UNIVERSIDAD DE CALDAS
NIT: 890801063

INVITACIÓN POR OFERTA PRIVADA No. 331 DE 2015

Proponentes

COLOMBIANET
Calle 55 No. 24-07
8862212/8852578
maria.ramirez@colombianet.com.co
Manizales

CARVAJAL TECNOLOGÍA Y SERVICIOS
Carrera 23C No 62-06 Oficina 701
8860509 Ext 30701
3164541842
liliana.betancourth@carvajal.com
Manizales

GLOBAL S.AS
Carrera 27 No. 37-19
8840809
global2008@yahoo.com
proyectos@globalsas.co
Manizales

COMPUREDES S.A.
Calle 19 No. 43G - 169 piso 8 Ed. Torres del Río (Medellín)
Calle 19 # 9 - 50 Oficina 2106 (Pereira)
(4) 444 61 00 EXT 1111
3182194439 - 3166976000-317 641 8824
adriana.sanchez@compuredes.com.co
sara.garcia@compured-es.com.co
Medellín- Pereira.

INGENIERÍA TELEMÁTICA
Calle 14 No 16-47 Barrio Pinares
gerencia@ingenieriatelematica.com.co
3347444
Pereira

OBJETO

Compra de un sistema de seguridad informática perimetral que sea del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés), donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento. Incluye instalación, configuración, programación y suscripción internacional por 3 años.

CRONOGRAMA

FECHA DE APERTURA: **DÍA** 20 **MES** 10
EECHA MAX. ENTREGA PROPUESTAS: **DÍA** 3 **MES** 11 **HORA** 5:00pm.
FECHA PROBABLE DE ADJUDICACIÓN: **DÍA** 9 **MES** 11

GENERALIDADES

El proponente deberá aportar los siguientes documentos:

1. Encontrarse inscrito en el BANCO DE PROVEEDORES de la Universidad de Caldas, lo que se podrá efectuar a través de la página principal www.ucaldas.edu.co, link de contratación, portal web de contratación, solicitud de registro de proveedor.

2. Carta de presentación de la propuesta: ANEXO 1

3. Carta de no inhabilidades y compromiso ético: ANEXO 2

4. Carta de especificaciones técnicas ANEXO 3, indicando que cumple en las respectivas tablas.

5. Formulario de estados financieros ANEXO 4 correspondiente a los años 2013 y 2014.

6. Certificado de Existencia y Representación legal con fecha de expedición no superior a 90 días.

7. Aportar propuesta económica al cual debe indicar (no es subsanable ni en su contenido, ni por su falta de presentación):
   IVA discriminado (si están obligados a ello)
   Valor total de la oferta

8. Aportar declaración de renta de los años 2013 y 2014.

9. Póliza de seriedad de la oferta por el diez porciento (10%) del valor del presupuesto convocado y vigente hasta la fecha señalada como probable para la adjudicación, firmada por el representante legal.

10. Copia de la cédula de ciudadanía del representante legal.

11. Certificación del Revisor Fiscal (cuando por disposición legal lo deban tener) o del representante legal, de estar a paz y salvo en los aportes a seguridad social y parafiscales de sus empleados. Adjuntando del Revisor Fiscal su tarjeta profesional, fotocopia de la cédula de ciudadanía y la certificación vigente de la Junta Central de Contadores de no haber sido sancionado.

12. El oferente debe certificar experiencia de mínimo tres (3) en contratos similares ejecutados en Colombia, en los últimos 3 años, que involucren la implementación de soluciones de seguridad perimetral y que sumados sus valores sea igual o superior al presupuesto de la presente invitación. Las certificaciones o copias de los contratos deben ser anexadas a la propuesta y deben contener como mínimo la siguiente información:
    - Nombre o razón social de la empresa contratante.
    - Objeto del contrato.
    - Valor del contrato ejecutado.
    - Fecha de inicio y fecha de finalización del contrato.
    - Datos de contacto: nombre, cargo y teléfono de quien certifica.

