Identificar el uso de tacttcas evasivas a traves de las comunicaciones cifradas; Actualizaci6n de la base de firmas de la aplicación de forma automatica:		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V. 1
R.F.C.: [redacted]
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	SUBTOTAL
		Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones traffic shaping), basado en IP de origen, usuarios y grupos; Los dispositivos de protecciónde red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario; Debe ser posible añadir multiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas; Debe ser compatible con multiples metodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación; Para mantener la seguridad de red eficiente debe ser soportar el control de las aplicaciones desconocidas y no solo en aplicaciones conocidas; Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz grafica, sin la necesidad de la acción del fabricante La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS- SQL, IMAP, DNS, LDAP, SSL y RTSP El fabricante debe permitir solicitar la inclusion de aplicaciones en su base de dates; Debe alertar al usuario cuando sea bloqueada una aplicación; Debe permitir la diferenciación de trafico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo; Debe permitir la diferenciacion de trafico de mensajeria Instantanea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo; Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video; Debe permitir la diferenciacion de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo; Debe ser posible la creación de grupos dinamicos de aplicaciones, basado en las caracteristicas de las mismas, tales coma: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc) Debe ser posible crear grupos dinarntcos de aplicaciones basados en caracteristicas de las mismas, tales como: nivel de riesgo de la aplicacion		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Debe ser posible crear grupos estaticos de aplicaciones basadas en caracterfsticas de las mismas, tales como: Categoria de Aplicacion • PREVENCION DE AMENAZAS Para proteger el entorno contra las ataques, deben tener modulo IPS, antivirus y anti-spyware integrado en el propio equipo; Debe incluir firmas de prevenci6n de intrusiones (IPS) y el bloqueo de archives maliciosos (antivirus y anti-spyware); Las caracteristicas de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no existe un contrato de garantfa del software con el fabricante; Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad; Debe implementar los siguientes tipos de acciones a las amenazas detectadas par IPS: permitir, permitir y generar registro, bloque, bloque del IP del atacante durante un tiempo y enviar tcp-reset; Las firmas deben ser capaces de ser activadas o desactivadas, o activadas solo en el modo de monitoreo; Deben ser posible crear politicas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas; Debe soportar granularidad en las politicas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes politicas par zona de seguridad, dirección de origen, dirección de destine, servicio y la combinaci6n de todos estos elementos Deber permitir el bloqueo de vulnerabilidades Debe permitir el bloqueo de exploits conocidos Debe incluir la protecciónContra ataques de denegacion de servicio Debe tener los siguientes mecanismos de inspección IPS: Analisis de patrones de estado de las conexiones; Debe tener los siguientes mecanismos de inspeccion IPS: analisis de decodificación de protocolo; Debe tener los siguientes mecanismos de inspeccion IPS: analisis para detectar anomalfas de protocolo; Debe tener los siguientes mecanismos de inspección IPS: Analisis heuristico; Debe tener los siguientes mecanismos de inspección IPS: Desfragmentaci6n IP; Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP; Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets) Debe ser inmune y capaz de prevenir los ataques basicos, tales como inundaciones SYN, ICMP, UDP, etc; Detectar y bloquear los escaneos de puertos de origen;		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initelo

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	SUBTOTAL
		Bloquear ataques realizados por gusanos (worms) conocidos; Contar con firmas especfficas para la rnitigacion de ataques DoS y DDoS; Contar con firm as para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow); Debe poder crear firmas personalizadas en la interfaz grafica del producto; Debe permitir utilizar operadores de negaci6n en la creacion de firmas. personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración ; Permitir bloqueo de virus y software espia en por lo menos los siguientes protocolos: HTIP, FTP, SMB, SMTP y POP3; Soportar el bloqueo de archives por tipo; Identificar y bloquear la comunicaci6n con redes de bots; Registrar en la consola de supervision la siguiente informaci6n sobre amenazas concretas: El nombre de la firma o el ataque, la apltcacion, el usuario, el origen y destine de las comunicaciones, adernas de las medidas adoptadas por el dispositivo; Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación; Debe permitir la captura de paquetes por tipo de firma IPS para definir el nurnero de paquetes capturados o permitir la captura del paquete que dio lugar a la descripci6n, asf como su contexto, facilitando el analisis forense y la identificación de falsos positives Debe tener la funci6n de protecci6na traves de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos; Los eventos deben identificar el país que origino la amenaza; Debe incluir protecci6ncontra virus en contenido HTML y Java script, software espia (spyware) y gusanos (worms) Tener protecci6ncontra descargas involuntarias mediante archives ejecutables maliciosos y HTIP Debe permitir la configuración de diferentes politicas de control de amenazas y ataques basados en politicas de firewall considerando usuarios, grupos de usuarios, origen, destine, zonas de seguridad, etc., es decir, cada polftica de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destine, zonas de seguridad • FILTRADO DE URL Debe permitir especificar la politica por tiempo, es decir, la definición de reglas para un tiempo o periodo determinado (dia, mes, afio, dfa de la semana y hara); Debe ser posible crear polfticas para usuarios, IPs, redes, o zonas de seguridad Debe tener la capacidad de crear politicas basadas en la visibilidad y el		

