aymundo Riva Palacio
apalacio@ejecentral.com.mx
tter: @rivapa

STRICTAMENTE ERSONAL

l ataque

sión contra los científicos solicitada el 24 de agosto pasado al juez de Distrito en El Altiplano, Gregorio Salazar Hernández, que revela sevicia y despropósito.

En esa reveladora solicitud señaló que los investigadores y académicos -muchos de ellos reconocidos internacionalmente-, tenían una conducta criminal, que de acuerdo con sus investigaciones, por las "enormes cantidades de dinero" y "capacidad económica obtenida de forma ilícita, podrían realizar actos de corrupción en algún centro con medidas de seguridad bajas o medio de peculado y uso ilícito de atribuciones y facultades, escaló a manejo de operaciones con recursos de origen de procedencia ilícita y delincuencia organizada, crímenes federales donde se ingresa a la cárcel sin posibilidad de defensa en libertad. Las penas que pidió en contra de los principales científicos imputados fueron de hasta 40 años de prisión.

Gertz Manero actuó de forma expedita. Nueve días antes de solicitar la orden de aprehensión, el 15 de agosto, recibió documentación y constancias de la Secretaría de Hacienda para con lo cual, al presentarle como "suplente", dejó en Ramírez de la O la carga de la denuncia, deslindándose, para efectos prácticos, de ella. La Secretaría de Hacienda, sin embargo, actuó en consecuencia con la demanda del Conacyt y una moción, sin saberse hasta este momento de dónde, para presentar la denuncia ante la Fiscalía General, y darle así los elementos para fincar los delitos de delincuencia organizada.

Las constancias que entregó Hacienda no explican en qué se sustentan las operaciones con recursos de procedencia ilícita, si la de- ...car o tomar distancia de las acusaciones por delincuencia organizada, respondió que "el que nada debe, nada teme".

El juez Salazar Hernández rechazó esta semana la segunda solicitud de orden de aprehensión contra los científicos, y antes de que terminara el día, la Fiscalía General, volvió a acometer contra ese grupo con una tercera petición para que los detengan. Se han eliminado, cuando menos por ahora, los delitos relacionados con delincuencia organizada, pero la embestida va para adelante y no va a terminar. Gertz Manero, con el apoyo presidencial, irá más allá de los límites, y hasta donde le permiten llegar.

Carlos Loret
de Mola A.
carlosloret@yahoo.com.mx

HISTORIAS DE REPORTERO

El medio abrazo de sonrisas forzadas AMLO-

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 88 fracción III de la Ley Orgánica de la Universidad de Guadalajara 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, 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 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 LIMITE DE INSCRIPCIÓN	JUNTA DE ACLARACIONES	PRESENTACIÓN Y APERTURA DE PROPUESTAS	ACTA DE LECTURA DE FALLO
LI-SEMS-009-2021	Adquisición de puntos de acceso inalámbricos y nodos de red, para el Sistema de Educación Media Superior de la Universidad de Guadalajara	28 de septiembre de 2021	06 de octubre de 2021 11:00 horas	13 de octubre de 2021 11:00 horas	29 de octubre de 2021 11:00 horas
LI-SEMS-010-2021	Adquisición de equipo de solución de seguridad UTM/NGFW, para el Sistema de Educación Media Superior de la Universidad de Guadalajara.	28 de septiembre de 2021	06 de octubre de 2021 13:00 horas	13 de octubre de 2021 13:00 horas	29 de octubre de 2021 13:00 horas

LOS INTERESADOS A PARTICIPAR EN LA PRESENTE LICITACIÓN DEBERÁN:
Solicitar su inscripción, requisito previo para poder adquirir las bases de la licitación a partir de la fecha de esta publicación, en días hábiles y hasta **28 de septiembre de 2021**, de las **10:00 a 14:00 horas**, ante la Coordinación de Servicios Generales del Sistema de Educación Media Superior de la Universidad de Guadalajara, ubicada en Liceo #496 4to. Piso, colonia Centro, en la ciudad de Guadalajara, Jalisco; asimismo, deberán obtener las bases de la licitación, previa aceptación de su registro, las cuales serán entregadas el día **29 de septiembre de 2021** de **10:00 a 14:00 horas.** Cumplir con los requisitos establecidos en la presente convocatoria y realizar el pago no rembolsable, de $2,500.00 (Dos mil quinientos pesos 00/100 M. N.) I.V.A. incluido, mediante depósito bancario en la cuenta institucional que se indique en la orden de pago.

LA JUNTA DE ACLARACIONES, CON CARÁCTER DE OBLIGATORIA, SERÁ:
LI-SEMS-009-2021 06 de octubre de 2021 a las 11:00 horas.
LI-SEMS-010-2021 06 de octubre de 2021 a las 13:00 horas.
En la Sala de Juntas (ala derecha) anexa 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.

DEL ACTO DE ENTREGA Y APERTURA DE PROPUESTAS:
LI-SEMS-009-2021 13 de octubre de 2021 a las 11:00 horas.
LI-SEMS-010-2021 13 de octubre de 2021 a las 13:00 horas.
En la Sala de Juntas (Ala derecha) anexa 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.
Dicho acto se realizará en sesión pública al que podrán asistir los participantes de esta licitación. La presentación de las propuestas deberá estar estructurada, conforme se establece en las bases de la licitación.
Fuente de los recursos corresponden a los recursos del Tus prioridades - Internet en escuelas F-1.3.13.3.

REQUISITOS QUE DEBEN CUMPLIR LOS INTERESADOS:
1. Solicitud por escrito dirigida al Ing. Fernando Calvillo Vargas, en papel membretado de la empresa (original y copia fotostática), firmada por el Representante Legal y/o persona física participante), donde expresen su interés en participar en la licitación, indicando el número y la descripción de ésta.
2. Acta constitutiva y sus modificaciones, que incluya la constancia ante el Registro Público de la Propiedad y de Comercio o en el caso de persona física, acta de nacimiento (copia fotostática simple).

Bases de la Licitación Pública LI-SEMS-010-2021

ADQUISICIÓN DE EQUIPO DE SOLUCIÓN DE SEGURIDAD UTM/NGFW, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA.

SEPTIEMBRE 2021

ÍNDICE

SECCIÓN I
INSTRUCCIONES A LOS LICITANTES

A. Introducción

1. Fuente de los recursos

1.1 Los recursos corresponden a: Proyecto 259928 TUS PRIORIDADES - INTERNET EN ESCUELAS, EQUIPAM. T (F-1.3.13.3) (AÑO: 2021).

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 equipo de solución utm/ngfw.

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 **6 de octubre de 2021, a las 13:00 horas**, 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 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 **16:00 horas del día 30 de septiembre de 2021**, 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. De la misma forma se podrá prorrogar fecha de la lectura de fallo, dentro del plazo de la vigencia de

las propuestas, la cual les será notificada por correo electrónico a todos los licitantes participantes.

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 adjudicarán por bloque, los licitantes deberán cotizar todas las partidas, **ya que la evaluación y la adjudicación de las propuestas se realizará por bloque.**

10. Requisitos para el proveedor

10.1 Los licitantes deberán ser compañías legalmente establecidas en territorio nacional, que se dediquen preponderantemente a la venta y suministro de equipo de solución utm/ngfw.

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 al Proyecto 259928

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 En caso de que el concursante adjudicado requiera **anticipo el cual será por un máximo del (30%)**, **deberá garantizar previo a su entrega, el 100% del importe total del anticipo otorgado, incluido el impuesto al valor agregado (IVA),** mediante constitución de fianza en original por una institución legalmente autorizada, a favor de la Universidad de Guadalajara, mismo que se establece en la sección V de las bases de la licitación.

14.6 Las fianzas que presente el licitante adjudicado deberán contener el número y nombre de la licitación, tal como se especifica en las presentes bases.

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: Mtro. Jesús Alberto Jiménez Herrera

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

b) Indicará: Propuesta para la Licitación Pública **LI-SEMS-010-2021** denominada ADQUISICIÓN DE EQUIPO DE SOLUCIÓN DE SEGURIDAD UTM/NGFW, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA., **fecha de la convocatoria y la frase "NO ABRIR ANTES DE LAS 13:00 HORAS DEL 13 DE OCTUBRE DE 2021".**

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 **13:00 HORAS DEL 13 DE OCTUBRE DE 2021".**

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 **13:00 HORAS DEL 13 DE OCTUBRE DE 2021.**, 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 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, el acta de 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 licitante 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 las condiciones de pago.

K) Si el licitante solicita en su propuesta anticipo superior al máximo establecido en las presentes bases.

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.

U) Si el licitante establece en su propuesta alguna sanción o penalización en contra de la convocante por cualquier motivo.

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 que a continuación se indican:

DEPENDENCIA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA DEL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR Ubicación en: **Edificio Valentín Gómez Farías** Dirección: Liceo No. 496 esq. Juan Álvarez (piso 6) **Teléfono:** 33 3942 4100 Ext. 14135

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 pago al proveedor se realizará con un máximo de 30% anticipo y el resto será pago posterior a la recepción de conformidad de los bienes adjudicados por la dependencia convocante 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.

2.2 El participante deberá de especificar en su propuesta en las condiciones de pago.

2.3 En caso de que el concursante adjudicado requiera un máximo de **anticipo de (30%)**, **deberá garantizar previo a su entrega, el 100% del importe total del anticipo otorgado, incluido el impuesto al valor agregado (IVA),** mediante constitución de fianza en original por una institución legalmente autorizada, a favor de la Universidad de Guadalajara.

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 de cotización**

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

7.2 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 de los bienes requeridos por el Sistema de Educación Media Superior, conforme a la siguiente tabla:

PARTIDA	CANTIDAD		DESCRIPCIÓN	C.U.	TOTAL
			SOLUCIÓN UTM/NGFW "TIPO A"		
		1.1)	Throughput de por lo menos 24 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete		
		1.2)	Soporte a por lo menos 4M conexiones simultaneas		
		1.3)	Soporte a por lo menos 450K nuevas conexiones por segundo		
		1.4)	Throughput de al menos 20 Gbps de VPN IPSec		
		1.5)	Estar licenciado para, o soportar sin necesidad de licencia, 2K tuneles de VPN IPSec site-to-site simultaneos		
		1.6)	Estar licenciado para, o soportar sin necesidad de licencia, 50K tuneles de clientes VPN IPSec simultaneos		
		1.7)	Throughput de al menos 4500 Mbps de VPN SSL		
		1.8)	Soportar al menos 5000 clientes de VPN SSL simultaneos		
		1.9)	Soportar al menos 7800 Mbps de throughput de IPS		
		1.10)	Soportar al menos 4000 Mbps de throughput de Inspeción SSL		
		1.11)	Throughput de al menos 5000 Mbps con las siguientes funcionalidades habilitadas simultaneamente para todas las firmas que la solución de seguridad tenga debidamente activadasy operativas: control de aplicaciones, IPS, Antivírus y Antispyware. Caso el fabricante tenga publicado multiples numeros de disempeño para cualquier de las funcionalidades, solamente el de valor más pequeño sera aceptado.		
		1.12)	Permitir gestionar como controladora inalámbrica al menos 512 Access Points y gestionar por lo menos 72 Switches de la misma marca del fabricante del UTM/NGFW dentro de la misma interfase de gestión		
		1.13)	Tener al menos 4 interfaces 10 Gbps SFPP, 8 interfases de 1 Gbps SFP, 16 interfases de 1GE RJ25, 2 interfases 1 Gbps RJ45 para Gestion y alta disponibilidad		
		1.15)	Estar licenciado y/o tener incluído sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance		
		1.16)	Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance		
		1.17)	Debe de incluir un token fisico para autenticacion de doble factor para la gestion del appliance o para el acceso VPN que debe ser de la misma marca propuesta		
		1.18)	Debe de 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus, Botnet IP/Domain, AntiSpam y Filtrado Web		
		1.19)	Debe de contar con una fuente de poder AC de 100-240 VAC, con la posibilidad de agregar una segunda para alta disponibilidad		
		1.20)	Deberá contar con 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema de firmware, y los siguientes módulos incluidos IPS ó Preventor de Intrusos, Antivirus , Protección contra Botnet IP/Domain, Módulo de Protección de Mobile Malware, Módulo de Sandbox en nube incluyendo Virus Outbreak and Content Disarm & Reconstruct, Control de aplicaciones, Filtrado Web & Video Filtering y Módulo de AntiSpam.		
			2) Requisitos Mínimos de Funcionalidad		
			Características Generales		
1	29	2.1)	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;		

			2.2)	Por funcionalidades de NGFW se entiende: aplicaciones de reconocimiento, prevención de amenazas, identificación de usuarios y control granular de permisos;		
			2.3)	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;		
			2.4)	La plataforma debe estar optimizada para aplicaciones de análisis de contenido en la capa 7;		
			2.5)	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;		
			2.6)	La gestión del equipo debe ser compatible con acceso a través de SSH, consola, web (HTTPS) y API abierta;		
			2.7)	La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red		
			2.8)	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;		
			2.9)	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;		
			2.10)	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;		
			2.11)	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);		
			2.12)	Los dispositivos de protección de red deben soportar DHCP Relay;		
			2.13)	Los dispositivos de protección de red deben soportar DHCP Server;		
			2.14)	Los dispositivos de protección de red deben soportar sFlow		
			2.15)	Los dispositivos de protección de red deben soportar Jumbo Frames;		
			2.16)	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas		
			2.17)	Debe ser compatible con NAT dinámica (varios-a-1);		
			2.18)	Debe ser compatible con NAT dinámica (muchos-a-muchos);		
			2.19)	Debe soportar NAT estática (1-a-1);		
			2.20)	Debe admitir NAT estática (muchos-a-muchos);		
			2.21)	Debe ser compatible con NAT estático bidireccional 1-a-1;		
			2.22)	Debe ser compatible con la traducción de puertos (PAT);		
			2.23)	Debe ser compatible con NAT Origen;		
			2.24)	Debe ser compatible con NAT de destino;		
			2.25)	Debe soportar NAT de origen y NAT de destino de forma simultánea;		
			2.26)	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;		
			2.27)	Debe ser compatible con NAT64 y NAT46;		
			2.28)	Debe implementar el protocolo ECMP;		
			2.29)	Debe soportar el balanceo de enlace hash por IP de origen;		
			2.30)	Debe soportar el balanceo de enlace hash por IP de origen y destino;		
			2.31)	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;		
			2.32)	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales		
			2.33)	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		
			2.34)	Enviar logs a sistemas de gestión externos simultáneamente;		
			2.35)	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;		
			2.36)	Debe soporta protección contra la suplantación de identidad (anti-spoofing);		
			2.37)	Implementar la optimización del tráfico entre dos dispositivos;		

		2.38) Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP); 2.39) Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3); 2.40) Soportar OSPF graceful restart; 2.41) 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); 2.42) Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red; 2.43) Debe soportar modo capa - 2 (L2) para la inspección de datos en línea y la visibilidad del tráfico; 2.44) Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en línea de tráfico; 2.45) Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas; 2.46) Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente; 2.47) Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3; 2.48) Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster; 2.49) La configuración de alta disponibilidad debe sincronizar: Sesiones; 2.50) La configuración de alta disponibilidad debe sincronizar: configuración, incluyendo, pero no limitados políticas de Firewalls, NAT, QoS y objetos de la red; 2.51) La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN; 2.52) La configuración de alta disponibilidad debe sincronizar: Tablas FIB; 2.53) En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace; 2.54) Debe soportar la creación de sistemas virtuales en el mismo equipo; 2.55) 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; 2.56) 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; 2.57) 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;		

		2.58)	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 Politica de Firewall		
		2.59)	Debe soportar controles de zona de seguridad		
		2.60)	Debe contar con políticas de control por puerto y protocolo		
		2.61)	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		
		2.62)	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad		
		2.63)	Control de política por código de país (por ejemplo: BR, USA., UK, RUS)		
		2.64)	Control, inspección y des encriptación de SSL por política para el tráfico entrante y la salida		
		2.65)	Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada;		
		2.66)	Debe descifrar las conexiones de entrada y salida de tráfico negociadas con TLS 1.2;		
		2.67)	Control de inspección y descifrado SSH por política;		
		2.68)	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;		
		2.69)	Traffic shaping QoS basado en políticas (garantía de prioridad y máximo);		
		2.70)	QoS basado en políticas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones;		
		2.71)	Soporte para objetos y reglas IPV6;		
		2.72)	Soporte objetos y reglas de multicast;		
		2.73)	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 unreachable por la máquina fuente de tráfico, TCP Reset para el cliente , RESET de TCP con el servidor o en ambos lados de la conexión;		
		2.74)	Soportar la calendarización de políticas con el fin de activar y desactivar las reglas en tiempos predefinidos de forma automática;		
			Control de Aplicación		
		2.75)	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo		

		2.76)	Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos		
		2.77)	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;		
		2.78)	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;		
		2.79)	Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;		
		2.80)	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;		
		2.81)	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		
		2.82)	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;		
		2.83)	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		
		2.84)	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;		
		2.85)	Actualización de la base de firmas de la aplicación de forma automática;		
		2.86)	Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos;		
		2.87)	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;		

		2.88)	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;		
		2.89)	Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;		
		2.90)	Para mantener la seguridad de red eficiente debe ser soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;		
		2.91)	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		
		2.92)	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		
		2.93)	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;		
		2.94)	Debe alertar al usuario cuando sea bloqueada una aplicación;		
		2.95)	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;		
		2.96)	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;		
		2.97)	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;		
		2.98)	Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;		
		2.99)	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)		
		2.100)	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: nivel de riesgo de la aplicación		
		2.101)	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación		
			Prevención de Amenazas		
		2.102)	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;		

		2.103)	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);		
		2.104)	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;		
		2.105)	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad;		
		2.106)	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;		
		2.107)	Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo;		
		2.108)	Deben ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad		
		2.109)	Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas;		
		2.110)	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		
		2.111)	Deber permitir el bloqueo de vulnerabilidades		
		2.112)	Debe permitir el bloqueo de exploits conocidos		
		2.113)	Debe incluir la protección contra ataques de denegación de servicio		
		2.114)	Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones;		
		2.115)	Debe tener los siguientes mecanismos de inspección IPS: análisis de decodificación de protocolo;		
		2.116)	Debe tener los siguientes mecanismos de inspección IPS: análisis para detectar anomalías de protocolo;		
		2.117)	Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico;		
		2.118)	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;		
		2.119)	Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;		
		2.120)	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets)		
		2.121)	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones SYN, ICMP , UDP, etc;		
		2.122)	Detectar y bloquear los escaneos de puertos de origen;		
		2.123)	Bloquear ataques realizados por gusanos (worms) conocidos;		
		2.124)	Contar con firmas específicas para la mitigación de ataques DoS y DDoS;		
		2.125)	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);		

		2.126)	Debe poder crear firmas personalizadas en la interfaz gráfica del producto;		
		2.127)	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;		
		2.128)	Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;		
		2.129)	Soportar el bloqueo de archivos por tipo;		
		2.130)	Identificar y bloquear la comunicación con redes de bots;		
		2.131)	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;		
		2.132)	Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;		
		2.133)	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		
		2.134)	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;		
		2.135)	Los eventos deben identificar el país que origino la amenaza;		
		2.136)	Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms)		
		2.137)	Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP		
		2.138)	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		
		2.139)	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);		
		2.140)	Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad		
		2.141)	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;		