13. Certificación en la tecnología ofertada. El oferente deberá acreditar mediante comunicación del fabricante, ser canal autorizado de la herramienta de seguridad perimetral de la marca ofrecida. El oferente debe anexar certificación del fabricante como canal gold.

14. El oferente debe anexar certificados expedidos por el fabricante con mínimo de 3 años de antigüedad que avalen la capacidad técnica del personal que realizará la implementación de la seguridad perimetral.

15. Analistas de redes: 2 Ingenieros de Sistemas y/o Electrónicos y/o Afines, certificados por el fabricante con mínimo 3 años de antigüedad como expertos en la herramienta, calificados cada uno de ellos para ejecutar el alcance del contrato. Incluir con la oferta fotocopia del diploma profesional de los dos analistas y las certificaciones.

16. Los flujos de caja operativo positivo en los últimos seis (6) meses (mes a mes) del año 2014, conforme se solicitan en la revisión financiera.

17. Todas las certificaciones del fabricante solicitadas en generalidades y especificaciones técnicas.

ESPECIEICACIONES TÉCNICAS (VER ANEXO 3)

OBLIGACIONES

El **CONTRATISTA** se obligará a:

1. Cumplir con todas y cada una de las condiciones técnicas presentadas en la oferta que corresponderán a las solicitadas en la presente invitación a cotizar.

2. Estar a paz y salvo con los aportes a seguridad social y parafiscales.

3. Permitir que en la instalación esté presente el personal de la Universidad de Caldas que determine el supervisor del contrato.

PARTICIPACIÓN DE LAS VEEDURÍAS CIUDADANAS

La Universidad de Caldas, con el fin de garantizar las diferentes formas de participación ciudadana y control social, convoca a las veedurías ciudadanas que de conformidad con la Ley 850 de 2003 podrán ejercer el control y vigilancia de la gestión pública contractual, durante las etapas precontractual, contractual y postcontractual.

DURACIÓN DEL CONTRATO

Para la puesta en funcionamiento el contratista contará con cuarenta y cinco (45) días hábiles desde la fecha de legalización y el soporte respectivo durará tres (3) años contados a partir de la puesta en funcionamiento del sistema de seguridad perimetral.

REVISIÓN Y EVALUACIÓN DE LAS PROPUESTAS

La revisión y evaluación de las propuestas presentadas constará de un estudio jurídico, uno financiero, una evaluación técnica y finalmente la asignación de puntaje de cada una de las propuestas, de acuerdo a lo establecido en la presente invitación.

REVISIÓN JURÍDICA

Jurídicamente se examinará que dentro de la propuesta hayan sido aportados los documentos. Queda entendido que las propuestas cuyos documentos no se encuentren

ajustados a las condiciones y especificaciones que sobre ellos se hayan solicitado, o que habiéndolo solicitado, no hayan sido subsanados oportunamente, serán eliminadas en esta fase y no continuarán en examen.

Conforme a lo anterior, y en consecuencia, a la propuesta que sea eliminada en la fase de revisión jurídica no se le asignará ninguna puntuación y, por lo mismo, no será objeto de comparación con otras propuestas, ni tampoco referente para la calificación de las mismas.

REVISIÓN FINANCIERA:

Se calcularán los siguientes indicadores financieros y se verificará el cumplimiento de las condiciones que se detallan a continuación. Queda entendido que las propuestas cuyos documentos no se encuentren ajustados a las condiciones y especificaciones que sobre ellos se hayan solicitado, o que habiéndolo solicitado, no hayan sido subsanados oportunamente, serán eliminadas en esta fase.

FLUJOS DE CAJA: Se deberá acreditar un flujo de caja operativo positivo en los últimos seis (6) meses (mes a mes) del año 2014, certificados por el revisor fiscal, cuando este exista de acuerdo con los requerimientos de ley, o en su defecto, por el representante legal, con el aval de un contador público.