SEMS
SECRETARÍA ADMINISTRATIVA

4

initel

Empresa: INITEL S.A. DE C.V. 1
R.F.C.: [redacted]
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	SUBTOTAL
		control de quien esta utilizando las URL esto mediante la integración con las servicios de directorio Active Directory, y la base de datos local; Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quien esta usando las URL que mediante la integración con las servicios de directorio Active Directory, y la base de dates local, en modo de proxy transparente y explicito; Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL Debe tener la base de datos de URLs en cache en el equipo o en la nube del fabricante, evitando retrasos de comunicaci6n I validaci6n de direcciones URL; Tener por lo menos 60 categorías de URL; Debe tener la funcionalidad de exclusion de URLs por categoria Permitir pagina de bloqueo personalizada; Permitir el bloqueo y continuaci6n (que permite al usuario acceder a un sitio bloqueado potencialmente inforrnandole en la pantalla de bloqueo y permitiendo el uso de un bot6n Continuar para que el usuario pueda seguir teniendo acceso al sitio); • IDENTIFICACION DE USUARIOS Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quien esta usando dichas aplicaciones a traves de la integración con los servicios de directorio, a través de la autenticaciónLDAP, Active Directory, E-directorio y base de datos local; Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las polfticas / control basados en usuarios y grupos de usuarios; Debe tener integración y soporte para Microsoft Active Directory para los siguientes sistemas operativos: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2; Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener lf mites licenciados de usuarios o cualquier restricci6n de uso como, pero no limitado a, utilizaci6n de sistemas virtuales, segmentos de red, etc; Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios; Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y		

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa:	INITEL S.A. DE C.V.
R.F.C.:	[redacted] 1
Dirección:	[redacted] 3
Teléfono:	[redacted] 5
web:	[redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media Superior de la Universidad de Guadalajara

PRESENTE

[redacted]

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

grupos de usuarios;
Debe permitir el control sin necesidad de instalaci6n de software de cliente,
el equipo que solicita salida a Internet, antes de iniciar la navegaci6n, entre a
un portal de autentificaci6n residente en el equipo de seguridad (portal
cautivo);
Debe soportar la identificación de varios usuarios conectados a la misma
dirección IP en entornos Citrix
y Microsoft Terminal Server, lo que permite
una visibilidad y un control granular por usuario en el uso de las aplicaciones
que se encuentran en estos servicios;
Debe de implementar la creación de grupos de usuarios en el firewall,
basada atributos del LDAP I AD
Permitir la integración con tokens para la autenticaciónde usuarios,
incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
Proporcionar al menos un token de forma nativa, lo que permite la
autenticaciónde dos factores
•
QOS TRAFFIC SHAPING
Con el fin de controlar el trafico y aplicaciones cuyo con sumo puede ser
excesivo (como YouTube, Ustream, etc.) y tienen un alto consume de ancho
de banda, se requiere de la solución que, adernas de permitir o denegar
dichas solicitudes, debe tener la capacidad de controlar el ancho de banda
maxima cuando son solicitados por los diferentes usuarios o aplicaciones,
tanto de audio coma de video streaming;
Soportar la creación de politicas de QoS y Traffic Shaping par dirección de
origen;
Soportar la creación de politicas de QoS y Traffic Shaping por dirección de
destine;
Soportar la creación de polfticas de QoS y Traffic Shaping par usuario y
grupo;
Soportar la creación de politicas de QoS y Traffic Shaping para aplicaciones
incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
Soportar la creación de polfticas de calidad de servicio y Traffic Shaping por
puerto;
QoS debe permitir la definición de trafico con ancho de banda garantizado;
QoS debe permitir la definición de trafico
con maxima ancho de banda;
QoS debe permitir la definición de cola de prioridad;
Soportar la priorización de protocolo en tiempo real de voz (VoIP) como
H.323, SIP, SCCP; MGCP y aplicaciones coma Skype;
Soportar marcación de paquetes DiffServ, incluso par aplicación;