		2.142)	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;		
		2.143)	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL		
		2.144)	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;		
		2.145)	Tener por lo menos 60 categorías de URL;		
		2.146)	Debe tener la funcionalidad de exclusión de URLs por categoría		
		2.147)	Permitir página de bloqueo personalizada;		
		2.148)	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		
		2.149)	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;		
		2.150)	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;		
		2.151)	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;		
		2.152)	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;		
		2.153)	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;		
		2.154)	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;		
		2.155)	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);		

			2.156)	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;		
			2.157)	Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos del LDAP / AD		
			2.158)	Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.		
			2.159)	Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores		
				QoS Traffic Shaping		
			2.160)	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;		
			2.161)	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;		
			2.162)	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;		
			2.163)	Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;		
			2.164)	Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;		
			2.165)	Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;		
			2.166)	QoS debe permitir la definición de tráfico con ancho de banda garantizado;		
			2.167)	QoS debe permitir la definición de tráfico con máximo ancho de banda;		
			2.168)	QoS debe permitir la definición de cola de prioridad;		
			2.169)	Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype;		
			2.170)	Soportar marcación de paquetes DiffServ, incluso por aplicación;		
			2.171)	Soportar la modificación de los valores de DSCP para Diffserv;		
			2.172)	Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service)		
			2.173)	Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shapig;		
			2.174)	Debe soportar QoS (traffic-shaping) en la interfaz agregada o redundantes;		
				Filtro de Datos		

		2.175)	Permite la creación de filtros para archivos y datos predefinidos;		
		2.176)	Los archivos deben ser identificados por tamaño y tipo;		
		2.177)	Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);		
		2.178)	Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;		
		2.179)	Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;		
		2.180)	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		
		2.181)	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;		
		2.182)	Debe permitir la visualización de los países de origen y destino en los registros de acceso;		
		2.183)	Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.		
			VPN		
		2.184)	Soporte VPN de sitio a sitio y cliente a sitio;		
		2.185)	Soportar VPN IPSec;		
		2.186)	Soportar VPN SSL;		
		2.187)	La VPN IPSec debe ser compatible con 3DES;		
		2.188)	La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;		
		2.189)	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y el Grupo 14;		
		2.190)	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);		
		2.191)	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);		
		2.192)	La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI		
		2.193)	Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;		
		2.194)	Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec		
		2.195)	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;		
		2.196)	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;		

		2.197) Las características de VPN SSL se deben cumplir con o sin el uso de agentes;			
		2.198) 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;			
		2.199) Asignación de DNS en la VPN de cliente remoto;			
		2.200) 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;			
		2.201) Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;			
		2.202) Suportar lectura y revisión de CRL (lista de revocación de certificados);			
		2.203) Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;			
		2.204) Debe permitir que la conexión a la VPN se establece de la siguiente manera: Antes de que el usuario se autentique en su estación			
		2.205) Debería permitir la conexión a la VPN se establece de la siguiente manera: Después de la autenticación de usuario en la estación;			
		2.206) Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo demanda de los usuarios;			
		2.207) Deberá mantener una conexión segura con el portal durante la sesión;			
		2.208) 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			
		2.209) Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada			
		2.210) Soportar servicio del servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos			
		2.211) Soporte IPv4 e IPv6 por SSID			
		2.212) 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			
		2.213) Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point			
		2.214) Soportar monitoreo y supresión de puntos de acceso indebidos			
		2.215) Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS			
		2.216) Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows			
		2.217) Permitir la visualización de los dispositivos inalámbricos conectados por usuario			

		2.218)	Permitir la visualización de los dispositivos inalámbricos conectados por IP		
		2.219)	Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación		
		2.220)	Permitir la visualización de los dispositivos inalámbricos conectados por canal		
		2.221)	Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado		
		2.222)	Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal		
		2.223)	Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación		
		2.224)	Debe soportar Fast Roaming en autenticación con portal cautivo		
		2.225)	Debe soportar configuración de portal cautivo por SSID		
		2.226)	Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico		
		2.227)	Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP.		
		2.228)	Debe ser compatible con el protocolo 802.1x RADIUS		
		2.229)	La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal		
		2.230)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática		
		2.231)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática		
		2.232)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP		
		2.233)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por dns		
		2.234)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por broadcast		
		2.235)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por multicast		
		2.236)	La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue)		
		2.237)	La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico		
		2.238)	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		
		2.239)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP		
		2.240)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding		
		2.241)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding		
		2.242)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication		
		2.243)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding		
		2.244)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI		
		2.245)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack		

		2.246)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response			
		2.247)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication			
		2.248)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection			
		2.249)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge			
		2.250)	Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas			
		2.251)	Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso			
		2.252)	La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible			
		2.253)	La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario			
		2.254)	Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID			
		2.255)	Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso			
		2.256)	Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio			
		2.257)	La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh			
		2.258)	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			
		2.259)	La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS			
		2.260)	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			
		2.261)	Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso			
		2.262)	Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso			
		2.263)	Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica;			
		2.264)	Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión			
		2.265)	Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados			
		2.266)	La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz			
		2.267)	Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados			
		2.268)	Debe permitir asociación dinámicas de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS			
		2.269)	Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling			

		2.270) Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico			
		2.271) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones			
		2.272) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino			
		2.273) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza			
		2.274) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones			
		2.275) la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico			
		2.276) El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo			
		2.277) El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales			
		2.278) La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico			
		2.279) La controladora inalámbrica deberá soportar aceleración de tunnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico			
		2.280) La controladora inalámbrica debe soportar protocolo LLDP			
		2.281) Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta			
		2.282) Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC Adyacente			
		2.283) Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos			
		1 2.284) La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado			
		2.285) La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas			
		2.286) La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada			
		2.287) Deberá soportar la conversion de Multicast a Unicast para mejorar el rendimiento del tiempo de aire			
		SOLUCIÓN UTM/NGFW "TIPO B"			
		1.1) Throughput de por lo menos 11 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete			
		1.2) Soporte a por lo menos 3M conexiones simultaneas			
		1.3) Soporte a por lo menos 280K nuevas conexiones por segundo			
		1.4) Throughput de al menos 13 Gbps de VPN IPSec			
		1.5) Estar licenciado para, o soportar sin necesidad de licencia, 2K tuneles de VPN IPSec site-to-site simultaneos			
		1.6) Estar licenciado para, o soportar sin necesidad de licencia, 16K tuneles de clientes VPN IPSec simultaneos			
		1.7) Throughput de al menos 2000 Mbps de VPN SSL			
2	**41**	1.8) Soportar al menos 500 clientes de VPN SSL simultaneos			

		1.9) Soportar al menos 5000 Mbps de throughput de IPS 1.10) Soportar al menos 4000 Mbps de throughput de Inspeción SSL 1.11) Throughput de al menos 3000 Mbps con las siguientes funcionalidades habilitadas simultaneamente para todas las firmas que la solución de seguridad tenga debidamente activadasy operativas: control de aplicaciones, IPS, Antivírus y Antispyware. Caso el fabricante tenga publicado multiples numeros de disempeño para cualquier de las funcionalidades, solamente el de valor más pequeño sera aceptado. 1.12) Permitir gestionar como controladora inalámbrica al menos 256 Access Points y gestionar por lo menos 64 Switches de la misma marca del fabricante del UTM/NGFW dentro de la misma interfase de gestion 1.13) Tener al menos 4 interfaces 10 Gbps SFPP, 8 interfases de 1 Gbps SFP, 16 interfases de 1GE RJ45, 2 interfases 1 Gbps RJ45 para Gestion y alta disponibilidad 1.15) Estar licenciado y/o tener incluído sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance 1.16) Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance 1.17) Debe de incluir un token fisico para autenticacion de doble factor para la gestion del appliance o para el acceso VPN que debe ser de la misma marca propuesta 1.18) Debe de 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus, Botnet IP/Domain, AntiSpam y Filtrado Web 1.19) Debe de contar con dos fuentes de poder AC de 100-240 VAC para alta disponibilidad 1.20) Deberá contar con 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema de firmware, y los siguientes módulos incluidos IPS ó Preventor de Intrusos, Antivirus , Protección contra Botnet IP/Domain, Módulo de Protección de Mobile Malware, Módulo de Sandbox en nube incluyendo Virus Outbreak and Content Disarm & Reconstruct, Control de aplicaciones, Filtrado Web & Video Filtering y Módulo de AntiSpam. **2) Requisitos Mínimos de Funcionalidad** **Características Generales** 2.1) 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. ; 2.2) Por funcionalidades de NGFW se entiende: aplicaciones de reconocimiento, prevención de amenazas, identificación de usuarios y control granular de permisos; 2.3) 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; 2.4) La plataforma debe estar optimizada para aplicaciones de análisis de contenido en la capa 7; 2.5) 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; 2.6) La gestión del equipo debe ser compatible con acceso a través de SSH, consola, web (HTTPS) y API abierta; 2.7) La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red 2.8) Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q; 2.9) Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP; 2.10) Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding; 2.11) Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM); 2.12) Los dispositivos de protección de red deben soportar DHCP Relay; 2.13) Los dispositivos de protección de red deben soportar DHCP Server; 2.14) Los dispositivos de protección de red deben soportar sFlow 2.15) Los dispositivos de protección de red deben soportar Jumbo Frames; 2.16) Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas 2.17) Debe ser compatible con NAT dinámica (varios-a-1); 2.18) Debe ser compatible con NAT dinámica (muchos-a-muchos); 2.19) Debe soportar NAT estática (1-a-1); 2.20) Debe admitir NAT estática (muchos-a-muchos); 2.21) Debe ser compatible con NAT estático bidireccional 1-a-1; 2.22) Debe ser compatible con la traducción de puertos (PAT); 2.23) Debe ser compatible con NAT Origen; 2.24) Debe ser compatible con NAT de destino;		

		2.25)	Debe soportar NAT de origen y NAT de destino de forma simultánea;		
		2.26)	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;		
		2.27)	Debe ser compatible con NAT64 y NAT46;		
		2.28)	Debe implementar el protocolo ECMP;		
		2.29)	Debe soportar el balanceo de enlace hash por IP de origen;		
		2.30)	Debe soportar el balanceo de enlace hash por IP de origen y destino;		
		2.31)	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;		
		2.32)	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales		
		2.33)	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		
		2.34)	Enviar logs a sistemas de gestión externos simultáneamente;		
		2.35)	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;		
		2.36)	Debe soporta protección contra la suplantación de identidad (anti-spoofing);		
		2.37)	Implementar la optimización del tráfico entre dos dispositivos;		
		2.38)	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);		
		2.39)	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);		
		2.40)	Soportar OSPF graceful restart;		
		2.41)	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);		
		2.42)	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;		
		2.43)	Debe soportar modo capa - 2 (L2) para la inspección de datos en línea y la visibilidad del tráfico;		
		2.44)	Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en línea de tráfico;		
		2.45)	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;		
		2.46)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;		
		2.47)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;		
		2.48)	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;		
		2.49)	La configuración de alta disponibilidad debe sincronizar: Sesiones;		
		2.50)	La configuración de alta disponibilidad debe sincronizar: configuración, incluyendo, pero no limitados políticas de Firewalls, NAT, QoS y objetos de la red;		
		2.51)	La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN;		
		2.52)	La configuración de alta disponibilidad debe sincronizar: Tablas FIB;		
		2.53)	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;		
		2.54)	Debe soportar la creación de sistemas virtuales en el mismo equipo;		
		2.55)	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;		
		2.56)	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;		
		2.57)	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;		
		2.58)	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 Politica de Firewall			
		2.59)	Debe soportar controles de zona de seguridad		
		2.60)	Debe contar con políticas de control por puerto y protocolo		
		2.61)	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		

			2.62)	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad		
			2.63)	Control de política por código de país (por ejemplo: BR, USA., UK, RUS)		
			2.64)	Control, inspección y des encriptación de SSL por política para el tráfico entrante y la salida		
			2.65)	Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada;		
			2.66)	Debe descifrar las conexiones de entrada y salida de tráfico negociadas con TLS 1.2;		
			2.67)	Control de inspección y descifrado SSH por política;		
			2.68)	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;		
			2.69)	Traffic shaping QoS basado en políticas (garantía de prioridad y máximo);		
			2.70)	QoS basado en políticas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones;		
			2.71)	Soporte para objetos y reglas IPV6;		
			2.72)	Soporte objetos y reglas de multicast;		
			2.73)	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 unreachable por la máquina fuente de tráfico, TCP Reset para el cliente , RESET de TCP con el servidor o en ambos lados de la conexión;		
			2.74)	Soportar la calendarización de políticas con el fin de activar y desactivar las reglas en tiempos predefinidos de forma automática;		
			Control de Aplicación			
			2.75)	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo		
			2.76)	Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos		
			2.77)	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;		
			2.78)	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;		
			2.79)	Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;		
			2.80)	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;		
			2.81)	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		
			2.82)	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;		
			2.83)	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		
			2.84)	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;		
			2.85)	Actualización de la base de firmas de la aplicación de forma automática;		
			2.86)	Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos;		
			2.87)	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;		
			2.88)	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;		
			2.89)	Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;		
			2.90)	Para mantener la seguridad de red eficiente debe ser soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;		
			2.91)	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		
			2.92)	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		
			2.93)	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;		
			2.94)	Debe alertar al usuario cuando sea bloqueada una aplicación;		
			2.95)	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;		

		2.96)	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;		
		2.97)	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;		
		2.98)	Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;		
		2.99)	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)		
		2.100)	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: nivel de riesgo de la aplicación		
		2.101)	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación		
		Prevención de Amenazas			
		2.102)	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;		
		2.103)	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);		
		2.104)	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;		
		2.105)	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad;		
		2.106)	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;		
		2.107)	Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo;		
		2.108)	Deben ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad		
		2.109)	Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas;		
		2.110)	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		
		2.111)	Deber permitir el bloqueo de vulnerabilidades		
		2.112)	Debe permitir el bloqueo de exploits conocidos		
		2.113)	Debe incluir la protección contra ataques de denegación de servicio		
		2.114)	Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones;		
		2.115)	Debe tener los siguientes mecanismos de inspección IPS: análisis de decodificación de protocolo;		
		2.116)	Debe tener los siguientes mecanismos de inspección IPS: análisis para detectar anomalías de protocolo;		
		2.117)	Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico;		
		2.118)	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;		
		2.119)	Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;		
		2.120)	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets)		
		2.121)	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones SYN, ICMP , UDP, etc;		
		2.122)	Detectar y bloquear los escaneos de puertos de origen;		
		2.123)	Bloquear ataques realizados por gusanos (worms) conocidos;		
		2.124)	Contar con firmas específicas para la mitigación de ataques DoS y DDoS;		
		2.125)	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);		
		2.126)	Debe poder crear firmas personalizadas en la interfaz gráfica del producto;		
		2.127)	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;		
		2.128)	Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;		
		2.129)	Soportar el bloqueo de archivos por tipo;		
		2.130)	Identificar y bloquear la comunicación con redes de bots;		
		2.131)	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;		

		2.132) Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación; 2.133) 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 2.134) 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; 2.135) Los eventos deben identificar el país que origino la amenaza; 2.136) Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms) 2.137) Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP 2.138) 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** 2.139) 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); 2.140) Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad 2.141) 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; 2.142) 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; 2.143) Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL 2.144) 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; 2.145) Tener por lo menos 60 categorías de URL; 2.146) Debe tener la funcionalidad de exclusión de URLs por categoría 2.147) Permitir página de bloqueo personalizada; 2.148) 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** 2.149) 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; 2.150) 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; 2.151) 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; 2.152) 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; 2.153) 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; 2.154) 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; 2.155) 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); 2.156) 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; 2.157) Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos del LDAP / AD 2.158) Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma. 2.159) Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores **QoS Traffic Shaping** 2.160) 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; 2.161) Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen; 2.162) Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;		

2.163) Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
2.164) Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
2.165) Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
2.166) QoS debe permitir la definición de tráfico con ancho de banda garantizado;
2.167) QoS debe permitir la definición de tráfico con máximo ancho de banda;
2.168) QoS debe permitir la definición de cola de prioridad;
2.169) Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype;
2.170) Soportar marcación de paquetes DiffServ, incluso por aplicación;
2.171) Soportar la modificación de los valores de DSCP para Diffserv;
2.172) Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service)
2.173) Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shapig;
2.174) Debe soportar QoS (traffic-shaping) en la interfaz agregada o redundantes;

Filtro de Datos

2.175) Permite la creación de filtros para archivos y datos predefinidos;
2.176) Los archivos deben ser identificados por tamaño y tipo;
2.177) Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);
2.178) Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
2.179) Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
2.180) 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

2.181) Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
2.182) Debe permitir la visualización de los países de origen y destino en los registros de acceso;
2.183) Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

VPN

2.184) Soporte VPN de sitio a sitio y cliente a sitio;
2.185) Soportar VPN IPSec;
2.186) Soportar VPN SSL;
2.187) La VPN IPSec debe ser compatible con 3DES;
2.188) La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;
2.189) La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y el Grupo 14;
2.190) La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
2.191) La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
2.192) La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI
2.193) Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
2.194) Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec
2.195) Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;
2.196) 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;
2.197) Las características de VPN SSL se deben cumplir con o sin el uso de agentes;
2.198) 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;

		2.199) Asignación de DNS en la VPN de cliente remoto; 2.200) 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; 2.201) Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local; 2.202) Suportar lectura y revisión de CRL (lista de revocación de certificados); 2.203) Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL; 2.204) Debe permitir que la conexión a la VPN se establece de la siguiente manera: Antes de que el usuario se autentique en su estación 2.205) Debería permitir la conexión a la VPN se establece de la siguiente manera: Después de la autenticación de usuario en la estación; 2.206) Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo demanda de los usuarios; 2.207) Deberá mantener una conexión segura con el portal durante la sesión; 2.208) 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** 2.209) Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada 2.210) Soportar servicio del servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos 2.211) Soporte IPv4 e IPv6 por SSID 2.212) 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 2.213) Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point 2.214) Soportar monitoreo y supresión de puntos de acceso indebidos 2.215) Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS 2.216) Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows 2.217) Permitir la visualización de los dispositivos inalámbricos conectados por usuario 2.218) Permitir la visualización de los dispositivos inalámbricos conectados por IP 2.219) Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación 2.220) Permitir la visualización de los dispositivos inalámbricos conectados por canal 2.221) Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado 2.222) Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal 2.223) Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación 2.224) Debe soportar Fast Roaming en autenticación con portal cautivo 2.225) Debe soportar configuración de portal cautivo por SSID 2.226) Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico 2.227) Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP. 2.228) Debe ser compatible con el protocolo 802.1x RADIUS 2.229) La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal 2.230) La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática 2.231) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática 2.232) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP 2.233) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por dns 2.234) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por broadcast 2.235) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por multicast 2.236) La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue)		

		2.237)	La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico		
		2.238)	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		
		2.239)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP		
		2.240)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding		
		2.241)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding		
		2.242)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication		
		2.243)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding		
		2.244)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI		
		2.245)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack		
		2.246)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response		
		2.247)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication		
		2.248)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection		
		2.249)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge		
		2.250)	Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas		
		2.251)	Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso		
		2.252)	La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible		
		2.253)	La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario		
		2.254)	Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID		
		2.255)	Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso		
		2.256)	Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio		
		2.257)	La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh		
		2.258)	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		
		2.259)	La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS		
		2.260)	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		
		2.261)	Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso		
		2.262)	Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso		
		2.263)	Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica;		
		2.264)	Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión		
		2.265)	Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados		
		2.266)	La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz		
		2.267)	Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados		
		2.268)	Debe permitir asociación dinámicas de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS		
		2.269)	Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling		
		2.270)	Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico		
		2.271)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones		
		2.272)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino		
		2.273)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza		
		2.274)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones		
		2.275)	la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico		