CAPITAL DE TRABAJO: Se calculará con base en la siguiente formula y su resultado deberá ser mayor o igual a 50 SMLMV

CT = AC – PC donde,

CT: Capital de trabajo
AC: Activo corriente
PC: Pasivo Corriente

NIVEL DE ENDEUDAMIENTO: deberá ser menor o igual al cincuenta por ciento (50%)

E= PT / AT≤ 0.50 donde,

E: Nivel de endeudamiento
PT: Pasivo total
AT: Activo total

RELACIÓN PATRIMONIAL: deberá ser menor o igual a cinco (5) conforme a la siguiente fórmula.

RP= VC / P ≤ 5.0 donde,

RP: Relación patrimonial
VC: Valor presupuestado para la convocatoria
P: Patrimonio = Activo Total – Pasivo Total

NOTA: Para llevar a cabo este análisis, el proponente deberá diligenciar el formato Anexo No 4 Estado Financiero, a la presente convocatoria, el cual deberá suscribir el representante legal, el contador de la empresa y el revisor fiscal, para los años 2013 y 2014.

REVISIÓN TÉCNICA

Se revisará que la propuesta presentada cumpla con los requerimientos solicitados en el acápite de especificaciones técnicas, documentos que no serán subsanables ni en su contenido ni por su falta de presentación.

ASIGNACIÓN DE PUNTAJE

Se asignará el puntaje correspondiente a las propuestas que haya superado la revisión jurídica, técnica y financiera. Para tal efecto, se determinan los siguientes:

Factores de evaluación

En el valor de las propuestas se entenderá incluido el valor de impuestos y descuentos, el IVA deberá estar discriminado. La Universidad evaluará las propuestas con un puntaje máximo de **100** puntos de acuerdo con el siguiente factor:

Factor Económico (100 puntos)
Se asignarán 100 puntos a la propuesta que ofrezca el menor valor y proporcionalmente se asignarán los puntajes correspondientes a las demás ofertas. Se debe diligenciar el siguiente cuadro de valores.

ITEM	CANTIDAD	IVA	VALOR TOTAL
Equipos de Seguridad Perimetral	2		
Equipo de análisis	1		
Años de soporte y Actualización por parte del fabricante	3 años		
Servicio de Instalación, configuración, parametrización y puesta en funcionamiento	1		
TOTAL OFERTA			

Para el efecto se calculará así el puntaje de este factor:

$$Pts_i = \frac{Pts \times Min(V_1, V_2, .., V_n)}{V_i}$$, donde:

Pts_i es el puntaje que se asignará al proveedor i
Pts es el puntaje máximo asignado para el factor de evaluación.
$Min(V_1, V_2, ..., V_n)$ es el mínimo valor de precio de entre todos los proveedores.
V_i es el valor de precio del proveedor i.

FACTORES DE DESEMPATE

En caso de que se presente un empate entre dos o más propuestas en el puntaje obtenido se aplicará el siguiente criterio de desempate:

En caso de empate, se utilizará, como método aleatorio, un número de balotas igual al número de oferentes en empate marcadas con el nombre de cada uno de los proponentes, a fin de que, por azar, se escoja al ganador.

PRESUPUESTO

El contrato será cubierto con cargo al certificado de disponibilidad presupuestal No. 2371 del 30 de septiembre de 2015 y hasta por la suma de $204.250.000.

CAUSALES DE RECHAZO DE LAS PROPUESTAS

Son causales de rechazo de las propuestas:

1. Cotizar por un valor superior al presupuesto convocado
2. Incumplir con lo indicado en la parte de especificaciones técnicas de los bienes o servicios solicitados. En todos los ítems debe quedar que cumple.
3. Entregar la propuesta en día, horario y lugar diferente al señalado en el cronograma.
4. No aportar su propuesta económica
5. No aportar aquellos documentos que sean necesarios para los factores de evaluación

COMUNICACIÓN DEL RESULTADO DEL ESTUDIO TÉCNICO Y ECONÓMICO

Una vez realizado el respectivo análisis técnico y económico o el cuadro comparativo, se realizará la comunicación de los mismos al proponente, al correo electrónico respectivo, a su vez, el participante contará con un término de dos días hábiles para presentar objeciones y de ser así deberá ser manifestada vía correo electrónico a la dirección que para el efecto se determina en el ítem de comunicaciones.