Soportar la modificación de los valores de DSCP para Diffserv;

Soportar priorización de trafico utilizando información de Tipo de Servicio
(Type of Service)
Proporcionar estadisticas en tiempo real para clases de QoS y Traffic Sha pig;

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

Debe soportar QoS (traffic-shaping) en la interfaz agregada o redundantes;

•

FILTRO DE DATOS
Permite la creación de filtros para archivos y dates predefinidos;

Los archivos deben ser identificados por tamafio y tipo;
Permitir identificar y opcionalmente prevenir la transferencia de varios tipos
de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTIP, FTP,
SMTP, etc.);
Soportar la identificación de archivos comprimidos o la aplicación de politicas
sobre el contenido de este tipo de archivos;
Soportar la identificación de archives cifrados y la aplicación de polittcas
sobre el contenido de este tipo de archivos;
Permitir identificar y opcionalmente prevenir la transferencia de información
sensible, incluyendo, pero no limitado a, nurnero de tarjeta de credito,
permitiendo la creación de nuevos tipos de datos a traves de expresiones
regulares;

•

GEO LOCALIZACION
Soportar la creación de poHticas por geo-localizaci6n, permitiendo bloquear
el trafico de cierto Pais/Parses;
Debe permitir la visualizacionde los pafses de origen y destino en los
registros de acceso;
Debe permitir la creación de zonas geograficas por medio de la interfaz
grafica de usuario y la creación de politicas usando las mismas.

•

VPN
Soporte VPN de sitio a sitio y cliente a sitio;
Soportar VPN IP Sec;
Soportar VPN SSL;
la VPN IPSec debe ser compatible con 3DES;
La VPN IPSec debe ser compatible con la autenticaciónMOS y SHA-1;
la VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2;
Grupo 5 y el Grupo 14;
La VPN IPSec debe ser compatible con Internet Key Exchange (IKEvi y v2);
la VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced
Encryption Standard);
La VPN IPSec debe ser compatible con la autenticaciona traves de
certificados IKE PKI
Debe tener Interoperabilidad con los siguientes fabricantes: Cisco, Check
Point, Juniper, Palo Alto Networks, Forti net, SonicWall;
Soportar VPN para 1Pv4 e 1Pv6, asl como el trafico 1Pv4 dentro de tuneles
IPv6 IPSec
Debe permitir activar y desactivar tuneles IPSec VPN desde la interfaz grafica
de la solución, lo que facilita el proceso troubleshooting;
La VPN SSL debe soportar que el usdario pueda realizar la conexión a traves
de cliente instalado en el sistema operativo de su maquina o a traves de la
interfaz web;

SEMS
SECRETARÍA ADMINISTRATIVA

4
[redacted]

initel

Empresa:	INITEL S.A. DE C.V.
R.F.C.:	[redacted] 1
Dirección:	[redacted] 3
Teléfono:	[redacted] 5
web:	[redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL

Las caracteristicas de VPN SSL se deben cumplir con o sin el uso de agentes;
Debe permitir que todo el trafico de los usuarios VPN remotos fluya hacia el
tunel VPN, previniendo la comunicaci6n directa con dispositivos locales
coma un proxy;
Asignaci6n de DNS en la VPN de cliente remoto;
Debe permitir la creación de polfticas de control de aplicaciones, IPS,
antivirus, filtrado de URL y AntiSpyware para el trafico de clientes remotos
conectados a la VPN SSL;
Suportar autenticaciónvia AD/LDAP, Secure id, certificado y base de usuarios
local;
Suportar lectura y revision de CRL (lista de revocaci6n de certificados);
Permitir la aplicación de poHticas de seguridad y visibilidad para las
aplicaciones que circulan dentro de tuneles SSL;
Debe permitir que la conexión a la VPN se establece de la siguiente manera:
Antes de que el usuario se autentique en su estaci6n
Deberfa permitir la conexión a la VPN se establece de la siguiente manera:
Oespues de la autenticaciónde usuario en la estaci6n;
Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo
demanda de los usuarios;
Debera mantener una conexión segura con el portal durante la sesi6n;
El agente de VPN SSL o IPSEC cliente a sitio debe ser compatible con al
menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y
64 bits) y Mac OS X (vl0.10 o superior);
•
WIRELESS CONTROLLER
Debera gestionar de manera centralizada puntos de acceso del mismo
fabricante de la solución ofertada
Soportar servicio del servidor DHCP por SSID para proporcionar direcciones
IP a los clientes malarnbrtcos
Soporte 1Pv4 e 1Pv6 por SSID
Permitir elegir si el trafico de cada 5510 se enviara a la controladora o
directamente por la interfaz de punto de acceso en una VLAN dada
Permitir definir que redes se acceden a traves de la controladora y que redes
seran accedidas directamente por la interfaz del Access Point