		2.276) El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo 2.277) El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales 2.278) La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico 2.279) La controladora inalámbrica deberá soportar aceleración de tunnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico 2.280) La controladora inalámbrica debe soportar protocolo LLDP 2.281) Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta 2.282) Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC Adyacente 2.283) Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos 2.284) La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado 2.285) La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas 2.286) La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada 2.287) Deberá soportar la conversion de Multicast a Unicast para mejorar el rendimiento del tiempo de aire		
3	1	**SOLUCIÓN DE ADMNISTRACION CENTRALIZADA SD-WAN UTM/NGFW Y SOLUCIÓN DE CORRELACION DE LOGS Y INCIDENTES DE SEGURIDAD SD-WAN UTM/NGFW** **1) Solución de Administración Centralizada** 1.1) Solución de Administracion centralizada de Dispositivos SD-WAN UTM/NGFW con Licenciamiento de Actualizaciones de Firmware, soporte 24x7 por 60 meses. 1.2) La solución deberá ser escalable en 10, 100 y hasta 1000 dispositivos , con soporte en Hypervisor Vmware, Microsoft HyperV, Xen Server, KVM 1.3) Debe permitir gerenciar al menos 100 dispositivos **2) Requisitos Mínimos de Funcionalidad** **Funcionalidades Generales** 2.1) Debe permitir Gerenciar los dispositivos de la misma marca que los equipos ofertados, generando politicas centralizadas, control de cambios, revision de versiones, respaldos de configuracion y perfiles de usuarios 2.2) Si la solución es virtualizada, debe ser compatible con el ambiente VMware ESXi 5.5 e 6.0; 2.3) Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2 2.4) Si la solución es virtualizada, debe ser compatible con el ambiente Citrix XenServer 6.0+ 2.5) Si la solución es virtualizada, debe ser compatible con el ambiente Open Source Xen 4.1+ 2.6) Si la solución es virtualizada, debe ser compatible con el ambiente KVM 2.7) Si la solución es virtualizada, debe ser compatible con el ambiente Amazon Web Services (AWS) 2.8) No debe haber límites a la cantidad de múltiples vCPU si el aparato es virtual; 2.9) No debe haber límites a la expansión de memória RAM si el aparto es virtual; 2.10) En la fecha de la propuesta, ninguno de los modelos de la oferta pueden estar en el sítio del fabricante en listados de end-of-life o end-of-sales; 2.11) La gestión de la solición debe soportar aceso por SSH, cliente o WEB (HTTPS) y API abierta; 2.12) Debe permitir aceso concurrentes de administradores; 2.13) Debe tener interfaz basada en línea de comando para administración de la solución de gestión; 2.14) Debe tener un mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos; 2.15) Bloquear cambios, en el caso de acceso simultaneo de dos o más administradores; 2.16) Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, accesso de lectura, creación de usuários, cambio de configuraciones; 2.17) Generar alertas automáticos por Email 2.18) Generar alertas automáticos por SNMP 2.19) Generar alertas automáticos por Syslog 2.20) Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horário; 2.21) Debe ser permitido al administrador transferir los backups a un servidor FTP. 2.22) Debe ser permitido al administrador transferir los backups a un servidor SCP 2.23) Debe ser permitido al administrador transferir los backups a un servidor SFTP 2.24) Los cambios realizados en un servidor de gestión debe ser automaticamente replicados al servidor redundante; 2.25) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de cuentas de usuários LOCALES 2.26) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa TACACS 2.27) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa LDAP 2.28) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa RADIUS 2.29) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de Certificado Digital X.509 (PKI) 2.30) Debe soportar sincronización de reloj interno por protocolo NTP. 2.31) Debe registrar las acciones efectuadas por cualquier usuário; 2.32) Deben ser fornecidos manuales de instalación, configuración y operación de toda la solución, e los idiomas portugués o inglés, com apresentación de buena calidad; 2.33) Debe suportar SNMP versión 2 y la versión 3 en los equipos de gestión; 2.34) Debe permitir habilitar o deshabilitar, para cada interfaz de red de la solución de gestión, permisos de acceso HTTP, HTTPS, SSH, SNMP y Telnet; 2.35) Debe permitir virtualizar la solución de gestión, de manera que cada administrador pueda gerenciar, visualizar y editar solo los dispositivos autorizados y registrados en su ambiente virtualizado; 2.36) La solución de gestión debe permitir crear administradores que tengan acceso a todas las instancias de virtualización; **Funcionalidades de APIs** 2.37) Debe soportar XML API 2.38) Debe soportar JSON API **Funcionalidades de Gestión de SDWAN UTM/NGFW** 2.39) La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación; 2.40) La gestión debe permitir la creación y administración de políticas de IPS, Antivírus y Anti-Spyware;		

2.41) La gestión debe permitir la creación y administración de políticas de Filtro de URL;
2.42) Permitir buscar cuáles reglas un objeto está siendo utilizado;
2.43) Debe atribuir secuencialmente un número a cada regla de firewall;
2.44) Debe atribuir secuencialmente un número a cada regla de firewall;DOS;
2.45) Permitir la creación de reglas que permanezcan activas en horário definido;
2.46) Permitir backup de las configuraciones y rollback de configuración para la última configuración salva;
2.47) Debe tener mecanismos de validación de políticas avisando cuando hayan reglas que ofusquen o conflictuen con otras (shadowing);
2.48) Debe posibilitar la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas;
2.49) Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión;
2.50) Cada servidor de gestión debe ser hospedado en un equipo independiente, no ejecutando función de firewall;
2.51) La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador atualizar licencias en los aparatos a través de esta herramienta;
2.52) La solución debe permitir la distribución y instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos;
2.53) Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados;
2.54) Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas despuez de la aprobación de otro administrador;
2.55) Tener "wizard" en la solución de gestion para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de los mismos;
2.56) Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados cuando el mismo es agregado a la solución de gestión;
2.57) Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horário de lo sistema y firmware;
2.58) Tener "wizard" en la solución de gestion para instalación de políticas y configuraciones de los dispositivos;
2.59) Permitir crear en la solución de gestión templates de configuración de los dispositivos con informadiones de DNS, SNMP, configuraciones de LOG y administración;
2.60) Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos;
2.61) Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión;
2.62) Permitir configurar y visualizar balanceo de enlaces en los dispositivos gestionados de forma centralizada;
2.63) Permitir crear vários paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos;
2.64) Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada;
2.65) Permitir la creación de reglas anti DoS de forma centralizada;
2.66) Permitir la creación de objetos que serán utilizados en las políticas de forma centralizada;
2.67) Permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topologia (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía;
2.68) Permitir la utilizacion de Zero Touch Provisioning para automatizar las configuraciones de los Dispositivos administrados
2.69) Permitir la utilizacion de Plantillas para automatizar la configuracion de los Modulos de SD-WAN de los dispositivos Gerenciados

1) Características
1.1) Solución de Correlación de Logs centralizada de Dispositivos SD-WAN UTM/NGFW con Licenciamiento de Actualizaciones de Sistema de Firmware, soporte 24x7 por 60 meses.
1.2) Tener capacidad de recibir al menos 50 GBytes de logs diarios
1.3) Deberá Soportar Identificadores de Compromiso
1.4) Deberá soportar módulo de SoC
1.5) Soportar módulo de "Outbreak Alert Service"
1.6) Deberá ser por cuestiones de compatibilidad , la misma marca que los dispositivos SD-WAN UTM / NGFW
1.7) La solución debe ser escalable o stackeable en 5GB/50GB/500 GB logs al día
2) Requisitos Mínimos de Funcionalidad
Funcionalidades Generales
2.1) Si la solución es virtualizada, debe ser compatible con el ambiente VMware ESXi 5.0/5.1/5.5/6.0/6.5/6.7;
2.2) Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2/2016
2.3) Si la solución es virtualizada, debe ser compatible con el ambiente Citrix XenServer 6.0+
2.4) Si la solución es virtualizada, debe ser compatible con el ambiente Open Source Xen 4.1+
2.5) Si la solución es virtualizada, debe ser compatible con el ambiente KVM on Redhat 6.5+ and Ubuntu 17.04
2.6) Si la solución es virtualizada, debe ser compatible con el ambiente Nutanix AHV (AOS 5.10.5)
2.7) Si la solución es virtualizada, debe ser compatible con el ambiente Amazon Web Services (AWS)
2.8) Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Azure.
2.9) Si la solución es virtualizada, debe ser compatible con el ambiente Google Cloud (GCP)
2.10) Si la solución es virtualizada, debe ser compatible con el ambiente Oracle Cloud Infrastructure (OCI)
2.11) Si la solución es virtualizada, debe ser compatible con el ambiente Alibaba Coud (AliCloud)
2.12) Si la solución es virtualizada, no debe haber límites a la cantidad de múltiples vCPU
2.13) Si la solución es virtualizada, no debe haber límites a la expansión de memoria RAM
2.14) Debe soportar acceso vía SSH, WEB (HTTPS) para la gestion de la solución
2.15) Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía linea de comandos en consola de gestión.
2.16) Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
2.17) Soporte SNMP versión 2 y 3
2.18) Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
2.19) Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
2.20) Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH
2.21) Autenticación de usuarios de acceso a la plataforma via LDAP
2.22) Autenticación de usuarios de acceso a la plataforma via Radius
2.23) Autenticación de usuarios de acceso a la plataforma via TACACS+
2.24) Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos
2.25) Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
2.26) Generación de informes en tiempo real de tráfico, en formato de gráfica tabla
2.27) Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
2.28) Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.

2.29) Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado
2.30) Contar con mecanismos de borrado automático de logs antiguos.
2.31) Permitir la importación y exportación de reportes
2.32) Debe contar con la capacidad de crear informes en formato HTML
2.33) Debe contar con la capacidad de crear informes en formato PDF
2.34) Debe contar con la capacidad de crear informes en formato XML
2.35) Debe contar con la capacidad de crear informes en formato CSV
2.36) Debe permitir exportar los logs en formato CSV
2.37) Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
2.38) Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
2.39) La solución debe contar con reportes predefinidos
2.40) Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución
2.41) Debe ser posible la duplicación de reportes existentes para su posterior edición.
2.42) Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
2.43) Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
2.44) Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
2.45) Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
2.46) Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
2.47) Debe permitir descargar de la plataforma los archivos de logs para uso externo.
2.48) Tener la capacidad de generar y enviar reportes periódicos automáticamente.
2.49) Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
2.50) Permitir el envío por email de manera automática de reportes.
2.51) Debe permitir que el reporte a enviar por email sea al destinatario específico.
2.52) Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
2.53) Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
2.54) Debe permitir el uso de filtros en los reportes.
2.55) Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
2.56) Permitir especificar el idioma de los reportes creados
2.57) Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
2.58) Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
2.59) Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.
2.60) Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
2.61) Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.
2.62) Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
2.63) Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
2.64) Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
2.65) Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
2.66) Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos
2.67) Debe permitir visualizar en tiempo real los logs recibidos.
2.68) Debe permitir el reenvío de logs en formato syslog.
2.69) Debe permitir el reenvío de logs en formato CEF (Common Event Format).
2.70) Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red
2.71) Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
2.72) Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.
2.73) Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red
2.74) Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
2.75) Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.
2.76) Debe incluir dashboard para operaciones SOC que monitorea actividad VPN ren su red.
2.77) Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs
2.78) Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)
2.79) Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC
2.80) Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3
2.81) Debe permitir generar alertas de eventos a partir de logs recibidos
2.82) Debe permitir crear incidentes a partir de alertas de eventos para endpoint
2.83) Debe permitir la integración al sistema de tickets ServiceNow
2.84) Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
2.85) Debe permitir respaldar logs en nube publica de Amazon S3
2.86) Debe permitir respaldar logs en nube publica de Microsoft Azure
2.87) Debe permitir respaldar logs en nube publica de Gooogle Cloud
2.88) Debe soportar el estándar SAML para autenticación de usuarios administradores

Reportes de Firewall

2.89) Debe contar con reporte de cumplimiento de PCI DSS
2.90) Debe contar con reporte de utilización de aplicaciones SaaS
2.91) Debe contar con reporte de prevención de perdida de datos (DLP)
2.92) Debe contar con reporte de VPN
2.93) Debe contar con reporte de Sistema de prevención de intrusos (IPS)
2.94) Debe contar con reporte de reputación de cliente
2.95) Debe contar con reporte de análisis de seguridad de usuario
2.96) Debe contar con reporte de análisis de amenaza cibernética
2.97) Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad
2.98) Debe contar con reporte de tráfico DNS
2.99) Debe contar con reporte tráfico de correo electrónico
2.100) Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red

		2.101) Debe contar con reporte de Top 10 de Websites utilizadas en la red 2.102) Debe contar con reporte de uso de redes sociales **Reportes de Fabric** 2.103) Debe contar con reporte de evaluación de riesgo para correo electrónico **Reportes de Wireless** 2.104) Debe contar con reporte de cumplimiento PCI de Wireless. 2.105) Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WIFi **Reportes de Endpoint** 2.106) Debe contar con reporte de vulnerabilidades de solución gestionada de seguridad de equipo terminal. **Reportes de WAF** 2.107) Debe contar con reporte de aplicaciónes web, si se cuenta con plataforma de seguridad web **Reportes de SD-WAN** Debe de contar con reportes de la utilizacion del modulo de SD-WAN de los dispositivos que realicen la correlacion en la solución..		
SUBTOTAL				
IVA				
TOTAL				

Condiciones de pago:
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**
- **En los precios ofertados deberá de considerarse el costo de flete para la entrega a cada dependencia beneficiada.**

A T E N T A M E N T E

_____, Jalisco; a _____de _____ 2021

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

ANEXO PARA LA PROPUESTA ECONÓMICA

Condiciones para el participante:

1. El participante deberá incluir en su propuesta carta original expedida por el fabricante constatando su estado actual de revendedor autorizado con mínimo nivel advanced.

2. El participante deberá incluir en su propuesta carta original expedida por el fabricante constatando el personal certificado Network Security Expert

a. Al menos 1 NSE4
b. Al menos 1 NSE5
c. Al Menos 1 NSE7

3. El participante deberá incluir en su propuesta carta original expedida por el representante legal del fabricante/mayorista sobre sus capacidades de implementación y experiencia en proyectos similares al presente concurso.

FORMATO PARA PROPUESTA TÉCNICA

PARTIDA	CANTIDAD	DESCRIPCIÓN TÉCNICA COTIZADA EN PROPUESTA ECONÓMICA
1	**29**	
2	**41**	
3	**1**	

Nota:

Se deberán anexar folletos y/o manuales que ilustren su propuesta

A T E N T A M E N T E

_____, Jalisco; a _____de _____ 2021

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

SECCION IV

CARTA DE SERIEDAD DE LA PROPUESTA

Licitación Pública No. LI-SEMS-010-2021

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 24 de septiembre 2021, mediante la cual se invita a participar en la Licitación Pública arriba indicada, relativa a la ADQUISICIÓN DE EQUIPO DE SOLUCIÓN DE SEGURIDAD UTM/NGFW, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA. , 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 _____ 2021

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

Sección V

CARTA COMPROMISO

Licitación Pública No. LI-SEMS-010-2021

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 EQUIPO DE SOLUCIÓN DE SEGURIDAD UTM/NGFW, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA., 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, ante una institución legalmente autorizada para emitirla, correspondiente al 10% del monto total adjudicado en el contrato respectivo, para asegurar su debido cumplimiento.

Si nuestra oferta es aceptada, contrataremos a favor de la Universidad de Guadalajara una fianza, ante una institución legalmente autorizada para emitirla, correspondiente al 100% del monto total que se reciba por concepto de anticipo, para garantizar la correcta aplicación de los recursos del anticipo. (Anticipo máximo 30%).

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 2021

_____

NOMBRE Y FIRMA
REPRESENTANTE LEGAL DE LA EMPRESA O PERSONA FÍSICA

UNIVERSIDAD DE GUADALAJARA
Sistema de Educación Media Superior
Secretaría Administrativa
Coordinación de Cómputo e Informática

SEMS/CCEI/0097/21
ASUNTO: Administrativas

Ing. Fernando Calvillo Vargas
Coordinador de Servicios Generales del SEMS
Presente.

Por medio del presente le envío un cordial saludo, asimismo y en respuesta a su oficio SEMS/CSG/0651/2021 fechado el día 13 de octubre 2021, anexo dictamen técnico de las propuestas de las empresas que se presentaron en el concurso No. LI-SEMS-010-2021 denominado "ADQUISICIÓN DE EQUIPO DE SOLUCION DE SEGURIDAD UTM/NGFW, PARA EL SISTEMA DE EDUCACION MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA."

Sin más por el momento, me despido reiterándoles mis más distinguidas consideraciones.

Atentamente
"Piensa y Trabaja"
"Año del legado de Fray Antonio Alcalde en Guadalajara"
Guadalajara, Jalisco; 14 de Octubre de 2021

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

Ing. María Esmeralda Olmos de la Cruz
Coordinación de Cómputo e Informática

Ocmej/mmm

DICTAMEN TÉCNICO

Fecha 14 de octubre de 2021

LICITACIÓN: LI-SEMS-010-2021
DEPENDENCIA: SISTEMA DE EDUCACION MEDIA SUPERIOR
NOMBRE: ADQUISICIÓN DE EQUIPO DE SOLUCIÓN DE SEGURIDAD UTM/NGFW, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA.
1.- Relación de las proposiciones declaradas solventes, porque cumplen con todos los requisitos técnicos solicitados:

EMPRESAS
INITEL, S.A. DE C.V.
SODENET, S. DE RL. DE C.V.

PARTIDA 1

	SOLUCIÓN UTM/NGFW "TIPO A"
1.1)	Throughput de por lo menos 24 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete
1.2)	Soporte a por lo menos 4M conexiones simultaneas
1.3)	Soporte a por lo menos 450K nuevas conexiones por segundo
1.4)	Throughput de al menos 20 Gbps de VPN IPSec
1.5)	Estar licenciado para, o soportar sin necesidad de licencia, 2K tuneles de VPN IPSec site-to-site simultaneos
1.6)	Estar licenciado para, o soportar sin necesidad de licencia, 50K tuneles de clientes VPN IPSec simultaneos
1.7)	Throughput de al menos 4500 Mbps de VPN SSL
1.8)	Soportar al menos 5000 clientes de VPN SSL simultaneos
1.9)	Soportar al menos 7800 Mbps de throughput de IPS
1.10)	Soportar al menos 4000 Mbps de throughput de Inspeción SSL
1.11)	Throughput de al menos 5000 Mbps con las siguientes funcionalidades habilitadas simultaneamente para todas las firmas que la solución de seguridad tenga debidamente activadasy operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado multiples numeros de disempeño para cualquier de las funcionalidades, solamente el de valor más pequeño sera aceptado.
1.12)	Permitir gestionar como controladora inalámbrica al menos 512 Access Points y gestionar por lo menos 72 Switches de la misma marca del fabricante del UTM/NGFW dentro de la misma interfase de gestión
1.13)	Tener al menos 4 interfaces 10 Gbps SFPP, 8 interfases de 1 Gbps SFP, 16 interfases de 1GE RJ25, 2 interfases 1 Gbps RJ45 para Gestion y alta disponibilidad
1.15)	Estar licenciado y/o tener incluído sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance
1.16)	Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance

1.17)	Debe de incluir un token fisico para autenticacion de doble factor para la gestion del appliance o para el acceso VPN que debe ser de la misma marca propuesta
1.18)	Debe de 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus, Botnet IP/Domain, AntiSpam y Filtrado Web
1.19)	Debe de contar con una fuente de poder AC de 100-240 VAC, con la posibilidad de agregar una segunda para alta disponibilidad
1.20)	Deberá contar con 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema de firmware, y los siguientes módulos incluidos IPS ó Preventor de Intrusos, Antivirus , Protección contra Botnet IP/Domain, Módulo de Protección de Mobile Malware, Módulo de Sandbox en nube incluyendo Virus Outbreak and Content Disarm & Reconstruct, Control de aplicaciones, Filtrado Web & Video Filtering y Módulo de AntiSpam.