ADJUDICACIÓN

La Universidad adjudicará el contrato al proponente que cumpla con las condiciones técnicas y se ajuste al presupuesto.

La Universidad se reserva el derecho de adjudicar parcialmente, ampliar plazos o declarar desierta esta convocatoria.

COMUNICACIONES

Las dudas y objeciones a la presente convocatoria serán recepcionadas en las oficinas respectivas y/o a través del correo electrónico **juntadecompras@ucaldas.edu.co**. No se atenderán llamadas ni visitas presenciales.

LEGALIZACIÓN

El oferente a quien se adjudique el contrato, dentro de los 5 días siguientes a su firma, deberá cumplir con los siguientes requisitos:

1. Cancelar lo correspondiente al 1% del valor del contrato antes de IVA por concepto de estampilla Pro-Universidades de Caldas y Nacional para lo cual con la firma del contrato el contratista autoriza a la Universidad a descontar del primer pago lo correspondiente al valor de la estampilla.

2. Constituir pólizas que garanticen:
   Cumplimiento del contrato por el equivalente al 20% del valor total, vigente durante su ejecución y 2 meses más.
   Calidad y correcto funcionamiento del bien equivalente al 50% del valor total del contrato, vigente durante su ejecución y un año más.

3. Afiliación al sistema de Pensiones y Salud. Deberá aportar la certificación del Gerente o Revisor Fiscal, donde certifique que se encuentran a paz y salvo en el pago seguridad social y parafiscales de sus empleados.

Todos los gastos que demande la legalización del contrato corren por cuenta del contratista.

FORMA DE PAGO

Se realizará un solo pago al proveedor dentro de los 15 días hábiles siguientes a la presentación de la documentación: Certificado de pago de la actualización del sistema de seguridad por 3 años, el certificado de aportes a seguridad social y parafiscales, el recibido a satisfacción del supervisor y la factura o cuenta de cobro.

No se aceptarán solicitudes de pago de anticipos, ni aquellas que involucren el valor de los servicios de transporte.

RÉGIMEN CONTRACTUAL APLICABLE

En los términos de la Ley 30 de 1992, la Universidad de Caldas se sujetará en la presente Contratación al Acuerdo 03 de 2009, y sus modificaciones, emanadas del Consejo Superior de la Universidad de Caldas.

ENTREGA DE PROPUESTAS

Para efectos de hora de cierre de la convocatoria, se tomará como referencia la hora oficial señalada en la página Web de la Superintendencia de Industria y Comercio. No podrá participar en la presente convocatoria, quien llegue posterior a la fecha y hora de cierre o radique su oferta en lugar diferente al señalado

La propuesta será presentada o enviada antes de la fecha y hora indicada en sobre cerrado indicando en su exterior el número de la presente convocatoria a la CALLE 65 No 26-10 UNIVERSIDAD DE CALDAS, SEDE PRINCIPAL, OFICINA DE CONTRATACIÓN.

Agradece su participación,

FELIPE CÉSAR LONDOÑO LÓPEZ
Rector

Elaboró: Luz Miryam Orozco
Revisó: Sebastián Gutiérrez
Aprobó: Diana C. Zuluaga.

ANEXO 1
CARTA DE PRESENTACIÓN DE LA OFERTA

Lugar: _____, fecha: _____

Señores
UNIVERSIDAD DE CALDAS

REF: Invitación a cotizar

El suscrito _____, actuando en calidad de _____ de la empresa _____, habiendo examinado cuidadosamente la oferta de la referencia y recibidas las aclaraciones solicitadas, presento oferta para el proceso de la referencia, de acuerdo con las especificaciones técnicas y las condiciones comerciales y contractuales que se detallan en la misma.