Soportar monitoreo y supresi6n de puntos de acceso indebidos

Proporcionar autenticacióna la red inalambrica a traves de bases de datos
externas, tales como LDAP o RADIUS
Permitir autenticar a los usuarios de la red inalarnbrica de manera
transparente en dominios Windows
Permitir la visualizaciónde los dispositivos inalambricos conectados por
usuario
Permitir la visualizaciónde los dispositivos inalambricos conectados por IP
Permitir la visualizaciónde los dispositivos inalarnbricos conectados por tipo
de autenticación

SEMS
SECRETARÍA ADMINISTRATIVA

4

[redacted]

inite

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	SUBTOTAL
		Permitir la visualizaciónde los dispositivos inalambricos conectados por canal Permitir la visualizaciónde los dispositivos inalarnbricos conectados por ancho de banda usado Permitir la visualizaciónde los dispositivos inalambricos conectados por potencia de la sefial Permitir la visualizaciónde los dispositivos inalarnbricos conectados por tiempo de asociación Debe soportar Fast Roaming en autenticacióncon portal cautivo Debe soportar configuración de portal cautivo por SSID Permitir bloqueo de trafico entre los clientes conectados a un SSID y AP espedfico Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y lo TKIP. Debe ser compatible con el protocolo 802.lx RADIUS La controladora tnalarnbrica debera permitir configurar los para metros de radio como banda y canal La controlàdora debera permitir rnetodos de descubrimiento de puntos de acceso de manera automatica La controladora debera permitir rnetcdos de descubrimiento de puntos de acceso por IP estatica La controladora debera permitir rnetodos de descubrimiento de puntos de acceso por DHCP La controladora debera permitir metodos de descubrimiento de puntos de acceso por dns La controladora debera permitir metodos de descubrimiento de puntos de acceso por broadcast La controladora debera permitir metodos de descubrimiento de puntos de acceso par multicast La controladora Inalambrica debera suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue) La controladora debera contar con proteccion contra ataques ARP Poisoning en el controlador Inalarnbrico La controladora debera contar con mecanismos de protecciónde tramas de administraci6n de acuerdo a las especificaciones de la alianza Wi-Fi y estandar 802.llac La controladora inalambrtca debera tener de manera integrada sistema de deteccion de intrusion inalarnbrica contra ataques tipo ASLEAP La controladora inalambrica debera tener de manera integrada sistema de deteccion de intrusion inalarnbrica contra ataques tipo Association Frame Flooding La controladora inalarnbrica debera tener de manera integrada sistema de deteccion de intrusion inalambrica contra ataques tipo Authentication Frame Flooding La controladora tnalarnbrtca debera tener de manera integrada sistema de		

SEMS
SECRETARÍA ADMINISTRATIVA

4 [redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		detección de intrusion inalarnbrica contra ataques tipo Broadcasting De-authentication la controladora inalambrica debera tener de manera integrada sistema de detección de intrusion inalarnbrica contra ataques tipo EAPOL Packet flooding La controladora inalambrica debera tener de manera integrada sistema de deteccion de intrusion inalarnbrica contra ataques tipo Invalid MAC OUI La controladora inatarnbrtca debera tener de manera integrada sistema de deteccion de intrusion inalambrtca contra ataques tipo Long Duration Attack La controladora inalambrica debera tener de manera integrada sistema de deteccion de intrusion inalarnbrica contra ataques tipo Null SSID probe response La controladora inalambrtca debera tener de manera integrada sistema de deteccion de intrusion tnalambrica contra ataques tipo Spoofed De-authentication La controladora inalambrica debera tener de manera integrada sistema de deteccion de intrusion inalarnbrtca contra ataques tipo Weak WEP IV Detection La controladora tnalambrica debera tener de manera integrada sistema de detección de intrusion inalarnbrica contra ataques tipo Wireless Bridge Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas Permitir seleccionar el día y hara en que se producira la optimizaci6n de aprovisionamiento automatics de canales en los puntos de acceso La controladora inalambrica debe permitir agendar horarios para determinar en que memento la red inalarnbrica (SSID) se encuentra disponible La controladora inalarnbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario Permitir configurar el numero rnaxirno de clientes que pueden ser permitidos par SSID Permitir configurar el numero rnaxirno de clientes que pueden ser permitidos par punto de acceso Permitir configurar el numero maxi mo de clientes que pueden ser permitidos par Radio La controladora debe permitir crear, administrar y autorizar las redes inalarnbricas mesh Ofrecer un mecanismo de creacion autornatica y/o manual de usuarios visitantes y contrasefias, que puedan ser enviados par correo electronico o SMS a los usuarios, con ajuste de tiempo de expiraci6n de la contrasefia La comunicacion entre la controladora y el punto de acceso inalarnbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS		