2) Requisitos Mínimos de Funcionalidad

Características Generales

2.1)	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;
2.2)	Por funcionalidades de NGFW se entiende: aplicaciones de reconocimiento, prevención de amenazas, identificación de usuarios y control granular de permisos;
2.3)	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;
2.4)	La plataforma debe estar optimizada para aplicaciones de análisis de contenido en la capa 7;
2.5)	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;
2.6)	La gestión del equipo debe ser compatible con acceso a través de SSH, consola, web (HTTPS) y API abierta;
2.7)	La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
2.8)	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
2.9)	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
2.10)	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
2.11)	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
2.12)	Los dispositivos de protección de red deben soportar DHCP Relay;
2.13)	Los dispositivos de protección de red deben soportar DHCP Server;
2.14)	Los dispositivos de protección de red deben soportar sFlow
2.15)	Los dispositivos de protección de red deben soportar Jumbo Frames;
2.16)	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas
2.17)	Debe ser compatible con NAT dinámica (varios-a-1);
2.18)	Debe ser compatible con NAT dinámica (muchos-a-muchos);
2.19)	Debe soportar NAT estática (1-a-1);
2.20)	Debe admitir NAT estática (muchos-a-muchos);
2.21)	Debe ser compatible con NAT estático bidireccional 1-a-1;
2.22)	Debe ser compatible con la traducción de puertos (PAT);
2.23)	Debe ser compatible con NAT Origen;
2.24)	Debe ser compatible con NAT de destino;
2.25)	Debe soportar NAT de origen y NAT de destino de forma simultánea;
2.26)	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
2.27)	Debe ser compatible con NAT64 y NAT46;
2.28)	Debe implementar el protocolo ECMP;
2.29)	Debe soportar el balanceo de enlace hash por IP de origen;
2.30)	Debe soportar el balanceo de enlace hash por IP de origen y destino;

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.31) 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;

2.32) Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales

2.33) 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

2.34) Enviar logs a sistemas de gestión externos simultáneamente;

2.35) Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;

2.36) Debe soporta protección contra la suplantación de identidad (anti-spoofing);

2.37) Implementar la optimización del tráfico entre dos dispositivos;

2.38) Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);

2.39) Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);

2.40) Soportar OSPF graceful restart;

2.41) 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);

2.42) Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;

2.43) Debe soportar modo capa - 2 (L2) para la inspección de datos en línea y la visibilidad del tráfico;

2.44) Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en línea de tráfico;

2.45) Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;

2.46) Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;

2.47) Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;

2.48) Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;

2.49) La configuración de alta disponibilidad debe sincronizar: Sesiones;

2.50) La configuración de alta disponibilidad debe sincronizar: configuración, incluyendo, pero no limitados políticas de Firewalls, NAT, QoS y objetos de la red;

2.51) La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN;

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.52) La configuración de alta disponibilidad debe sincronizar: Tablas FIB;

2.53) En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;

2.54) Debe soportar la creación de sistemas virtuales en el mismo equipo;

2.55) 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;

2.56) 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;

2.57) 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;

2.58) 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

2.59) Debe soportar controles de zona de seguridad

2.60) Debe contar con políticas de control por puerto y protocolo

2.61) 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

2.62) Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad

2.63) Control de política por código de país (por ejemplo: BR, USA., UK, RUS)

2.64) Control, inspección y des encriptación de SSL por política para el tráfico entrante y la salida

2.65) Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada;

2.66) Debe descifrar las conexiones de entrada y salida de tráfico negociadas con TLS 1.2;

2.67) Control de inspección y descifrado SSH por política;

2.68) 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;

2.69) Traffic shaping QoS basado en políticas (garantía de prioridad y máximo);

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.70) QoS basado en políticas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones;

2.71) Soporte para objetos y reglas IPV6;

2.72) Soporte objetos y reglas de multicast;

2.73) 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 unreachable por la máquina fuente de tráfico, TCP Reset para el cliente , RESET de TCP con el servidor o en ambos lados de la conexión;

2.74) Soportar la calendarización de políticas con el fin de activar y desactivar las reglas en tiempos predefinidos de forma automática;

Control de Aplicación

2.75) Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo

2.76) Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos

2.77) 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;

2.78) 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;

2.79) Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;

2.80) 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;

2.81) 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

2.82) 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;

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.83) 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

2.84) Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;

2.85) Actualización de la base de firmas de la aplicación de forma automática;

2.86) Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos;

2.87) 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;

2.88) 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;

2.89) Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;

2.90) Para mantener la seguridad de red eficiente debe ser soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;

2.91) 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

2.92) 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

2.93) El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;

2.94) Debe alertar al usuario cuando sea bloqueada una aplicación;

2.95) Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;

2.96) Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.97) Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;

2.98) Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;

2.99) 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)

2.100) Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: nivel de riesgo de la aplicación

2.101) Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación

Prevención de Amenazas

2.102) Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;

2.103) Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);

2.104) 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;

2.105) Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad;

2.106) 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;

2.107) Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo;

2.108) Deben ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad

2.109) Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas;

2.110) 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

2.111) Deber permitir el bloqueo de vulnerabilidades

2.112) Debe permitir el bloqueo de exploits conocidos

2.113) Debe incluir la protección contra ataques de denegación de servicio

2.114) Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones;

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.115) Debe tener los siguientes mecanismos de inspección IPS: análisis de decodificación de protocolo;

2.116) Debe tener los siguientes mecanismos de inspección IPS: análisis para detectar anomalías de protocolo;

2.117) Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico;

2.118) Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;

2.119) Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;

2.120) Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets)

2.121) Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones SYN, ICMP , UDP, etc;

2.122) Detectar y bloquear los escaneos de puertos de origen;

2.123) Bloquear ataques realizados por gusanos (worms) conocidos;

2.124) Contar con firmas específicas para la mitigación de ataques DoS y DDoS;

2.125) Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);

2.126) Debe poder crear firmas personalizadas en la interfaz gráfica del producto;

2.127) 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;

2.128) Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;

2.129) Soportar el bloqueo de archivos por tipo;

2.130) Identificar y bloquear la comunicación con redes de bots;

2.131) 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;

2.132) Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;

2.133) 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

2.134) 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;

2.135) Los eventos deben identificar el país que origino la amenaza;

2.136) Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms)

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.137) Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP

2.138) 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

2.139) 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);

2.140) Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad

2.141) 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;

2.142) 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;

2.143) Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL

2.144) 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;

2.145) Tener por lo menos 60 categorías de URL;

2.146) Debe tener la funcionalidad de exclusión de URLs por categoría

2.147) Permitir página de bloqueo personalizada;

2.148) 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

2.149) 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;

2.150) 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;

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.151) 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;

2.152) 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;

2.153) 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;

2.154) 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;

2.155) 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);

2.156) 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;

2.157) Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos del LDAP / AD

2.158) Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.

2.159) Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores

QoS Traffic Shaping

2.160) 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;

2.161) Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;

2.162) Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.163) Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;

2.164) Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;

2.165) Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;

2.166) QoS debe permitir la definición de tráfico con ancho de banda garantizado;

2.167) QoS debe permitir la definición de tráfico con máximo ancho de banda;

2.168) QoS debe permitir la definición de cola de prioridad;

2.169) Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype;

2.170) Soportar marcación de paquetes DiffServ, incluso por aplicación;

2.171) Soportar la modificación de los valores de DSCP para Diffserv;

2.172) Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service)

2.173) Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shapig;

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

Filtro de Datos

2.175) Permite la creación de filtros para archivos y datos predefinidos;

2.176) Los archivos deben ser identificados por tamaño y tipo;

2.177) Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);

2.178) Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;

2.179) Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;

2.180) 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

2.181) Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;

2.182) Debe permitir la visualización de los países de origen y destino en los registros de acceso;

2.183) Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

VPN

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.184) Soporte VPN de sitio a sitio y cliente a sitio;

2.185) Soportar VPN IPSec;

2.186) Soportar VPN SSL;

2.187) La VPN IPSec debe ser compatible con 3DES;

2.188) La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;

2.189) La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y el Grupo 14;

2.190) La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);

2.191) La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);

2.192) La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI

2.193) Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

2.194) Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec

2.195) Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;

2.196) 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;

2.197) Las características de VPN SSL se deben cumplir con o sin el uso de agentes;

2.198) 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;

2.199) Asignación de DNS en la VPN de cliente remoto;

2.200) 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;

2.201) Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;

2.202) Suportar lectura y revisión de CRL (lista de revocación de certificados);

2.203) Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;

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

2.205) Debería permitir la conexión a la VPN se establece de la siguiente manera: Después de la autenticación de usuario en la estación;

2.206) Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo demanda de los usuarios;

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.207) Deberá mantener una conexión segura con el portal durante la sesión;

2.208) 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

2.209) Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada

2.210) Soportar servicio del servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos

2.211) Soporte IPv4 e IPv6 por SSID

2.212) 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

2.213) Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point

2.214) Soportar monitoreo y supresión de puntos de acceso indebidos

2.215) Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS

2.216) Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows

2.217) Permitir la visualización de los dispositivos inalámbricos conectados por usuario

2.218) Permitir la visualización de los dispositivos inalámbricos conectados por IP

2.219) Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación

2.220) Permitir la visualización de los dispositivos inalámbricos conectados por canal

2.221) Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado

2.222) Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal

2.223) Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación

2.224) Debe soportar Fast Roaming en autenticación con portal cautivo

2.225) Debe soportar configuración de portal cautivo por SSID

2.226) Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico

2.227) Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP.

2.228) Debe ser compatible con el protocolo 802.1x RADIUS

2.229) La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.230) La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática

2.231) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática

2.232) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP

2.233) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por dns

2.234) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por broadcast

2.235) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por multicast

2.236) La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue)

2.237) La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico

2.238) 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

2.239) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP

2.240) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding

2.241) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding

2.242) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication

2.243) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding

2.244) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI

2.245) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack

2.246) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response

2.247) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication

2.248) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection

2.249) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge

2.250) Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas

2.251) Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso

2.252) La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible

2.253) La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario

2.254) Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID

2.255) Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso

2.256) Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio

2.257) La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.258) 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

2.259) La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS

2.260) 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

2.261) Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso

2.262) Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso

2.263) Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica;

2.264) Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión

2.265) Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados

2.266) La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz

2.267) Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados

2.268) Debe permitir asociación dinámicas de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS

2.269) Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling

2.270) Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico

2.271) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones

2.272) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino

2.273) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza

2.274) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones

2.275) la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico

2.276) El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.277) El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales

2.278) La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico

2.279) La controladora inalámbrica deberá soportar aceleración de tunnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico

2.280) La controladora inalámbrica debe soportar protocolo LLDP

2.281) Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta

2.282) Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC Adyacente

2.283) Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos

1 2.284) La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado

2.285) La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas

2.286) La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada

2.287) Deberá soportar la conversion de Multicast a Unicast para mejorar el rendimiento del tiempo de aire

INITEL, S.A. DE C.V.	SODENET, S. DE RL. DE C.V.
CUMPLE	CUMPLE

PARTIDA 2

SOLUCIÓN UTM/NGFW "TIPO B"

1.1) Throughput de por lo menos 11 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete

1.2) Soporte a por lo menos 3M conexiones simultaneas

1.3) Soporte a por lo menos 280K nuevas conexiones por segundo

1.4) Throughput de al menos 13 Gbps de VPN IPSec

1.5) Estar licenciado para, o soportar sin necesidad de licencia, 2K tuneles de VPN IPSec site-to-site simultaneos

1.6) Estar licenciado para, o soportar sin necesidad de licencia, 16K tuneles de clientes VPN IPSec simultaneos

1.7) Throughput de al menos 2000 Mbps de VPN SSL

1.8) Soportar al menos 500 clientes de VPN SSL simultaneos

1.9) Soportar al menos 5000 Mbps de throughput de IPS

1.10) Soportar al menos 4000 Mbps de throughput de Inspeción SSL

1.11) Throughput de al menos 3000 Mbps con las siguientes funcionalidades habilitadas simultaneamente para todas las firmas que la solución de seguridad tenga debidamente activadasy operativas: control de aplicaciones, IPS, Antivírus y Antispyware. Caso el fabricante tenga publicado multiples numeros de disempeño para cualquier de las funcionalidades, solamente el de valor más pequeño sera aceptado.

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

1.12)	Permitir gestionar como controladora inalámbrica al menos 256 Access Points y gestionar por lo menos 64 Switches de la misma marca del fabricante del UTM/NGFW dentro de la misma interfase de gestion
1.13)	Tener al menos 4 interfaces 10 Gbps SFPP, 8 interfases de 1 Gbps SFP, 16 interfases de 1GE RJ45, 2 interfases 1 Gbps RJ45 para Gestion y alta disponibilidad
1.15)	Estar licenciado y/o tener incluído sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance
1.16)	Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance
1.17)	Debe de incluir un token fisico para autenticacion de doble factor para la gestion del appliance o para el acceso VPN que debe ser de la misma marca propuesta
1.18)	Debe de 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus, Botnet IP/Domain, AntiSpam y Filtrado Web
1.19)	Debe de contar con dos fuentes de poder AC de 100-240 VAC para alta disponibilidad
1.20)	Deberá contar con 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema de firmware, y los siguientes módulos incluidos IPS ó Preventor de Intrusos, Antivirus , Protección contra Botnet IP/Domain, Módulo de Protección de Mobile Malware, Módulo de Sandbox en nube incluyendo Virus Outbreak and Content Disarm & Reconstruct, Control de aplicaciones, Filtrado Web & Video Filtering y Módulo de AntiSpam.

2) Requisitos Mínimos de Funcionalidad

Características Generales

2.1)	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. ;
2.2)	Por funcionalidades de NGFW se entiende: aplicaciones de reconocimiento, prevención de amenazas, identificación de usuarios y control granular de permisos;
2.3)	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;
2.4)	La plataforma debe estar optimizada para aplicaciones de análisis de contenido en la capa 7;
2.5)	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;
2.6)	La gestión del equipo debe ser compatible con acceso a través de SSH, consola, web (HTTPS) y API abierta;
2.7)	La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
2.8)	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
2.9)	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
2.10)	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
2.11)	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
2.12)	Los dispositivos de protección de red deben soportar DHCP Relay;
2.13)	Los dispositivos de protección de red deben soportar DHCP Server;
2.14)	Los dispositivos de protección de red deben soportar sFlow
2.15)	Los dispositivos de protección de red deben soportar Jumbo Frames;
2.16)	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas
2.17)	Debe ser compatible con NAT dinámica (varios-a-1);
2.18)	Debe ser compatible con NAT dinámica (muchos-a-muchos);
2.19)	Debe soportar NAT estática (1-a-1);
2.20)	Debe admitir NAT estática (muchos-a-muchos);
2.21)	Debe ser compatible con NAT estático bidireccional 1-a-1;
2.22)	Debe ser compatible con la traducción de puertos (PAT);
2.23)	Debe ser compatible con NAT Origen;
2.24)	Debe ser compatible con NAT de destino;
2.25)	Debe soportar NAT de origen y NAT de destino de forma simultánea;
2.26)	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
2.27)	Debe ser compatible con NAT64 y NAT46;

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.28)	Debe implementar el protocolo ECMP;
2.29)	Debe soportar el balanceo de enlace hash por IP de origen;
2.30)	Debe soportar el balanceo de enlace hash por IP de origen y destino;
2.31)	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;
2.32)	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales
2.33)	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
2.34)	Enviar logs a sistemas de gestión externos simultáneamente;
2.35)	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
2.36)	Debe soporta protección contra la suplantación de identidad (anti-spoofing);
2.37)	Implementar la optimización del tráfico entre dos dispositivos;
2.38)	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
2.39)	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
2.40)	Soportar OSPF graceful restart;
2.41)	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);
2.42)	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
2.43)	Debe soportar modo capa - 2 (L2) para la inspección de datos en línea y la visibilidad del tráfico;
2.44)	Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en línea de tráfico;
2.45)	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
2.46)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
2.47)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
2.48)	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
2.49)	La configuración de alta disponibilidad debe sincronizar: Sesiones;
2.50)	La configuración de alta disponibilidad debe sincronizar: configuración, incluyendo, pero no limitados políticas de Firewalls, NAT, QoS y objetos de la red;
2.51)	La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN;
2.52)	La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
2.53)	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
2.54)	Debe soportar la creación de sistemas virtuales en el mismo equipo;
2.55)	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;
2.56)	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;
2.57)	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;
2.58)	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 Politica de Firewall

2.59)	Debe soportar controles de zona de seguridad
2.60)	Debe contar con políticas de control por puerto y protocolo
2.61)	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
2.62)	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad
2.63)	Control de política por código de país (por ejemplo: BR, USA., UK, RUS)

2.64) Control, inspección y des encriptación de SSL por política para el tráfico entrante y la salida

2.65) Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada;

2.66) Debe descifrar las conexiones de entrada y salida de tráfico negociadas con TLS 1.2;

2.67) Control de inspección y descifrado SSH por política;

2.68) 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;

2.69) Traffic shaping QoS basado en políticas (garantía de prioridad y máximo);

2.70) QoS basado en políticas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones;

2.71) Soporte para objetos y reglas IPV6;

2.72) Soporte objetos y reglas de multicast;

2.73) 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 unreachable por la máquina fuente de tráfico, TCP Reset para el cliente , RESET de TCP con el servidor o en ambos lados de la conexión;

2.74) Soportar la calendarización de políticas con el fin de activar y desactivar las reglas en tiempos predefinidos de forma automática;

Control de Aplicación

2.75) Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo

2.76) Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos

2.77) 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;

2.78) 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;

2.79) Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;

2.80) 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;

2.81) 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

2.82) 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;

2.83) 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

2.84) Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;

2.85) Actualización de la base de firmas de la aplicación de forma automática;

2.86) Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos;

2.87) 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;

2.88) 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;

2.89) Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;

2.90) Para mantener la seguridad de red eficiente debe ser soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;

2.91) 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

2.92) 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

2.93) El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;

2.94) Debe alertar al usuario cuando sea bloqueada una aplicación;

2.95) Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;

2.96) Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;

2.97) Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;

2.98) Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;

2.99) 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)

2.100) Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: nivel de riesgo de la aplicación

2.101) Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación

Prevención de Amenazas

2.102) Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;

2.103) Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);

2.104) 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;

2.105) Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad;

2.106) 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;

2.107) Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo;

2.108) Deben ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad

2.109) Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas;

2.110) 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

2.111) Deber permitir el bloqueo de vulnerabilidades

2.112) Debe permitir el bloqueo de exploits conocidos

2.113) Debe incluir la protección contra ataques de denegación de servicio

2.114) Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones;

2.115) Debe tener los siguientes mecanismos de inspección IPS: análisis de decodificación de protocolo;

2.116) Debe tener los siguientes mecanismos de inspección IPS: análisis para detectar anomalías de protocolo;

2.117) Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico;

2.118) Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;

2.119) Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;

2.120) Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets)

2.121) Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones SYN, ICMP , UDP, etc;

2.122) Detectar y bloquear los escaneos de puertos de origen;

2.123) Bloquear ataques realizados por gusanos (worms) conocidos;

2.124) Contar con firmas específicas para la mitigación de ataques DoS y DDoS;

2.125) Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);

2.126) Debe poder crear firmas personalizadas en la interfaz gráfica del producto;

2.127) 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;

2.128) Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;

2.129) Soportar el bloqueo de archivos por tipo;

2.130) Identificar y bloquear la comunicación con redes de bots;

2.131) 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;

2.132) Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;

2.133) 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

2.134) 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;

2.135) Los eventos deben identificar el país que origino la amenaza;

2.136) Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms)

2.137) Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP

2.138) 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

2.139) 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);

2.140) Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad

2.141) 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;

2.142) 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;

2.143) Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL

2.144) 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;

2.145) Tener por lo menos 60 categorías de URL;

2.146) Debe tener la funcionalidad de exclusión de URLs por categoría

2.147) Permitir página de bloqueo personalizada;

2.148) 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

2.149) 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;

2.150) 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;

2.151) 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;

2.152) 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;

2.153) 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;

2.154) 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;

2.155) 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);

2.156) 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;

2.157) Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos del LDAP / AD

2.158) Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.