De ser aceptada la oferta nos comprometemos a presentar la documentación requerida, dentro del tiempo establecido para ello en la invitación a cotizar.

Ejecutaremos el contrato por los precios y plazos señalados en nuestra oferta, en las condiciones contractuales y técnicas exigidas en los documentos de la contratación y previstos por las normas que rigen la contratación con la Universidad de Caldas y de conformidad con la aceptación de nuestra oferta.

Mantendremos válida nuestra oferta durante sesenta (60) días calendario, contados desde la fecha de cierre del proceso de contratación, contados a partir de la fecha de cierre.

Finalmente declaro que la información contenida en nuestra oferta es exacta y veraz y que aportaremos las pruebas que la Universidad de Caldas considere necesarias para verificar su exactitud.

Atentamente,

_____
Firma
Representante legal: _____
Cédula de Ciudadanía: _____ de _____
Razón o denominación social de la firma Proponente: _____
NIT: _____
Dirección del Proponente: _____
Ciudad: _____
Teléfono (s): _____ Fax: _____
E-mail: _____
Régimen al que pertenecen: _____

ANEXO 2
DECLARACIÓN DE NO INHABILIDAD Y COMPROMISO ÉTICO

Lugar_____, fecha_____

Señores
UNIVERSIDAD DE CALDAS

REF: Invitación a cotizar

El suscrito_____, obrando en nombre y representación legal de la empresa _____, legalmente constituida, tal como consta en el certificado de existencia y representación, se permite manifestar que el representante legal, los socios, su junta directiva y la sociedad oferente, no están incursos en causales de inhabilidad e incompatibilidad consagradas en las leyes Colombianas, que impidan su participación en el proceso contractual y en la celebración del respectivo contrato y en caso de sobrevenir alguna de ellas, cederemos el contrato previa autorización escrita de LA UNIVERSIDAD o se dará por terminado el mismo.

En consonancia con lo anterior, dejo especial constancia que actualmente SI ___ NO ___ soy servidor público y que SI ___ NO ___ tengo vínculos de parentesco, hasta el segundo grado de consanguinidad, segundo de afinidad o primero civil con los servidores públicos de los niveles directivo, asesor ejecutivo o con los miembros de la junta o consejo directivo, o con las personas que ejerzan el control interno o fiscal de la Universidad de Caldas.

La anterior manifestación se entiende hecha bajo la gravedad de juramento (Art. 25 de Ley 962 de 2005)*

Igualmente me permito manifestar que me comprometo a actuar con rectitud, idoneidad, responsabilidad, respeto y eficiencia, ha exigir de mi personal igual condición y a no desarrollar ninguna conducta que atente contra los reglamentos universitarios y principios de la contratación estatal.

Se suscribe el presente compromiso como acuerdo real, garantizando actuar dentro del marco de la ética, la moral, transparencia y objetividad en nuestras actuaciones.

_____
Firma
Representante legal: _____
Cédula de Ciudadanía: _____ de _____

*Al efecto se hace saber que quien falte a la verdad en forma total o parcial, incurrirá en sanciones conforme dispone nuestro ordenamiento penal.

ANEXO 3

CARTA DE PRESENTACIÓN DE ESPECIFICACIONES TÉCNICAS

Lugar: _____, fecha: _____

Señores
UNIVERSIDAD DE CALDAS

REF: Invitación a cotizar.

El suscrito_____, obrando en nombre y representación legal de la empresa _____, legalmente constituida, tal como consta en el certificado de existencia y representación, se permite enunciar las especificaciones técnicas a cumplir en la ejecución del contrato que resulte de la presente invitación:

Funcionalidades y características del Sistema:

Para la configuración y parametrización de los requerimientos y necesidades, se debe proveer los siguientes equipos y servicios:

ÍTEM	CANTIDAD
Equipos de Seguridad Perimetral.	2
Equipo de análisis.	1
Años de soporte y Actualización por parte del fabricante.	3 años
Servicio de instalación, configuración, parametrización y puesta en funcionamiento.	1

Características del dispositivo:

1. El dispositivo debe ser un equipo de propósito específico.
2. Basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.
3. Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).
4. Capacidad de re-ensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).
5. El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red.

6. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
7. El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.
8. El equipo de seguridad debe soportar el uso del protocolo ICAP con el fin de poder delegar tareas a equipos terceros con el fin de liberar procesamiento del mismo.

A continuación se establecen los requerimientos de los servicios y funcionalidades que debe de cumplir la plataforma; responder cumple o no cumple y adjuntar documentos que evidencien la respuesta:

Firewall: Para esta amenaza y/o el aspecto de seguridad anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs		
Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.		
Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.		
Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando		
Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.		

Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo.		
Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)		
Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.		
Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)		
Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.		
Capacidad de hacer traslación de direceiones dinámico, muchos a uno, PAT.		
Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario),		
La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.		
En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID		
En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.		

El equipo deberá permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios o identificador de dispositivos para el caso de dispositivos móviles como smartphones y tabletas.		
El equipo deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN		
La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.		
La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada		
La solución será capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente		
El dispositivo de seguridad podrá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas		
La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo		
La solución podrá crear e implementar políticas de tipo Multicast y determinar el sentido de la política, así como también la habilitación del NAT dentro de cada interface del dispositivo		
El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces.		

El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS		
La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o especifica		
La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.		
El dispositivo integrara la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados		
El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico		
Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis		
La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH		

Conectividad y Sistema de ruteo: Para esta amenaza y/o el aspecto de seguridad se debe anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (*Relay*) de solicitudes DHCP.		
Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.		
Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.		

Soporte a políticas de ruteo (policy routing).		
El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace		
Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS		
Soporte a ruteo dinámico RIPng, OSPFv3		
La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.		
Soporte de ECMP (Equal Cost Multi-Path)		
Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.		
Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.		
Soporte a ruteo de multicast		
La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.		
La solución podrá habilitar políticas de ruteo en IPv6		
La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6		
La solución deberá soportar la creación de políticas de tipo Firewall y VPN y subtipo por dirección IP, tipos de dispositivo y por usuario, con IPv6		
La solución será capaz de habilitar funcionalidades de UTM (Antivirus, Filtrado Web, Control de Aplicaciones, IPS,Filtrado de correo, DLP, ICAP y VoIP) dentro de las políticas creadas		

con direccionamiento IPv6		
El dispositivo debe integrar la autenticación por usuario o dispositivo en IPv6		
El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explicito		
Deberá ser capaz de integrar políticas con proxy explicito en IPv6		
La solución podrá restringir direcciones IPv6 en modo proxy explicito		
Deberá hacer NAT de la red en IPv6		
La solución será capaz de comunicar direccionamiento IPv6 a servicios con IPv4 a través de NAT		
Como dispositivo de seguridad deberá soportar la inspección de tráfico IPv6 basada en flujo		
La solución deberá ser capaz de habilitar políticas de seguridad con funcionalidades IPS, Filtrado Web, Control de Aplicaciones, Antivirus y DLP, para la inspección de tráfico en IPv6 basado en flujos		
La solución contara con una base de administración de información interna generada por sesiones sobre IPv6		
Deberá ser capaz de habilitar la funcionalidad de Traffic Shaper por IP dentro de las políticas creadas en IPv6		
El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6		
La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface		

La solución deberá contar con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad		
El dispositivo podrá ser configurado mediante DHCP en IPv6 para comunicarse con un servidor TFTP donde se encontrara el archivo de configuración		
El dispositivo podrá hacer la función como servidor DHCP IPv6		
La solución será capaz de configurar la autenticación por usuario por interface en IPv6		

VPN IPSec/L2TP/PPTP: Para esta amenaza y/o el aspecto de seguridad se debe anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)		
Soporte para IKEv2 y IKE Configuration Method		
Debe soportar la configuración de túneles PPTP		
Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.		
Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits		
Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.		
Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.		
Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.		