SEMS
SECRETARÍA ADMINISTRATIVA

4 [redacted]

initel

Empresa:	INITEL S.A. DE C.V.
R.F.C.:	[redacted] 1
Dirección:	[redacted] 3
Teléfono:	[redacted] 5
web:	[redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara

PRESENTE

Fecha:	30 de octubre de 2017
Licitación:	LI-SEMS-040-2017

"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
		Debe tener un mecanismo de ajuste automatico de potencia de la serial con el fin de reducir la interferencia entre canales entre dos puntos de acceso administrados Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualizaci6n a traves de la interfaz grafica. Permitir que sean deshabilitados clientes inalarnbricos que tengan baja tasa de transmisi6n Permitir ignorar a los clientes inalambricos que tienen serial debti, estableciendo un umbral de serial a partir de la cual los clientes son ignorados la controladora debe permitir configurar el valor de Short Guard Interval para 802.lln y 802.llac en 5 GHz Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados Debe permitir asociación dinarntcas de VIANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS Debe permitir asociación dinarnica de VIANs a los usuarios autenticados en un SSID especifico mediante vlan pooling Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalambnco la controladora inalarnbrica debe permitir identificar los clientes WiFi que presenten algun riesgo basado en aplicaciones la controladora inalambrica debe permitir identificar los clientes WiFi que presenten algun riesgo basado en dirección de destine la controladora inalambrica debe permitir identificar los clientes WiFi que presenten algun riesgo basado en amenaza la controladora inalarnbrica debe permitir identificar los clientes WiFi que presenten algun riesgo basado en sesiones la controladora Inalambrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de trafico El controlador inalambrico debe tener interface de administraci6n integrado en el mismo equipo El controlador inalambnco debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el node secundario y nodes principales la controladora Inalambrica debera soportar aceleraci6n de trafico del protocolo CAPWAP a traves de un procesador de red de prop6sito espedfico la controladora inalarnbrica debera soportar aceleraci6n de tunnel de trafico de puente inalambnco a traves de un procesador de red de prop6sito espedfico la controladora inalarnbrica debe soportar protocolo LLDP		

SEMS
SECRETARÍA ADMINISTRATIVA

4 [redacted]

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: [redacted] 1
Dirección: [redacted] 3
Teléfono: [redacted] 5
web: [redacted] 6

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media
Superior de la Universidad de Guadalajara
PRESENTE

Fecha: 30 de octubre de 2017
Licitación: LI-SEMS-040-2017
"Adquisiciones de equipos de seguridad de siguiente generación para la red de Escuelas Preparatorias del Sistema de Educación Media Superior, con cargo al Programa de Mejoramiento a la Conectividad y a los Servicios Dorsales de Tecnologías de Información y Comunicación de la Red Universitaria".

PARTIDA	CANTIDAD	DESCRIPCION	PRECIO UNITARIO	SUBTOTAL
		Debe permitir tecnica de detección de APs intrusos On-wire a traves de dirección MAC exacta Debe permitir tecnica de detección de APs intrusos On-wire a traves de dirección MAC Adyacente Debe permitir la visualizaciónde los usuarios conectados en forma de topologia 16gica de red representando la cantidad de dates transmitidos y recibidos la controladora inalarnbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado La controladora malarnbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas la controladora inalambrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada Debera soportar la conversion de Multicast a Unicast para mejorar el rendimiento del tiempo de aire		

SUBTOTAL	$	10,046,867.59
IVA	$	1,607,498.81
TOTAL	$	11,654,366.40

Total con Letra: Once Millones Seiscientos Cincuenta y Cuatro Mil Trescientos Sesenta y Seis Pesos 40/100 M.N.