2.159) Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores

QoS Traffic Shaping

2.160) 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;

2.161) Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;

2.162) Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;

2.163) Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;

2.164) Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;

2.165) Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;

2.166) QoS debe permitir la definición de tráfico con ancho de banda garantizado;

2.167) QoS debe permitir la definición de tráfico con máximo ancho de banda;

2.168) QoS debe permitir la definición de cola de prioridad;

2.169) Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype;

2.170) Soportar marcación de paquetes DiffServ, incluso por aplicación;

2.171) Soportar la modificación de los valores de DSCP para Diffserv;

2.172) Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service)

2.173) Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shapig;

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

Filtro de Datos

2.175) Permite la creación de filtros para archivos y datos predefinidos;

2.176) Los archivos deben ser identificados por tamaño y tipo;

2.177) Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);

2.178) Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;

2.179) Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;

2.180) 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

2.181) Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;

2.182) Debe permitir la visualización de los países de origen y destino en los registros de acceso;

2.183) Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

VPN

2.184) Soporte VPN de sitio a sitio y cliente a sitio;

2.185) Soportar VPN IPSec;

2.186) Soportar VPN SSL;

2.187) La VPN IPSec debe ser compatible con 3DES;

2.188) La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;

2.189) La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y el Grupo 14;

2.190) La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);

2.191) La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);

2.192) La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI

2.193) Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

2.194) Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec

2.195) Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;

2.196) 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;

2.197) Las características de VPN SSL se deben cumplir con o sin el uso de agentes;

2.198) 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;

2.199) Asignación de DNS en la VPN de cliente remoto;

2.200) 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;

2.201) Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;

2.202) Suportar lectura y revisión de CRL (lista de revocación de certificados);

2.203) Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;

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

2.205) Debería permitir la conexión a la VPN se establece de la siguiente manera: Después de la autenticación de usuario en la estación;

2.206) Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo demanda de los usuarios;

2.207) Deberá mantener una conexión segura con el portal durante la sesión;

2.208) 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

2.209) Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada

2.210) Soportar servicio del servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos

2.211) Soporte IPv4 e IPv6 por SSID

2.212) 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

2.213) Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point

2.214) Soportar monitoreo y supresión de puntos de acceso indebidos

2.215) Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS

2.216) Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows

2.217) Permitir la visualización de los dispositivos inalámbricos conectados por usuario

2.218) Permitir la visualización de los dispositivos inalámbricos conectados por IP

2.219) Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación

2.220) Permitir la visualización de los dispositivos inalámbricos conectados por canal

2.221) Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado

2.222) Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal

2.223) Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación

2.224) Debe soportar Fast Roaming en autenticación con portal cautivo

2.225) Debe soportar configuración de portal cautivo por SSID

2.226) Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico

2.227) Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP.

2.228) Debe ser compatible con el protocolo 802.1x RADIUS

2.229) La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal

2.230) La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática

2.231) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática

2.232) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP

2.233) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por dns

2.234) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por broadcast

2.235) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por multicast

2.236) La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue)

2.237) La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico

2.238) 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

2.239) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP

2.240) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.241) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding

2.242) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication

2.243) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding

2.244) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI

2.245) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack

2.246) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response

2.247) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication

2.248) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection

2.249) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge

2.250) Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas

2.251) Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso

2.252) La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible

2.253) La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario

2.254) Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID

2.255) Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso

2.256) Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio

2.257) La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh

2.258) 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

2.259) La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS

2.260) 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

2.261) Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso

2.262) Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso

2.263) Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica;

2.264) Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión

2.265) Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados

2.266) La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz

2.267) Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados

2.268) Debe permitir asociación dinámicas de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS

2.269) Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling

2.270) Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico

2.271) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones

2.272) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino

2.273) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza

2.274) La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones

2.275) la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico

2.276) El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo

2.277) El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales

2.278) La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

2.279) La controladora inalámbrica deberá soportar aceleración de tunnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico
2.280) La controladora inalámbrica debe soportar protocolo LLDP
2.281) Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta
2.282) Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC Adyacente
2.283) Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos
2.284) La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado
2.285) La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas
2.286) La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada
2.287) Deberá soportar la conversion de Multicast a Unicast para mejorar el rendimiento del tiempo de aire

INITEL, S.A. DE C.V.	SODENET, S. DE RL. DE C.V.
CUMPLE	CUMPLE

PARTIDA 3

SOLUCIÓN DE ADMNISTRACION CENTRALIZADA SD-WAN UTM/NGFW Y SOLUCIÓN DE CORRELACION DE LOGS Y INCIDENTES DE SEGURIDAD SD-WAN UTM/NGFW

1) Solución de Administración Centralizada
1.1) Solución de Administracion centralizada de Dispositivos SD-WAN UTM/NGFW con Licenciamiento de Actualizaciones de Firmware, soporte 24x7 por 60 meses.
1.2) La solución deberá ser escalable en 10, 100 y hasta 1000 dispositivos , con soporte en Hypervisor Vmware, Microsoft HyperV, Xen Server, KVM
1.3) Debe permitir gerenciar al menos 100 dispositivos
2) Requisitos Mínimos de Funcionalidad
Funcionalidades Generales
2.1) Debe permitir Gerenciar los dispositivos de la misma marca que los equipos ofertados, generando politicas centralizadas, control de cambios, revision de versiones, respaldos de configuracion y perfiles de usuarios
2.2) Si la solución es virtualizada, debe ser compatible con el ambiente VMware ESXi 5.5 e 6.0;
2.3) Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2
2.4) Si la solución es virtualizada, debe ser compatible con el ambiente Citrix XenServer 6.0+
2.5) Si la solución es virtualizada, debe ser compatible con el ambiente Open Source Xen 4.1+
2.6) Si la solución es virtualizada, debe ser compatible con el ambiente KVM
2.7) Si la solución es virtualizada, debe ser compatible con el ambiente Amazon Web Services (AWS)
2.8) No debe haber límites a la cantidad de múltiples vCPU si el aparato es virtual;
2.9) No debe haber límites a la expansión de memória RAM si el aparto es virtual;
2.10) En la fecha de la propuesta, ninguno de los modelos de la oferta pueden estar en el sitio del fabricante en listados de end-of-life o end-of-sales;
2.11) La gestión de la solición debe soportar aceso por SSH, cliente o WEB (HTTPS) y API abierta;
2.12) Debe permitir aceso concurrentes de administradores;
2.13) Debe tener interfaz basada en línea de comando para administración de la solución de gestión;
2.14) Debe tener un mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos;
2.15) Bloquear cambios, en el caso de acceso simultaneo de dos o más administradores;
2.16) Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, accesso de lectura, creación de usuários, cambio de configuraciones;
2.17) Generar alertas automáticos por Email
2.18) Generar alertas automáticos por SNMP
2.19) Generar alertas automáticos por Syslog
2.20) Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horário;
2.21) Debe ser permitido al administrador transferir los backups a un servidor FTP.
2.22) Debe ser permitido al administrador transferir los backups a un servidor SCP
2.23) Debe ser permitido al administrador transferir los backups a un servidor SFTP
2.24) Los cambios realizados en un servidor de gestión debe ser automaticamente replicados al servidor redundante;
2.25) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de cuentas de usuários LOCALES
2.26) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa TACACS
2.27) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa LDAP
2.28) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa RADIUS
2.29) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de Certificado Digital X.509 (PKI)
2.30) Debe soportar sincronización de reloj interno por protocolo NTP.
2.31) Debe registrar las acciones efectuadas por cualquier usuário;
2.32) Deben ser fornecidos manuales de instalación, configuración y operación de toda la solución, e los idiomas portugués o inglés, com apresentación de buena calidad;
2.33) Debe suportar SNMP versión 2 y la versión 3 en los equipos de gestión;
2.34) Debe permitir habilitar o deshabilitar, para cada interfaz de red de la solución de gestión, permisos de acceso HTTP, HTTPS, SSH, SNMP y Telnet;
2.35) Debe permitir virtualizar la solución de gestión, de manera que cada administrador pueda gerenciar, visualizar y editar solo los dispositivos autorizados y registrados en su ambiente virtualizado;

2.36) La solución de gestión debe permitir crear administradores que tengan acceso a todas las instancias de virtualización;

Funcionalidades de APIs

2.37) Debe soportar XML API
2.38) Debe soportar JSON API

Funcionalidades de Gestión de SDWAN UTM/NGFW

2.39) La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación;
2.40) La gestión debe permitir la creación y administración de políticas de IPS, Antivírus y Anti-Spyware;
2.41) La gestión debe permitir la creación y administración de políticas de Filtro de URL;
2.42) Permitir buscar cuáles reglas un objeto está siendo utilizado;
2.43) Debe atribuir secuencialmente un número a cada regla de firewall;
2.44) Debe atribuir secuencialmente un número a cada regla de firewall;DOS;
2.45) Permitir la creación de reglas que permanezcan activas en horário definido;
2.46) Permitir backup de las configuraciones y rollback de configuración para la última configuración salva;
2.47) Debe tener mecanismos de validación de políticas avisando cuando hayan reglas que ofusquen o conflictuen con otras (shadowing);
2.48) Debe posibilitar la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas;
2.49) Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión;
2.50) Cada servidor de gestión debe ser hospedado en un equipo independiente, no ejecutando función de firewall;
2.51) La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador atualizar licencias en los aparatos a través de esta herramienta;
2.52) La solución debe permitir la distribución y instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos;
2.53) Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados;
2.54) Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas despuez de la aprobación de otro administrador;
2.55) Tener "wizard" en la solución de gestion para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de los mismos;
2.56) Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados cuando el mismo es agregado a la solución de gestión;
2.57) Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horário de lo sistema y firmware;
2.58) Tener "wizard" en la solución de gestion para instalación de políticas y configuraciones de los dispositivos;
2.59) Permitir crear en la solución de gestión templates de configuración de los dispositivos con informadiones de DNS, SNMP, configuraciones de LOG y administración;
2.60) Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos;
2.61) Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión;
2.62) Permitir configurar y visualizar balanceo de enlaces en los dispositivos gestionados de forma centralizada;
2.63) Permitir crear vários paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos;
2.64) Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada;
2.65) Permitir la creación de reglas anti DoS de forma centralizada;
2.66) Permitir la creación de objetos que serán utilizados en las políticas de forma centralizada;
2.67) Permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topologia (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía;
2.68) Permitir la utilizacion de Zero Touch Provisioning para automatizar las configuraciones de los Dispositivos administrados
2.69) Permitir la utilizacion de Plantillas para automatizar la configuracion de los Modulos de SD-WAN de los dispositivos Gerenciados

1) Características

1.1) Solución de Correlación de Logs centralizada de Dispositivos SD-WAN UTM/NGFW con Licenciamiento de Actualizaciones de Sistema de Firmware, soporte 24x7 por 60 meses.
1.2) Tener capacidad de recibir al menos 50 GBytes de logs diarios
1.3) Deberá Soportar Identificadores de Compromiso
1.4) Deberá soportar módulo de SoC
1.5) Soportar módulo de "Outbreak Alert Service"
1.6) Deberá ser por cuestiones de compatibilidad , la misma marca que los dispositivos SD-WAN UTM / NGFW
1.7) La solución debe ser escalable o stackeable en 5GB/50GB/500 GB logs al día

2) Requisitos Mínimos de Funcionalidad

Funcionalidades Generales

2.1) Si la solución es virtualizada, debe ser compatible con el ambiente VMware ESXi 5.0/5.1/5.5/6.0/6.5/6.7;
2.2) Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2/2016
2.3) Si la solución es virtualizada, debe ser compatible con el ambiente Citrix XenServer 6.0+
2.4) Si la solución es virtualizada, debe ser compatible con el ambiente Open Source Xen 4.1+
2.5) Si la solución es virtualizada, debe ser compatible con el ambiente KVM on Redhat 6.5+ and Ubuntu 17.04
2.6) Si la solución es virtualizada, debe ser compatible con el ambiente Nutanix AHV (AOS 5.10.5)
2.7) Si la solución es virtualizada, debe ser compatible con el ambiente Amazon Web Services (AWS)
2.8) Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Azure.
2.9) Si la solución es virtualizada, debe ser compatible con el ambiente Google Cloud (GCP)
2.10) Si la solución es virtualizada, debe ser compatible con el ambiente Oracle Cloud Infrastructure (OCI)
2.11) Si la solución es virtualizada, debe ser compatible con el ambiente Alibaba Coud (AliCloud)
2.12) Si la solución es virtualizada, no debe haber límites a la cantidad de múltiples vCPU
2.13) Si la solución es virtualizada, no debe haber límites a la expansión de memoria RAM
2.14) Debe soportar acceso vía SSH, WEB (HTTPS) para la gestion de la solución
2.15) Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía linea de comandos en consola de gestión.
2.16) Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
2.17) Soporte SNMP versión 2 y 3
2.18) Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
2.19) Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
2.20) Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH
2.21) Autenticación de usuarios de acceso a la plataforma via LDAP
2.22) Autenticación de usuarios de acceso a la plataforma via Radius
2.23) Autenticación de usuarios de acceso a la plataforma via TACACS+
2.24) Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos
2.25) Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
2.26) Generación de informes en tiempo real de tráfico, en formato de gráfica tabla
2.27) Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
2.28) Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
2.29) Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado
2.30) Contar con mecanismos de borrado automático de logs antiguos.
2.31) Permitir la importación y exportación de reportes

2.32) Debe contar con la capacidad de crear informes en formato HTML
2.33) Debe contar con la capacidad de crear informes en formato PDF
2.34) Debe contar con la capacidad de crear informes en formato XML
2.35) Debe contar con la capacidad de crear informes en formato CSV
2.36) Debe permitir exportar los logs en formato CSV
2.37) Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
2.38) Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
2.39) La solución debe contar con reportes predefinidos
2.40) Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución
2.41) Debe ser posible la duplicación de reportes existentes para su posterior edición.
2.42) Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
2.43) Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
2.44) Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
2.45) Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
2.46) Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
2.47) Debe permitir descargar de la plataforma los archivos de logs para uso externo.
2.48) Tener la capacidad de generar y enviar reportes periódicos automáticamente.
2.49) Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
2.50) Permitir el envío por email de manera automática de reportes.
2.51) Debe permitir que el reporte a enviar por email sea al destinatario específico.
2.52) Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
2.53) Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
2.54) Debe permitir el uso de filtros en los reportes.
2.55) Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
2.56) Permitir especificar el idioma de los reportes creados
2.57) Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
2.58) Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
2.59) Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.
2.60) Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
2.61) Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.
2.62) Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
2.63) Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
2.64) Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
2.65) Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
2.66) Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos
2.67) Debe permitir visualizar en tiempo real los logs recibidos.
2.68) Debe permitir el reenvío de logs en formato syslog.
2.69) Debe permitir el reenvío de logs en formato CEF (Common Event Format).
2.70) Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red
2.71) Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
2.72) Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.
2.73) Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red
2.74) Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
2.75) Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.
2.76) Debe incluir dashboard para operaciones SOC que monitorea actividad VPN ren su red.
2.77) Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs
2.78) Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)
2.79) Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC
2.80) Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3
2.81) Debe permitir generar alertas de eventos a partir de logs recibidos
2.82) Debe permitir crear incidentes a partir de alertas de eventos para endpoint
2.83) Debe permitir la integración al sistema de tickets ServiceNow
2.84) Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
2.85) Debe permitir respaldar logs en nube publica de Amazon S3
2.86) Debe permitir respaldar logs en nube publica de Microsoft Azure
2.87) Debe permitir respaldar logs en nube publica de Gooogle Cloud
2.88) Debe soportar el estándar SAML para autenticación de usuarios administradores

Reportes de Firewall

2.89) Debe contar con reporte de cumplimiento de PCI DSS
2.90) Debe contar con reporte de utilización de aplicaciones SaaS
2.91) Debe contar con reporte de prevención de perdida de datos (DLP)
2.92) Debe contar con reporte de VPN
2.93) Debe contar con reporte de Sistema de prevención de intrusos (IPS)
2.94) Debe contar con reporte de reputación de cliente
2.95) Debe contar con reporte de análisis de seguridad de usuario
2.96) Debe contar con reporte de análisis de amenaza cibernética
2.97) Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad
2.98) Debe contar con reporte de tráfico DNS
2.99) Debe contar con reporte tráfico de correo electrónico
2.100) Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red
2.101) Debe contar con reporte de Top 10 de Websites utilizadas en la red
2.102) Debe contar con reporte de uso de redes sociales

Reportes de Fabric

2.103) Debe contar con reporte de evaluación de riesgo para correo electrónico

Reportes de Wireless

2.104) Debe contar con reporte de cumplimiento PCI de Wireless.
2.105) Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WIFI

Reportes de Endpoint

2.106) Debe contar con reporte de vulnerabilidades de solución gestionada de seguridad de equipo terminal.

Reportes de WAF
2.107) Debe contar con reporte de aplicaciónes web, si se cuenta con plataforma de seguridad web
Reportes de SD-WAN
Debe de contar con reportes de la utilizacion del modulo de SD-WAN de los dispositivos que realicen la correlacion en la solución..

INITEL, S.A. DE C.V.	SODENET, S. DE RL. DE C.V.
CUMPLE	CUMPLE

Condiciones para el participante:

1. El participante deberá incluir en su propuesta carta original expedida por el fabricante constatando su estado actual de revendedor autorizado con mínimo nivel advanced.
2. El participante deberá incluir en su propuesta carta original expedida por el fabricante constatando el personal certificado Network Security Expert
   a. Al menos 1 NSE4
   b. Al menos 1 NSE5
   c. Al Menos 1 NSE7
3. El participante deberá incluir en su propuesta carta original expedida por el representante legal del fabricante/mayorista sobre sus capacidades de implementación y experiencia en proyectos similares al presente concurso.

INITEL, S.A. DE C.V.	SODENET, S. DE RL. DE C.V.
CUMPLE	NO CUMPLE

La empresa SODENET, S. de RL. De C.V. no cumple, ya que según los documentos que recibimos por parte de la Coordinación de Servicios Generales, no anexan la carta expedida por el fabricante constatando su estado actual de revendedor autorizado con mínimo nivel advanced y tampoco incluye en su propuesta carta original expedida por el fabricante constatando el personal certificado Network Security Expert.

ELABORÓ

TSU Brian Valerio Flores
Jefe de la Unidad de Redes y Telecomunicaciones

AUTORIZÓ

Ing. María Esmeralda Olmos de la Cruz
Coordinadora de Cómputo e Informática

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

DICTAMEN TÉCNICO

Guadalajara, Jalisco a 20 de octubre de 2020

LICITACION: LI-SEMS-009-2021
DEPENDENCIA: SISTEMA DE EDUCACION MEDIA SUPERIOR
NOMBRE: ADQUISICIÓN DE PUNTOS DE ACCESO INALÁMBRICOS Y NODOS DE RED, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA.

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

EMPRESAS	IMPORTE INCLUYE I.V.A
SOLUCIONES Y SERVICIOS INTEGRALES TELCO, S.A. DE C.V.	**$12´158,977.56**

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 24, 25, 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.-PROPUESTAS RECHAZADAS

3.1.-Se rechaza la propuesta de la empresa **REDEFONIA, S.A. DE C.V.,** debido a que se solicitan en la **SECCIÓN III** de las **BASES DE LA LICITACIÓN** los siguientes documentos:

6.-El participante deberá presentar certificados vigentes de al menos 2 ingenieros CCNA (Cisco Certified Network Associate), 1 ingeniero CCDA (Cisco Certified Design Associate) y 1 ingeniero CCNP Collaboration (Cisco Certified Network Professional Collaboration)

7.-El participante deberá presentar copia de un certificado vigente de ITIL Foundation v3, así como el currículum de la persona que lo poseea, quien deberá laborar para la empresa en cuestión.

8.-El participante deberá presentar copia de un certificado vigente de Project Manangement Professional (PMP), así como el currículum de la persona que lo poseea, quien deberá laborar para la empresa en cuestión.

Con base lo solicitado en las bases de la presente licitación, se observa que la empresa licitante de acuerdo a los documentos entregados, no presenta lo siguiente:

Los certificados vigentes de al menos 2 ingenieros CCNA (Cisco Certified Network Associate), 1 ingeniero CCDA (Cisco Certified Design Associate) y 1 ingeniero CCNP Collaboration (Cisco Certified Network Professional Collaboration). Asimismo, dentro de los documentos entregados no presentan copia de un certificado vigente de ITIL Foundation v3, así como el currículum de la empresa que lo posea, quien deberá laborar para la empresa en cuestión y no presenta copia de un certificado vigente de Project Manangement Profesisional (PMP), así como el currículum de la persona que lo posea, quien deberá laborar para la empresa en cuestión.

Con base a lo anterior, se rechaza la propuesta de la empresa **REDEFONIA, S.A. DE C.V.,** con base a lo establecido en la **SECCIÓN I "INSTRUCCIONES A LOS LICITANTES", inciso "G" Motivos por los que puede ser desechada la propuesta,** numeral **29 Causas por las que puede ser desechada la propuesta.**

Inciso "A"

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

Inciso "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.

Inciso "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.

4.- 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, 2 y 3**

Empresa: **SOLUCIONES Y SERVICIOS INTEGRALES TELCO, S.A. DE C.V.**

Por un importe de **$12´158,977.56 (Doce millones ciento cincuenta y ocho mil novecientos setenta y siete pesos 56/100 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 24, 25, 45 y 48., 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

DICTAMEN TÉCNICO

Guadalajara, Jalisco a 18 de octubre de 2021

LICITACIÓN: LI-SEMS-010-2021
DEPENDENCIA: SISTEMA DE EDUCACION MEDIA SUPERIOR
NOMBRE: ADQUISICIÓN DE EQUIPO DE SOLUCIÓN DE SEGURIDAD UTM/NGFW, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA.

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.	**$21,901,549.82**

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 24, 25, 45 y 47, en las condiciones generales 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 condiciones generales del concurso.

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.-PROPUESTAS RECHAZADAS

3.1.-Se rechaza la propuesta de la empresa **SODENET, S. DE R.L. DE C.V.,** debido a que se solicitan en la **SECCIÓN III** de las **BASES DE LA LICITACIÓN** los siguientes documentos:

Condiciones para el participante:

1. El participante deberá incluir en su propuesta carta original expedida por el fabricante constatando su estado actual de revendedor autorizado con mínimo nivel advanced.

2. El participante deberá incluir en su propuesta carta original expedida por el fabricante constatando el personal certificado Network Security Expert
a. Al menos 1 NSE4
b. Al menos 1 NSE5
c. Al Menos 1 NSE7

.

Con base lo solicitado en las bases de la presente licitación, se observa que la empresa licitante de acuerdo a los documentos entregados, no presenta lo siguiente:

Carta expedida por el fabricante constando su estado actual de revendedor autorizado como mínimo nivel advanced y tampoco incluye en su propuesta carta original expedida por el fabricante constatando el personal certificado Network Security Expert.
a. Al menos 1 NSE4
b. Al menos 1 NSE5
c. Al Menos 1 NSE7

Con base a lo anterior, se rechaza la propuesta de la empresa **SODENET, S. DE R.L. DE C.V.,** con base a lo establecido en la **SECCIÓN I "INSTRUCCIONES A LOS LICITANTES", inciso "G" Motivos por los que puede ser desechada la propuesta,** numeral **29 Causas por las que puede ser desechada la propuesta.**

Inciso "A"

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

Inciso "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.

Inciso "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.

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

Partida. **1, 2, 3**
Empresa: **INITEL, S.A. DE C.V.**
Por un monto total de **$21,901,549.82 (Veintiún millones novecientos un mil quinientos cuarenta y nueve pesos 82/100 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 y con las mejores condiciones generales en cada una de las partidas, en apego a lo establecido en los artículos 24, 25, 45 y 47 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara.

ELABORÓ

MTRA. ROSAURA RODRÍGUEZ RODRÍGUEZ
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-010-2021
DEPENDENCIA: SISTEMA DE EDUCACION MEDIA SUPERIOR
NOMBRE: ADQUISICIÓN DE EQUIPO DE SOLUCIÓN DE SEGURIDAD UTM/NGFW, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA.

En la Ciudad de Guadalajara, Jalisco siendo las **11:20 horas** del día **27 de octubre de 2021**, 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. Jorge Navarro Peña, 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, 2 y 3**
Empresa: **INITEL, S.A. DE C.V.**
Por un importe de **$21´901,549.82 (Veintiún millones novecientos un mil quinientos cuarenta y nueve pesos 82/100 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 24, 25, 45 y 47., del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara.

Lic. Jorge Navarro Peña
Presidente del Comité de Compras
y Adquisiciones del SEMS

Mtro. Jesús Alberto Jiménez Herrera
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	Mtra. María Guadalupe Cid Escobedo	**Acta Constitutiva**	Escritura pública No. 50,136 de fecha 27 de diciembre de 2002, ante la fe del Lic. Jorge Robles Farías, Notario Público No. 12, de Guadalajara, Jalisco.
Título	Apoderada	**Representante**	Teobaldo Leal Arriaga
		Título	Administrador General Único
Documento que acredita las facultades	Escritura Pública No. 48,826 de fecha 12 de noviembre de 2019, otorgada ante la fe del Lic. Samuel Fernández Ávila, Notario Público No. 15 de Tlaquepaque, Jalisco	**Documento que acredita las facultades**	Acta Constitutiva
		R.F.C.	INI030109U17
		Clave Patronal I.M.S.S.	[redacted] 1
Domicilio	Avenida Juárez número 976, Zona Centro, Código Postal 44100, en Guadalajara, Jalisco	**Domicilio**	Priv. Av. Patria 888 piso Int. P2-A oficina T, Colonia Jardines Universidad, Zapopan, Jalisco. C.P. 45110

OBJETO E IMPORTE

Denominación	Adquisición de equipo de solución de seguridad UTM/NGFW, para el Sistema de Educación Media Superior de la Universidad de Guadalajara.		
Clave	LI-SEMS-010-2021	**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	$21´901,549.82 IVA incluido	**Partidas**	1, 2 y 3
		Tipo de Recurso	☒ Estatal ☐ Federal
Forma de pago (periodicidad)	30% anticipo y 70% al entregar	**Fondo**	F-1.3.13.3, proyecto 259928, año 2021

PLAZO DE ENTREGA		INSTALACIÓN
Plazo de entrega	4 a 7 semanas	☒ SI incluye instalación
A partir de	la firma del presente contrato	☐ 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) Ninguna.

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**	29 de octubre de 2021
LA UNIVERSIDAD		EL VENDEDOR	
		[redacted] 2	
Representante	Mtra. María Guadalupe Cid Escobedo	**Representante**	Teobaldo Leal Arriaga
Título	Apoderada	**Título**	Administrador General Único
TESTIGOS			
Nombre	Mtro. Jesús Alberto Jiménez Herrera	**Nombre**	Ing. Fernando Calvillo Vargas
Cargo	Secretario Administrativo del Sistema de Educación Media Superior	**Cargo**	Coordinador de Servicios Generales 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.

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**.

[redacted] 2

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 del presente, entre ellos los de responsabilidad civil, daños a terceros en sus bienes o personas etc., el cual deberá de estar vigente hasta el cumplimiento total de sus obligaciones plasmadas a su cargo en el presente, acordándose que en caso de no contar con dicho seguro, **EL VENDEDOR** será directamente responsable por dichos conceptos.

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, cuando concurran circunstancias imprevistas o razones de interés general, previa notificación por escrito a **EL VENDEDOR** con cuando menos 5 (cinco) días naturales de anticipación.

Adicionalmente, acuerdan las partes que **LA UNIVERSIDAD** podrá suspender los trabajos y/o pagos objeto del presente, en caso de que se 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 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 acorado en el contrato y su anexo.
b) Si **EL VENDEDOR,** en su caso, no entrega los trabajos contratados totalmente terminados dentro del plazo señalado en el presente contrato y su anexo.
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.

[redacted]

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 Méxicana 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.

[redacted]

2

initel

Empresa: INITEL S.A. DE C.V.
R.F.C.: INI030109U17
Dirección: AV. PATRIA 888 PISO 2 A OFICINA T
Teléfono: [redacted]
web: www.initel.com.mx

Universidad de Guadalajara
Sistema de Educación Media Superior de la Universidad de Guadalajara
Mtro. Jesús Alberto Jiménez Herrera
Secretario Ejecutivo del Comité de Compras y Adquisiciones del Sistema de Educación Media Superior

Propuesta Económica

Fecha: 13 Octubre 2021
Licitación: LI-SEMS-010-2021
Denominada: ADQUISICIÓN DE EQUIPO DE SOLUCIÓN UTM/NGFW, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA

PARTIDA	CANTIDAD	CODIGO	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
1	29	FG-400E-BDL-950-36	**SOLUCIÓN UTM/NGFW "TIPO A"** Marca Fortinet, modelo Fortigate FG-400E Hardware plus 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP) for 36 months	$ 319,662.00	$ 9,270,198.00
2	41	FG-200F-BDL-950-36	**SOLUCIÓN UTM/NGFW "TIPO B"** Marca Fortinet, modelo Fortigate FG-200F Hardware plus 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP) for 36 months	$ 197,886.00	$ 8,113,326.00
3	1	FC2-10-AZVMS-465-01-60 FC2-10-FMGVS-448-01-60	**SOLUCIÓN DE ADMNISTRACION CENTRALIZADA SD-WAN UTM/NGFW Y SOLUCIÓN DE CORRELACION DE LOGS Y INCIDENTES DE SEGURIDAD SD-WAN UTM/NGFW** Marca Fortinet, modelos: FortiAnalyzer Virtual, Subscription license for 50 GB/Day Central Logging & Analytics. Include 24x7 FortiCare support, IOC, SOC subscription, and FortiGuard Outbreak Alert service for 60 months and Fortimanager Virtual, Subscription license for 100 devices/vdoms managed by FortiManager VM S-series. 24x7 FortiCare support plus FortiCare Best Practice services included for 69 months	$ 1,497,122.40	$ 1,497,122.40

Subtotal	$	18,880,646.40
I.V.A.	$	3,020,903.42
Total	$	21,901,549.82

Veintiún Millones Novecientos Un Mil Quinientos Cuarenta y Nueve Pesos 82/100 MN

SECRETARÍA ADMINISTRATIVA

Condiciones Comerciales

Moneda: Precios expresados en Moneda Nacional, sujetos a cambio sin previo aviso.
Tiempo de Entrega: 4 a 7 semanas despues de confirmado el pedido
Vigencia: 30 dias naturales.
Pago: 30% de anticipo y 70% al entregar
Garantía: 3 años en equipos FG-400E y FG-200F y 60 meses en SOLUCIÓN DE ADMNISTRACION CENTRALIZADA SD-WAN UTM/NGFW Y SOLUCIÓN DE CORRELACION DE LOGS Y INCIDENTES DE SEGURIDAD SD-WAN UTM/NGFW
Los precios ofertados consideran el costo de flete para la entrega a cada dependencia beneficiada.

[redacted]

[redacted]

Representante Legal
[redacted] Teobaldo Leal Arriaga
tleal@initel.com.mx
[redacted]
Initel S.A. De C.V.

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted] 3

ANEXO TECNICO

Descripción de los bienes requeridos por el Sistema de Educación Media Superior, conforme a la siguiente tabla:

PARTIDA	CANTIDAD	DESCRIPCIÓN	C.U.	TOTAL
		SOLUCIÓN UTM/NGFW "TIPO A"		
		1.1) Throughput de por lo menos 24 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete		
		1.2) Soporte a por lo menos 4M conexiones simultaneas		
		1.3) Soporte a por lo menos 450K nuevas conexiones por segundo		
		1.4) Throughput de al menos 20 Gbps de VPN IPSec		
		1.5) Estar licenciado para, o soportar sin necesidad de licencia, 2K tuneles de VPN IPSec site-to-site simultaneos		
		1.6) Estar licenciado para, o soportar sin necesidad de licencia, 50K tuneles de clientes VPN IPSec simultaneos		
		1.7) Throughput de al menos 4500 Mbps de VPN SSL		
		1.8) Soportar al menos 5000 clientes de VPN SSL simultaneos		
		1.9) Soportar al menos 7800 Mbps de throughput de IPS		
		1.10) Soportar al menos 4000 Mbps de throughput de Inspeción SSL		
		1.11) Throughput de al menos 5000 Mbps con las siguientes funcionalidades habilitadas simultaneamente para todas las firmas que la solución de seguridad tenga debidamente activadasy operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado multiples numeros de disempeño para cualquier de las funcionalidades, solamente el de valor más pequeño sera aceptado		
		1.12) Permitir gestionar como controladora inalámbrica al menos 512 Access Points y gestionar por lo menos 72 Switches de la misma marca del fabricante del UTM/NGFW dentro de la misma interfase de gestión		
		1.13) Tener al menos 4 interfaces 10 Gbps SFPP, 8 interfases de 1 Gbps SFP, 16 interfases de 1GE RJ25, 2 interfases 1 Gbps RJ45 para Gestion y alta disponibilidad		
		1.15) Estar licenciado y/o tener incluído sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance		
		1.16) Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance		
		1.17) Debe de incluir un token fisico para autenticacion de doble factor para la gestion del appliance o para el acceso VPN que debe ser de la misma marca propuesta		
		1.18) Debe de 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus, Botnet IP/Domain, AntiSpam y Filtrado Web		
		1.19) Debe de contar con una fuente de poder AC de 100-240 VAC, con la posibilidad de agregar una segunda para alta disponibilidad		
		1.20) Deberá contar con 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema de firmware, y los siguientes módulos incluidos IPS ó Preventor de Intrusos, Antivirus, Protección contra Botnet IP/Domain, Módulo de Protección de Mobile Malware, Módulo de Sandbox en nube incluyendo Virus Outbreak and Content Disarm & Reconstruct, Control de aplicaciones, Filtrado Web & Video Filtering y Módulo de AntiSpam.		
		2) Requisitos Mínimos de Funcionalidad		
		Caracteristicas Generales		
1	29	2.1) 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;		

SECRETARÍA ADMINISTRATIVA

[redacted] 2

[redacted] 2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

[redacted]

3

2.2)	Por funcionalidades de NGFW se entiende: aplicaciones de reconocimiento, prevención de amenazas, identificación de usuarios y control granular de permisos;
2.3)	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;
2.4)	La plataforma debe estar optimizada para aplicaciones de análisis de contenido en la capa 7;
2.5)	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;
2.6)	La gestión del equipo debe ser compatible con acceso a través de SSH, consola, web (HTTPS) y API abierta;
2.7)	La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
2.8)	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
2.9)	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
2.10)	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
2.11)	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
2.12)	Los dispositivos de protección de red deben soportar DHCP Relay;
2.13)	Los dispositivos de protección de red deben soportar DHCP Server;
2.14)	Los dispositivos de protección de red deben soportar sFlow
2.15)	Los dispositivos de protección de red deben soportar Jumbo Frames;
2.16)	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas
2.17)	Debe ser compatible con NAT dinámica (varios-a-1);
2.18)	Debe ser compatible con NAT dinámica (muchos-a-muchos);
2.19)	Debe soportar NAT estática (1-a-1);
2.20)	Debe admitir NAT estática (muchos-a-muchos);
2.21)	Debe ser compatible con NAT estático bidireccional 1-a-1;
2.22)	Debe ser compatible con la traducción de puertos (PAT);
2.23)	Debe ser compatible con NAT Origen;
2.24)	Debe ser compatible con NAT de destino;
2.25)	Debe soportar NAT de origen y NAT de destino de forma simultánea;
2.26)	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
2.27)	Debe ser compatible con NAT64 y NAT46;
2.28)	Debe implementar el protocolo ECMP;
2.29)	Debe soportar el balanceo de enlace hash por IP de origen;
2.30)	Debe soportar el balanceo de enlace hash por IP de origen y destino;
2.31)	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;
2.32)	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales
2.33)	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
2.34)	Enviar logs a sistemas de gestión externos simultáneamente;
2.35)	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
2.36)	Debe soporta protección contra la suplantación de identidad (anti-spoofing);
2.37)	Implementar la optimización del tráfico entre dos dispositivos;

SECRETARÍA ADMINISTRATIVA

[redacted]

2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

[redacted]