Condiciones Comerciales

Moneda:	Precios expresados en Moneda Nacional.
Tiempo de Entrega:	4 a 6 semanas despues de confirmado el pedido
Vigencia:	30 días naturales apartir de la fecha de apertura del sobre
Forma de pago:	Credito 15 días naturales
Garantía:	3 años
Notas:	Los precios ofertados consideran el costo de flete para la entrega a cada dependencia beneficiada.

4
[redacted]
eobaldo Leal Arriaga 7
[redacted] 6
5

SEMS
SECRETARÍA ADMINIS

4
[redacted]

1.- Se testan 58 RFC, con fundamento en el artículo 21, párrafo 1, fracción I, de la Ley de Transparencia y Acceso a la Información Pública de Estado de Jalisco y sus Municipios; así como el artículo 3, punto 1, fracción IX de la Ley de Protección de Datos personales en posesión de Sujetos Obligados del Estado de Jalisco y sus municipios, y al Lineamiento Quincuagésimo Octavo, fracción I, de los Lineamientos Generales de Protección de Información Confidencial y Reservada por contener datos de carácter personal.

2.- Se testan 2 claves del IMSS, con fundamento en el artículo 21, párrafo 1, fracción I, de la Ley de Transparencia y Acceso a la Información Pública de Estado de Jalisco y sus Municipios; así como el artículo 3, punto 1, fracción IX de la Ley de Protección de Datos personales en posesión de Sujetos Obligados del Estado de Jalisco y sus municipios, y al Lineamiento Quincuagésimo Octavo, fracción I, de los Lineamientos Generales de Protección de Información Confidencial y Reservada por contener datos de carácter personal.

3.- Se testan 56 domicilios, con fundamento en el artículo 21, párrafo 1, fracción I, de la Ley de Transparencia y Accso a la Información Pública de Estado de Jalisco y sus Municipios; así como el artículo 3, punto 1, fracción IX de la Ley de Protección de Datos personales en posesión de Sujetos Obligados del Estado de Jalisco y sus municipios, y al Lineamiento Quincuagésimo Octavo, fracción I, de los Lineamientos Generales de Protección de Información Confidencial y Reservada por contener datos de carácter personal.

4.- Se testan 68 firmas, con fundamento en el artículo 21, párrafo 1, fracción I, de la Ley de Transparencia y Acceso a la Información Pública de Estado de Jalisco y sus Municipios; así como el artículo 3, punto 1, fracción IX de la Ley de Protección de Datos personales en posesión de Sujetos Obligados del Estado de Jalisco y sus municipios, y al Lineamiento Quincuagésimo Octavo, fracción I, de los Lineamientos Generales de Protección de Información Confidencial y Reservada por contener datos de carácter personal.

5.- Se testan 56 teléfonos, con fundamento en el artículo 21, párrafo 1, fracción I, de la Ley de Transparencia y Acceso a la Información Pública de Estado de Jalisco y sus Municipios; así como el artículo 3, punto 1, fracción IX de la Ley de Protección de Datos personales en posesión de Sujetos Obligados del Estado de Jalisco y sus municipios, y al Lineamiento Quincuagésimo Octavo, fracción I, de los Lineamientos Generales de Protección de Información Confidencial y Reservada por contener datos de carácter personal.

6.- Se testan 56 páginas web, con fundamento en el artículo 21, párrafo 1, fracción I, de la Ley de Transparencia y Acceso a la Información Pública de Estado de Jalisco y sus Municipios; así como el artículo 3, punto 1, fracción IX de la Ley de Protección de Datos personales en posesión de Sujetos Obligados del Estado de Jalisco y sus municipios, y al Lineamiento Quincuagésimo Octavo, fracción I, de los Lineamientos Generales de Protección de Información Confidencial y Reservada por contener datos de carácter personal.

7.- Se testan 2 emails, con fundamento en el artículo 21, párrafo 1, fracción I, de la Ley de Transparencia y Acceso a la Información Pública de Estado de Jalisco y sus Municipios; así como el artículo 3, punto 1, fracción IX de la Ley de Protección de Datos personales en posesión de Sujetos Obligados del Estado de Jalisco y sus municipios, y al Lineamiento Quincuagésimo Octavo, fracción I, de los Lineamientos Generales de Protección de Información Confidencial y Reservada por contener datos de carácter personal.