3

2.38)	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
2.39)	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
2.40)	Soportar OSPF graceful restart;
2.41)	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);
2.42)	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
2.43)	Debe soportar modo capa - 2 (L2) para la inspección de datos en línea y la visibilidad del tráfico;
2.44)	Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en línea de tráfico;
2.45)	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
2.46)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
2.47)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
2.48)	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
2.49)	La configuración de alta disponibilidad debe sincronizar: Sesiones;
2.50)	La configuración de alta disponibilidad debe sincronizar: configuración, incluyendo, pero no limitados políticas de Firewalls, NAT, QoS y objetos de la red;
2.51)	La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN;
2.52)	La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
2.53)	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
2.54)	Debe soportar la creación de sistemas virtuales en el mismo equipo;
2.55)	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;
2.56)	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;
2.57)	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;

SECRETARÍA ADMINISTRATIVA

[redacted]

2

[redacted]

2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

[redacted]

2.58)	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
2.59)	Debe soportar controles de zona de seguridad
2.60)	Debe contar con políticas de control por puerto y protocolo
2.61)	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
2.62)	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad
2.63)	Control de política por código de país (por ejemplo: BR, USA., UK, RUS)
2.64)	Control, inspección y des encriptación de SSL por política para el tráfico entrante y la salida
2.65)	Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada;
2.66)	Debe descifrar las conexiones de entrada y salida de tráfico negociadas con TLS 1.2;
2.67)	Control de inspección y descifrado SSH por política;
2.68)	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;
2.69)	Traffic shaping QoS basado en políticas (garantía de prioridad y máximo);
2.70)	QoS basado en políticas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones;
2.71)	Soporte para objetos y reglas IPV6;
2.72)	Soporte objetos y reglas de multicast;
2.73)	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 unreachable por la máquina fuente de tráfico, TCP Reset para el cliente , RESET de TCP con el servidor o en ambos lados de la conexión;
2.74)	Soportar la calendarización de políticas con el fin de activar y desactivar las reglas en tiempos predefinidos de forma automática;
	Control de Aplicación
2.75)	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo

SECRETARÍA ADMINISTRATIVA

[redacted]

[redacted]

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

2.76)	Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos
2.77)	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, video, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
2.78)	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;
2.79)	Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;
2.80)	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;
2.81)	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
2.82)	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;
2.83)	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
2.84)	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
2.85)	Actualización de la base de firmas de la aplicación de forma automática;
2.86)	Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos;
2.87)	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;

SECRETARÍA ADMINISTRATIVA

[redacted]

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

2.88)	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;
2.89)	Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;
2.90)	Para mantener la seguridad de red eficiente debe ser soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
2.91)	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
2.92)	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
2.93)	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
2.94)	Debe alertar al usuario cuando sea bloqueada una aplicación;
2.95)	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
2.96)	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
2.97)	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;
2.98)	Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
2.99)	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)
2.100)	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: nivel de riesgo de la aplicación
2.101)	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación
	Prevención de Amenazas
2.102)	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;

SECRETARÍA ADMINISTRATIVA

[redacted] 2

[redacted] 2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

2.103)	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
2.104)	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;
2.105)	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad;
2.106)	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;
2.107)	Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo;
2.108)	Deben ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad
2.109)	Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas;
2.110)	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
2.111)	Deber permitir el bloqueo de vulnerabilidades
2.112)	Debe permitir el bloqueo de exploits conocidos
2.113)	Debe incluir la protección contra ataques de denegación de servicio
2.114)	Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones;
2.115)	Debe tener los siguientes mecanismos de inspección IPS: análisis de decodificación de protocolo;
2.116)	Debe tener los siguientes mecanismos de inspección IPS: análisis para detectar anomalías de protocolo;
2.117)	Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico;
2.118)	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
2.119)	Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;
2.120)	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets)
2.121)	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones SYN, ICMP , UDP, etc;
2.122)	Detectar y bloquear los escaneos de puertos de origen;
2.123)	Bloquear ataques realizados por gusanos (worms) conocidos;
2.124)	Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
2.125)	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);

SECRETARÍA ADMINISTRATIVA

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]3

2.126)	Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
2.127)	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;
2.128)	Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;
2.129)	Soportar el bloqueo de archivos por tipo;
2.130)	Identificar y bloquear la comunicación con redes de bots;
2.131)	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;
2.132)	Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
2.133)	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
2.134)	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;
2.135)	Los eventos deben identificar el país que origino la amenaza;
2.136)	Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms)
2.137)	Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP
2.138)	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
2.139)	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);
2.140)	Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad
2.141)	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;

SECRETARIA ADMINISTRATIVA

[redacted]2

[redacted]2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]3

2.142) 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;

2.143) Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL

2.144) 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;

2.145) Tener por lo menos 60 categorías de URL;

2.146) Debe tener la funcionalidad de exclusión de URLs por categoría

2.147) Permitir página de bloqueo personalizada;

2.148) 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

2.149) 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;

2.150) 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;

2.151) 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;

2.152) 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;

2.153) 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;

2.154) 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;

2.155) 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);

SECRETARÍA ADMINISTRATIVA

[redacted]2

[redacted]2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

2.156)	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;
2.157)	Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos del LDAP / AD
2.158)	Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
2.159)	Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores
	QoS Traffic Shaping
2.160)	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;
2.161)	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
2.162)	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
2.163)	Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
2.164)	Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
2.165)	Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
2.166)	QoS debe permitir la definición de tráfico con ancho de banda garantizado;
2.167)	QoS debe permitir la definición de tráfico con máximo ancho de banda;
2.168)	QoS debe permitir la definición de cola de prioridad;
2.169)	Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype;
2.170)	Soportar marcación de paquetes DiffServ, incluso por aplicación;
2.171)	Soportar la modificación de los valores de DSCP para Diffserv;
2.172)	Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service)
2.173)	Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shapig;
2.174)	Debe soportar QoS (traffic-shaping) en la interfaz agregada o redundantes;
	Filtro de Datos

SECRETARÍA ADMINISTRATIVA

[redacted]

[redacted]

[redacted]

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

2.175)	Permite la creación de filtros para archivos y datos predefinidos;
2.176)	Los archivos deben ser identificados por tamaño y tipo;
2.177)	Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);
2.178)	Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
2.179)	Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
2.180)	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 Localizacion
2.181)	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
2.182)	Debe permitir la visualización de los países de origen y destino en los registros de acceso;
2.183)	Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.
	VPN
2.184)	Soporte VPN de sitio a sitio y cliente a sitio;
2.185)	Soportar VPN IPSec;
2.186)	Soportar VPN SSL;
2.187)	La VPN IPSec debe ser compatible con 3DES;
2.188)	La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;
2.189)	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y el Grupo 14;
2.190)	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
2.191)	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
2.192)	La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI
2.193)	Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
2.194)	Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec
2.195)	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;
2.196)	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;

SECRETARÍA ADMINISTRATIVA

[redacted]

2

[redacted]

2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]3

2.197)	Las características de VPN SSL se deben cumplir con o sin el uso de agentes:
2.198)	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;
2.199)	Asignación de DNS en la VPN de cliente remoto;
2.200)	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;
2.201)	Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
2.202)	Suportar lectura y revisión de CRL (lista de revocación de certificados);
2.203)	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
2.204)	Debe permitir que la conexión a la VPN se establece de la siguiente manera: Antes de que el usuario se autentique en su estación
2.205)	Debería permitir la conexión a la VPN se establece de la siguiente manera: Después de la autenticación de usuario en la estación;
2.206)	Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo demanda de los usuarios;
2.207)	Deberá mantener una conexión segura con el portal durante la sesión;
2.208)	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
2.209)	Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada
2.210)	Soportar servicio del servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos
2.211)	Soporte IPv4 e IPv6 por SSID
2.212)	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
2.213)	Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point
2.214)	Soportar monitoreo y supresión de puntos de acceso indebidos
2.215)	Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS
2.216)	Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows
2.217)	Permitir la visualización de los dispositivos inalámbricos conectados por usuario

[redacted]2

[redacted]2

SECRETARÍA ADMINISTRATIVA

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

2.216)	Permitir la visualización de los dispositivos inalámbricos conectados por IP
2.219)	Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación
2.220)	Permitir la visualización de los dispositivos inalámbricos conectados por canal
2.221)	Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado
2.222)	Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal
2.223)	Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación
2.224)	Debe soportar Fast Roaming en autenticación con portal cautivo
2.225)	Debe soportar configuración de portal cautivo por SSID
2.226)	Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico
2.227)	Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP.
2.228)	Debe ser compatible con el protocolo 802.1x RADIUS
2.229)	La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal
2.230)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática
2.231)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática
2.232)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP
2.233)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por dns
2.234)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por broadcast
2.235)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por multicast
2.236)	La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue)
2.237)	La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico
2.238)	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
2.239)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP
2.240)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding
2.241)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding
2.242)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication
2.243)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding
2.244)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI
2.245)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack

SECRETARÍA ADMINISTRATIVA

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

2.246)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response
2.247)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication
2.248)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection
2.249)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge
2.250)	Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas
2.251)	Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso
2.252)	La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible
2.253)	La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario
2.254)	Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID
2.255)	Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso
2.256)	Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio
2.257)	La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh
2.258)	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
2.259)	La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS
2.260)	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
2.261)	Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso
2.262)	Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso
2.263)	Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica;
2.264)	Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión
2.265)	Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados
2.266)	La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz
2.267)	Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados
2.268)	Debe permitir asociación dinámicas de VLANs a los usuarios autenticados en un SSID específico mediante protocolo RADIUS
2.269)	Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID específico mediante vlan pooling

SECRETARÍA ADMINISTRATIVA

[redacted]

[redacted]

[redacted]

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted] 3

2.270)	Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico
2.271)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones
2.272)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino
2.273)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza
2.274)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones
2.275)	la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico
2.276)	El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo
2.277)	El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales
2.278)	La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico
2.279)	La controladora inalámbrica deberá soportar aceleración de tunnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico
2.280)	La controladora inalámbrica debe soportar protocolo LLDP
2.281)	Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta
2.282)	Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC Adyacente
2.283)	Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos
1 2.284)	La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado
2.285)	La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas
2.286)	La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada
2.287)	Deberá soportar la conversion de Multicast a Unicast para mejorar el rendimiento del tiempo de aire

SOLUCIÓN UTM/NGFW "TIPO B"

1.1)	Throughput de por lo menos 11 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete
1.2)	Soporte a por lo menos 3M conexiones simultaneas
1.3)	Soporte a por lo menos 280K nuevas conexiones por segundo
1.4)	Throughput de al menos 13 Gbps de VPN IPSec
1.5)	Estar licenciado para, o soportar sin necesidad de licencia, 2K tuneles de VPN IPSec site-to-site simultaneos
1.6)	Estar licenciado para, o soportar sin necesidad de licencia, 16K tuneles de clientes VPN IPSec simultaneos
1.7)	Throughput de al menos 2000 Mbps de VPN SSL
1.8)	Soportar al menos 500 clientes de VPN SSL simultaneos

SECRETARÍA ADMINIST

[redacted] 2

[redacted] 2

[redacted]

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

1.9)	Soportar al menos 5000 Mbps de throughput de IPS
1.10)	Soportar al menos 4000 Mbps de throughput de inspeción SSL
1.11)	Throughput de al menos 3000 Mbps con las siguientes funcionalidades habilitadas simultaneamente para todas las firmas que la solución de seguridad tenga debidamente activadasy operativas: control de aplicaciones, IPS, Antivírus y Antispyware. Caso el fabricante tenga publicado multiples numeros de disempeño para cualquier de las funcionalidades, solamente el de valor más pequeño sera aceptado.
1.12)	Permitir gestionar como controladora inalámbrica al menos 256 Access Points y gestionar por lo menos 64 Switches de la misma marca del fabricante del UTM/NGFW dentro de la misma interfase de gestion
1.13)	Tener al menos 4 interfaces 10 Gbps SFPP, 8 interfases de 1 Gbps SFP, 16 interfases de 1GE RJ45, 2 interfases 1 Gbps RJ45 para Gestion y alta disponibilidad
1.15)	Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance
1.16)	Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance
1.17)	Debe de incluir un token fisico para autenticacion de doble factor para la gestion del appliance o para el acceso VPN que debe ser de la misma marca propuesta
1.18)	Debe de 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema, Control de Aplicaciones, IPS, Antivirus, Botnet IP/Domain, AntiSpam y Filtrado Web
1.19)	Debe de contar con dos fuentes de poder AC de 100-240 VAC para alta disponibilidad
1.20)	Deberá contar con 36 meses de soporte del tipo 7x24, reemplazo siguiente dia habil, con actualizaciones de sistema de firmware, y los siguientes módulos incluidos IPS ó Preventor de Intrusos, Antivirus , Protección contra Botnet IP/Domain, Módulo de Protección de Mobile Malware, Módulo de Sandbox en nube incluyendo Virus Outbreak and Content Disarm & Reconstruct, Control de aplicaciones, Filtrado Web & Video Filtering y Módulo de AntiSpam.

2) Requisitos Mínimos de Funcionalidad

Caracteristicas Generales

2.1)	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.
2.2)	Por funcionalidades de NGFW se entiende: aplicaciones de reconocimiento, prevención de amenazas, identificación de usuarios y control granular de permisos;
2.3)	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;
2.4)	La plataforma debe estar optimizada para aplicaciones de análisis de contenido en la capa 7;
2.5)	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;
2.6)	La gestión del equipo debe ser compatible con acceso a través de SSH, consola, web (HTTPS) y API abierta;
2.7)	La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
2.8)	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
2.9)	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
2.10)	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
2.11)	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
2.12)	Los dispositivos de protección de red deben soportar DHCP Relay;
2.13)	Los dispositivos de protección de red deben soportar DHCP Server;
2.14)	Los dispositivos de protección de red deben soportar sFlow
2.15)	Los dispositivos de protección de red deben soportar Jumbo Frames;
2.16)	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas
2.17)	Debe ser compatible con NAT dinámica (varios-a-1);
2.18)	Debe ser compatible con NAT dinámica (muchos-a-muchos);
2.19)	Debe soportar NAT estática (1-a-1);
2.20)	Debe admitir NAT estática (muchos-a-muchos);
2.21)	Debe ser compatible con NAT estático bidireccional 1-a-1;
2.22)	Debe ser compatible con la traducción de puertos (PAT);
2.23)	Debe ser compatible con NAT Origen;
2.24)	Debe ser compatible con NAT de destino;

SECRETARÍA ADMINISTRATIVA

[redacted]

[redacted]

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]3

2.25)	Debe soportar NAT de origen y NAT de destino de forma simultánea;
2.26)	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
2.27)	Debe ser compatible con NAT64 y NAT46;
2.28)	Debe implementar el protocolo ECMP;
2.29)	Debe soportar el balanceo de enlace hash por IP de origen;
2.30)	Debe soportar el balanceo de enlace hash por IP de origen y destino;
2.31)	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;
2.32)	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales
2.33)	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
2.34)	Enviar logs a sistemas de gestión externos simultáneamente;
2.35)	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
2.36)	Debe soporta protección contra la suplantación de identidad (anti-spoofing);
2.37)	Implementar la optimización del tráfico entre dos dispositivos;
2.38)	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
2.39)	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
2.40)	Soportar OSPF graceful restart;
2.41)	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);
2.42)	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
2.43)	Debe soportar modo capa - 2 (L2) para la inspección de datos en línea y la visibilidad del tráfico;
2.44)	Debe soportar modo capa - 3 (L3) para la inspección de los datos de la visibilidad en línea de tráfico;
2.45)	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
2.46)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
2.47)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
2.48)	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
2.49)	La configuración de alta disponibilidad debe sincronizar: Sesiones;
2.50)	La configuración de alta disponibilidad debe sincronizar: configuración, incluyendo, pero no limitados políticas de Firewalls, NAT, QoS y objetos de la red;
2.51)	La configuración de alta disponibilidad debe sincronizar: las asociaciones de seguridad VPN;
2.52)	La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
2.53)	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
2.54)	Debe soportar la creación de sistemas virtuales en el mismo equipo;
2.55)	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;
2.56)	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;
2.57)	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;
2.58)	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

2.59)	Debe soportar controles de zona de seguridad
2.60)	Debe contar con políticas de control por puerto y protocolo
2.61)	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

[redacted]2

[redacted]2

SECRETARÍA ADMINISTRAT

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted] 3

2.62)	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad
2.63)	Control de política por código de país (por ejemplo: BR, USA., UK, RUS)
2.64)	Control, inspección y des encriptación de SSL por política para el tráfico entrante y la salida
2.65)	Debe soportar el bajado de certificados de inspección de conexiones SSL de entrada;
2.66)	Debe descifrar las conexiones de entrada y salida de tráfico negociadas con TLS 1.2;
2.67)	Control de inspección y descifrado SSH por política;
2.68)	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;
2.69)	Traffic shaping QoS basado en políticas (garantía de prioridad y máximo);
2.70)	QoS basado en políticas para marcación de paquetes (Diffserv marking), incluyendo por aplicaciones;
2.71)	Soporte para objetos y reglas IPV6;
2.72)	Soporte objetos y reglas de multicast;
2.73)	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 unreachable por la máquina fuente de tráfico, TCP Reset para el cliente . RESET de TCP con el servidor o en ambos lados de la conexión;
2.74)	Soportar la calendarización de políticas con el fin de activar y desactivar las reglas en tiempos predefinidos de forma automática;

Control de Aplicación

2.75)	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo
2.76)	Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos
2.77)	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, video, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
2.78)	Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmain, 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;
2.79)	Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;
2.80)	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;
2.81)	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
2.82)	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;
2.83)	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
2.84)	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
2.85)	Actualización de la base de firmas de la aplicación de forma automática;
2.86)	Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos;
2.87)	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;
2.88)	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;
2.89)	Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;
2.90)	Para mantener la seguridad de red eficiente debe ser soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
2.91)	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
2.92)	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
2.93)	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
2.94)	Debe alertar al usuario cuando sea bloqueada una aplicación;
2.95)	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;

[redacted] 2

SECRETARÍA ADMINIST

[redacted] 2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

2.96)	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
2.97)	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;
2.98)	Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
2.99)	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)
2.100)	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: nivel de riesgo de la aplicación
2.101)	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación

Prevención de Amenazas

2.102)	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
2.103)	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
2.104)	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;
2.105)	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad;
2.106)	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;
2.107)	Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo;
2.108)	Deben ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad
2.109)	Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas;
2.110)	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
2.111)	Deber permitir el bloqueo de vulnerabilidades
2.112)	Debe permitir el bloqueo de exploits conocidos
2.113)	Debe incluir la protección contra ataques de denegación de servicio
2.114)	Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones;
2.115)	Debe tener los siguientes mecanismos de inspección IPS: análisis de decodificación de protocolo;
2.116)	Debe tener los siguientes mecanismos de inspección IPS: análisis para detectar anomalías de protocolo.
2.117)	Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico;
2.118)	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
2.119)	Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;
2.120)	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets)
2.121)	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones SYN, ICMP , UDP, etc;
2.122)	Detectar y bloquear los escaneos de puertos de origen;
2.123)	Bloquear ataques realizados por gusanos (worms) conocidos;
2.124)	Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
2.125)	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
2.126)	Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
2.127)	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;
2.128)	Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;
2.129)	Soportar el bloqueo de archivos por tipo;
2.130)	Identificar y bloquear la comunicación con redes de bots;
2.131)	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;

SECRETARÍA ADMINISTRATIVA

[redacted]

2

[redacted]

2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

2.132)	Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
2.133)	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
2.134)	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;
2.135)	Los eventos deben identificar el país que origino la amenaza;
2.136)	Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms)
2.137)	Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP
2.138)	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	
2.139)	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);
2.140)	Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad
2.141)	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;
2.142)	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;
2.143)	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL
2.144)	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;
2.145)	Tener por lo menos 60 categorías de URL;
2.146)	Debe tener la funcionalidad de exclusión de URLs por categoría
2.147)	Permitir página de bloqueo personalizada;
2.148)	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	
2.149)	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;
2.150)	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;
2.151)	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;
2.152)	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;
2.153)	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;
2.154)	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;
2.155)	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);
2.156)	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;
2.157)	Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos del LDAP / AD
2.158)	Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
2.159)	Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores
QoS Traffic Shaping	
2.160)	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;
2.161)	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
2.162)	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;

SECRETARÍA ADMINISTRATIVA

[redacted]

2

[redacted]

2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

2.163) Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
2.164) Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
2.165) Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
2.166) QoS debe permitir la definición de tráfico con ancho de banda garantizado;
2.167) QoS debe permitir la definición de tráfico con máximo ancho de banda;
2.168) QoS debe permitir la definición de cola de prioridad;
2.169) Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype;
2.170) Soportar marcación de paquetes DiffServ, incluso por aplicación;
2.171) Soportar la modificación de los valores de DSCP para Diffserv;
2.172) Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service)
2.173) Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shapig;
2.174) Debe soportar QoS (traffic-shaping) en la interfaz agregada o redundantes;

Filtro de Datos

2.175) Permite la creación de filtros para archivos y datos predefinidos;
2.176) Los archivos deben ser identificados por tamaño y tipo;
2.177) Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);
2.178) Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
2.179) Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
2.180) 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

2.181) Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
2.182) Debe permitir la visualización de los países de origen y destino en los registros de acceso;
2.183) Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

VPN

2.184) Soporte VPN de sitio a sitio y cliente a sitio;
2.185) Soportar VPN IPSec;
2.186) Soportar VPN SSL;
2.187) La VPN IPSec debe ser compatible con 3DES;
2.188) La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;
2.189) La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y el Grupo 14;
2.190) La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
2.191) La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
2.192) La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI
2.193) Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
2.194) Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec
2.195) Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;
2.196) 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;
2.197) Las características de VPN SSL se deben cumplir con o sin el uso de agentes;
2.198) 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;

SECRETARÍA ADMINISTRATIVA

2

2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

2.199)	Asignación de DNS en la VPN de cliente remoto;
2.200)	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;
2.201)	Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
2.202)	Suportar lectura y revisión de CRL (lista de revocación de certificados);
2.203)	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
2.204)	Debe permitir que la conexión a la VPN se establece de la siguiente manera: Antes de que el usuario se autentique en su estación
2.205)	Debería permitir la conexión a la VPN se establece de la siguiente manera: Después de la autenticación de usuario en la estación;
2.206)	Debe permitir la conexión a la VPN se establece de la siguiente manera: Bajo demanda de los usuarios;
2.207)	Deberá mantener una conexión segura con el portal durante la sesión;
2.208)	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

2.209)	Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada
2.210)	Soportar servicio del servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos
2.211)	Soporte IPv4 e IPv6 por SSID
2.212)	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
2.213)	Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point
2.214)	Soportar monitoreo y supresión de puntos de acceso indebidos
2.215)	Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS
2.216)	Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows
2.217)	Permitir la visualización de los dispositivos inalámbricos conectados por usuario
2.218)	Permitir la visualización de los dispositivos inalámbricos conectados por IP
2.219)	Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación
2.220)	Permitir la visualización de los dispositivos inalámbricos conectados por canal
2.221)	Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado
2.222)	Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal
2.223)	Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación
2.224)	Debe soportar Fast Roaming en autenticación con portal cautivo
2.225)	Debe soportar configuración de portal cautivo por SSID
2.226)	Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico
2.227)	Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP.
2.228)	Debe ser compatible con el protocolo 802.1x RADIUS
2.229)	La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal
2.230)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática
2.231)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática
2.232)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP
2.233)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por dns
2.234)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por broadcast
2.235)	La controladora deberá permitir métodos de descubrimiento de puntos de acceso por multicast
2.236)	La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue)

SECRETARÍA ADMINISTRATIVA

[redacted]

[redacted]

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]3

2.237)	La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico
2.238)	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
2.239)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP
2.240)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding
2.241)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding
2.242)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication
2.243)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding
2.244)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI
2.245)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack
2.246)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response
2.247)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authenticación
2.248)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection
2.249)	La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge
2.250)	Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas
2.251)	Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso
2.252)	La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible
2.253)	La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario
2.254)	Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID
2.255)	Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso
2.256)	Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio
2.257)	La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh
2.258)	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
2.259)	La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS
2.260)	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
2.261)	Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso
2.262)	Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso
2.263)	Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica;
2.264)	Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión
2.265)	Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados
2.266)	La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz
2.267)	Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados
2.268)	Debe permitir asociación dinámicas de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS
2.269)	Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling
2.270)	Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico
2.271)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones
2.272)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino
2.273)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza
2.274)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones
2.275)	la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico

[redacted]2

[redacted]2

SECRETARÍA ADMINISTRATIVA

[redacted]

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted] 3

	2.276)	El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo
	2.277)	El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales
	2.278)	La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico
	2.279)	La controladora inalámbrica deberá soportar aceleración de tunnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico
	2.280)	La controladora inalámbrica debe soportar protocolo LLDP
	2.281)	Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta
	2.282)	Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC Adyacente
	2.283)	Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos
	2.284)	La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado
	2.285)	La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas
	2.286)	La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada
	2.287)	Deberá soportar la conversion de Multicast a Unicast para mejorar el rendimiento del tiempo de aire
3		**SOLUCIÓN DE ADMINISTRACIÓN CENTRALIZADA SD-WAN UTM/NGFW Y SOLUCIÓN DE CORRELACIÓN DE LOGS Y INCIDENTES DE SEGURIDAD SD-WAN UTM/NGFW** **1) Solución de Administración Centralizada** 1.1) Solución de Administracion centralizada de Dispositivos SD-WAN UTM/NGFW con Licenciamiento de Actualizaciones de Firmware, soporte 24x7 por 60 meses. 1.2) La solución deberá ser escalable en 10, 100 y hasta 1000 dispositivos , con soporte en Hypervisor Vmware, Microsoft HyperV, Xen Server, KVM 1.3) Debe permitir gerenciar al menos 100 dispositivos **2) Requisitos Mínimos de Funcionalidad** **Funcionalidades Generales** 2.1) Debe permitir Gerenciar los dispositivos de la misma marca que los equipos ofertados, generando políticas centralizadas, control de cambios, revision de versiones, respaldos de configuracion y perfiles de usuarios 2.2) Si la solución es virtualizada, debe ser compatible con el ambiente VMware ESXi 5.5 e 6.0; 2.3) Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2 2.4) Si la solución es virtualizada, debe ser compatible con el ambiente Citrix XenServer 6.0+ 2.5) Si la solución es virtualizada, debe ser compatible con el ambiente Open Source Xen 4.1+ 2.6) Si la solución es virtualizada, debe ser compatible con el ambiente KVM 2.7) Si la solución es virtualizada, debe ser compatible con el ambiente Amazon Web Services (AWS) 2.8) No debe haber límites a la cantidad de múltiples vCPU si el aparato es virtual; 2.9) No debe haber límites a la expansión de memória RAM si el aparto es virtual; 2.10) En la fecha de la propuesta, ninguno de los modelos de la oferta pueden estar en el sitio del fabricante en listados de end-of-life o end-of-sales; 2.11) La gestión de la solición debe soportar acesso por SSH, cliente o WEB (HTTPS) y API abierta; 2.12) Debe permitir acesso concurrentes de administradores; 2.13) Debe tener interfaz basada en línea de comando para administración de la solución de gestión; 2.14) Debe tener un mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos; 2.15) Bloquear cambios, en el caso de acceso simultaneo de dos o más administradores; 2.16) Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, accesso de lectura, creación de usuários, cambio de configuraciones; 2.17) Generar alertas automáticos por Email 2.18) Generar alertas automáticos por SNMP 2.19) Generar alertas automáticos por Syslog 2.20) Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horário; 2.21) Debe ser permitido al administrador transferir los backups a un servidor FTP. 2.22) Debe ser permitido al administrador transferir los backups a un servidor SCP 2.23) Debe ser permitido al administrador transferir los backups a un servidor SFTP 2.24) Los cambios realizados en un servidor de gestión debe ser automaticamente replicados al servidor redundante; 2.25) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de cuentas de usuários LOCALES 2.26) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa TACACS 2.27) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa LDAP 2.28) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa RADIUS 2.29) Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de Certificado Digital X.509 (PKI) 2.30) Debe soportar sincronización de reloj interno por protocolo NTP. 2.31) Debe registrar las acciones efectuadas por cualquier usuário; 2.32) Deben ser fornecidos manuales de instalación, configuración y operación de toda la solución, e los idiomas portugués o inglés, com apresentación de buena calidad; 2.33) Debe suportar SNMP versión 2 y la versión 3 en los equipos de gestión; 2.34) Debe permitir habilitar o deshabilitar, para cada interfaz de red de la solución de gestión, permisos de acceso HTTP, HTTPS, SSH, SNMP y Telnet; 2.35) Debe permitir virtualizar la solución de gestión, de manera que cada administrador pueda gerenciar, visualizar y editar solo los dispositivos autorizados y registrados en su ambiente virtualizado; 2.36) La solución de gestión debe permitir crear administradores que tengan acceso a todas las instancias de virtualización; **Funcionalidades de APIs** 2.37) Debe soportar XML API 2.38) Debe soportar JSON API **Funcionalidades de Gestión de SDWAN UTM/NGFW** 2.39) La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación; 2.40) La gestión debe permitir la creación y administración de políticas de IPS, Antivirus y Anti-Spyware;

SECRETARÍA ADMINISTRATIVA

[redacted] 2

[redacted] 2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted] 3

2.41) La gestión debe permitir la creación y administración de políticas de Filtro de URL;
2.42) Permitir buscar cuáles reglas un objeto está siendo utilizado;
2.43) Debe atribuir secuencialmente un número a cada regla de firewall;
2.44) Debe atribuir secuencialmente un número a cada regla de firewall;DOS;
2.45) Permitir la creación de reglas que permanezcan activas en horário definido;
2.46) Permitir backup de las configuraciones y rollback de configuración para la última configuración salva;
2.47) Debe tener mecanismos de validación de políticas avisando cuando hayan reglas que ofusquen o conflictuen con otras (shadowing);
2.48) Debe posibilitar la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas;
2.49) Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión;
2.50) Cada servidor de gestión debe ser hospedado en un equipo independiente, no ejecutando función de firewall;
2.51) La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador atualizar licencias en los aparatos a través de esta herramienta;
2.52) La solución debe permitir la distribución y instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos;
2.53) Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados;
2.54) Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas despuez de la aprobación de otro administrador;
2.55) Tener "wizard" en la solución de gestion para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de los mismos;
2.56) Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados cuando el mismo es agregado a la solución de gestión;
2.57) Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horário de lo sistema y firmware;
2.58) Tener "wizard" en la solución de gestion para instalación de políticas y configuraciones de los dispositivos;
2.59) Permitir crear en la solución de gestión templates de configuración de los dispositivos con informadiones de DNS, SNMP, configuraciones de LOG y administración;
2.60) Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos;
2.61) Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión;
2.62) Permitir configurar y visualizar balanceo de enlaces en los dispositivos gestionados de forma centralizada;
2.63) Permitir crear vários paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos;
2.64) Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada;
2.65) Permitir la creación de regias anti DoS de forma centralizada;
2.66) Permitir la creación de objetos que serán utilizados en las políticas de forma centralizada;
2.67) Permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topologia (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía;
2.68) Permitir la utilizacion de Zero Touch Provisioning para automatizar las configuraciones de los Dispositivos administrados Gerenciados
2.69) Permitir la utilizacion de Plantillas para automatizar la configuracion de los Modulos de SD-WAN de los dispositivos

1) Caracteristicas

1.1) Solución de Correlación de Logs centralizada de Dispositivos SD-WAN UTM/NGFW con Licenciamiento de Actualizaciones de Sistema de Firmware, soporte 24x7 por 60 meses.
1.2) Tener capacidad de recibir al menos 50 GBytes de logs diarios
1.3) Deberá Soportar Identificadores de Compromiso
1.4) Deberá soportar módulo de SoC
1.5) Soportar módulo de "Outbreak Alert Service"
1.6) Deberá ser por cuestiones de compatibilidad , la misma marca que los dispositivos SD-WAN UTM / NGFW
1.7) La solución debe ser escalable o stackeable en 5GB/50GB/500 GB logs al día

2) Requisitos Minimos de Funcionalidad

Funcionalidades Generales

2.1) Si la solución es virtualizada, debe ser compatible con el ambiente VMware ESXi 5.0/5.1/5.5/6.0/6.5/6.7;
2.2) Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2/2016
2.3) Si la solución es virtualizada, debe ser compatible con el ambiente Citrix XenServer 6.0+
2.4) Si la solución es virtualizada, debe ser compatible con el ambiente Open Source Xen 4.1+
2.5) Si la solución es virtualizada, debe ser compatible con el ambiente KVM on Redhat 6.5+ and Ubuntu 17.04
2.6) Si la solución es virtualizada, debe ser compatible con el ambiente Nutanix AHV (AOS 5.10.5)
2.7) Si la solución es virtualizada, debe ser compatible con el ambiente Amazon Web Services (AWS)
2.8) Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Azure.
2.9) Si la solución es virtualizada, debe ser compatible con el ambiente Google Cloud (GCP)
2.10) Si la solución es virtualizada, debe ser compatible con el ambiente Oracle Cloud Infrastructure (OCI)
2.11) Si la solución es virtualizada, debe ser compatible con el ambiente Alibaba Coud (AliCloud)
2.12) Si la solución es virtualizada, no debe haber límites a la cantidad de múltiples vCPU
2.13) Si la solución es virtualizada, no debe haber límites a la expansión de memoria RAM
2.14) Debe soportar acceso vía SSH, WEB (HTTPS) para la gestion de la solución
2.15) Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía linea de comandos en consola de gestión.
2.16) Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
2.17) Soporte SNMP versión 2 y 3
2.18) Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
2.19) Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
2.20) Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH
2.21) Autenticación de usuarios de acceso a la plataforma vía LDAP
2.22) Autenticación de usuarios de acceso a la plataforma vía Radius
2.23) Autenticación de usuarios de acceso a la plataforma vía TACACS+
2.24) Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos
2.25) Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
2.26) Generación de informes en tiempo real de tráfico, en formato de gráfica tabla
2.27) Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
2.28) Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.

[redacted] 2

SECRETARÍA ADMINISTRATIVA

[redacted] 2

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL
TEL: [redacted]

[redacted]

2.29) Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado
2.30) Contar con mecanismos de borrado automático de logs antiguos.
2.31) Permitir la importación y exportación de reportes
2.32) Debe contar con la capacidad de crear informes en formato HTML
2.33) Debe contar con la capacidad de crear informes en formato PDF
2.34) Debe contar con la capacidad de crear informes en formato XML
2.35) Debe contar con la capacidad de crear informes en formato CSV
2.36) Debe permitir exportar los logs en formato CSV
2.37) Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
2.38) Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
2.39) La solución debe contar con reportes predefinidos
2.40) Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución
2.41) Debe ser posible la duplicación de reportes existentes para su posterior edición.
2.42) Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
2.43) Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
2.44) Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
2.45) Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
2.46) Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
2.47) Debe permitir descargar de la plataforma los archivos de logs para uso externo.
2.48) Tener la capacidad de generar y enviar reportes periódicos automáticamente.
2.49) Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
2.50) Permitir el envío por email de manera automática de reportes.
2.51) Debe permitir que el reporte a enviar por email sea al destinatario específico.
2.52) Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
2.53) Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
2.54) Debe permitir el uso de filtros en los reportes.
2.55) Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
2.56) Permitir especificar el idioma de los reportes creados
2.57) Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
2.58) Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
2.59) Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.
2.60) Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
2.61) Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.
2.62) Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
2.63) Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
2.64) Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
2.65) Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
2.66) Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos
2.67) Debe permitir visualizar en tiempo real los logs recibidos.
2.68) Debe permitir el reenvío de logs en formato syslog.
2.69) Debe permitir el reenvío de logs en formato CEF (Common Event Format).
2.70) Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red
2.71) Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
2.72) Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.
2.73) Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red
2.74) Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
2.75) Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.
2.76) Debe incluir dashboard para operaciones SOC que monitorea actividad VPN ren su red.
2.77) Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs
2.78) Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)
2.79) Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC
2.80) Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3
2.81) Debe permitir generar alertas de eventos a partir de logs recibidos
2.82) Debe permitir crear incidentes a partir de alertas de eventos para endpoint
2.83) Debe permitir la integración al sistema de tickets ServiceNow
2.84) Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
2.85) Debe permitir respaldar logs en nube publica de Amazon S3
2.86) Debe permitir respaldar logs en nube publica de Microsoft Azure
2.87) Debe permitir respaldar logs en nube publica de Google Cloud
2.88) Debe soportar el estándar SAML para autenticación de usuarios administradores

Reportes de Firewall

2.89) Debe contar con reporte de cumplimiento de PCI DSS
2.90) Debe contar con reporte de utilización de aplicaciones SaaS
2.91) Debe contar con reporte de prevención de perdida de datos (DLP)
2.92) Debe contar con reporte de VPN
2.93) Debe contar con reporte de Sistema de prevención de intrusos (IPS)
2.94) Debe contar con reporte de reputación de cliente
2.95) Debe contar con reporte de análisis de seguridad de usuario
2.96) Debe contar con reporte de análisis de amenaza cibernética
2.97) Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad
2.98) Debe contar con reporte de tráfico DNS
2.99) Debe contar con reporte tráfico de correo electrónico
2.100) Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red

SECRETARÍA ADMINISTRATIV

[redacted]

[redacted]

[redacted]

INITEL S.A DE C.V
Av. Patria 888 Piso 2A Oficina T
Jardines Universidad C.P.45110
Zapopan, JAL

[redacted] 3

2.101	Debe contar con reporte de Top 10 de Websites utilizadas en la red
2.102	Debe contar con reporte de uso de redes sociales
Reportes de Fabric	
2.103	Debe contar con reporte de evaluación de riesgo para correo electrónico
Reportes de Wireless	
2.104	Debe contar con reporte de cumplimiento PCI de Wireless
2.105	Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WiFi.
Reportes de Endpoint	
2.106	Debe contar con reporte de vulnerabilidades de solución gestionada de seguridad de equipo terminal
Reportes de WAF	
2.107	Debe contar con reporte de aplicaciones web si se cuenta con plataforma de seguridad web
Reportes de SD-WAN	
	Debe de contar con reportes de la utilización del módulo de SD-WAN de los dispositivos que realicen la conexión en la solución

ATENTAMENTE
Zapopan, Jalisco; a 13 de octubre de 2021

[redacted] 2

4 Teobaldo Leal Arriaga
Representante Legal
Initel S.A. de C.V.

SECRETARÍA ADMINISTRATIVA

[redacted] 2

1.- Se testa una clave patronal 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.
2.- Se testan sesenta y dos 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.
3.- Se testan veintidós 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.
4.- Se testan dos grados académicos, 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 VIII, de los Lineamientos Generales de Protección de Información Confidencial y Reservada por contener datos de carácter personal.