La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN)		
En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.		
Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.		

VPN SSL: Para esta amenaza y/o el aspecto de seguridad se debe anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
Capacidad de realizar SSL VPNs.		
Soporte a certificados PKI X.509 para construcción de VPNs SSL.		
Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.		
Soporte de renovación de contraseñas para LDAP y RADIUS.		
Soporte a asignación de aplicaciones permitidas por grupo de usuarios		
Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.		
Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.		
Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)		

La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS		
Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL		
Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente		
Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.		
Los portales personalizados deberán soportar al menos la definición de: Widgets a mostrar Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC Esquema de colores Soporte para Escritorio Virtual Política de verificación de la estación de trabajo		
La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.		
Para la configuración de clúster, en caso de caída de uno de los dispositivos, la VPN SSL que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente.		

Traffic Shapping / QoS: Para esta amenaza y/o el aspecto de seguridad se debe anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO

		CUMPLE
Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall		
Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión		
Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.		
Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo		
Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo		
Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia		

Autenticación y Certificación Digital: Para esta amenaza y/o el aspecto de seguridad se debe anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
Capacidad de integrarse con Servidores de Autenticación RADIUS.		
Capacidad nativa de integrarse con directorios LDAP		
Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On"		

Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.		
Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.		
Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)		
La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.		
Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.		
Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo: Longitud mínima permitida Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc. Expiración de contraseña.		
Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.		

Antivirus: Para esta amenaza y/o el aspecto de seguridad se debe anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.		

El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruídos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.		
Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.		
El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.		
La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso.		
El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.		
El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos.		
El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos http, FTP, IMAP, POP3, SMTP		
El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.		
El Antivirus deberá incluír capacidades de detección y detención de tráfico spyware, adware y otros tipos de		

malware/grayware que pudieran circular por la red.		
El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger.		
El antivirus deberá ser capaz de filtrar archivos por extensión		
El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo		
Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)		

AntiSpam: Para esta amenaza y/o el aspecto de seguridad anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
La capacidad antispam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.		
La capacidad AntiSpam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).		

La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM		
En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.		

Filtraje de URLs (URL Filtering): Para esta amenaza y/o el aspecto de seguridad se debe anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.		
Debe poder categorizar contenido Web requerido mediante IPv6.		
Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.		
Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso.		
Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión		

siendo establecida		
La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo).		
Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Estos mensajes de remplazo deberán poder aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo.		
Los mensajes de remplazo deben poder ser personalizados por categoría de filtrado de contenido.		
Capacidad de filtrado de scripts en páginas web (JAVA/Active X).		
La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Bùsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing.		
Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.		
Será posible exceptuar la inspección de HTTPS por categoría.		
Debe contar con la capacidad de implementar el filtro de Educacion de Youtube por Perfil de Filtro de Contenido para trafico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido de tipo Educativo en Youtube, bloqueando cualquier tipo de contenido		

no Educativo.		
El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección:		
Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa.		
Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad.		
Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado.		
Se debe incluir la funcionalidad de reputación basada en filtrado de URLs.		
La funcionalidad de reputación busca que, al acceder a páginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc.) se asigne un puntaje a cada usuario o IP cada vez visita una página de esta índole. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red.		
El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.		
Se debe incorporar la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter)		
En dicho sistema cada organismo obtiene un ID de Youtube para habilitar el contenido educativo del mismo. Se deberá insertar dicho código en la configuración de filtrado de URLs del equipo para poder habilitar únicamente el contenido educativo de Youtube.		

Protección contra intrusos (IPS): Para esta amenaza y/o el aspecto de seguridad se debe anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.		
Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.		
Capacidad de detección de más de 4000 ataques.		
Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)		
El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.		
El detector y preventor de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection).		
Basado en análisis de firmas en el flujo de datos en la red, y		

deberá permitir configurar firmas nuevas para cualquier protocolo.		
Actualización automática de firmas para el detector de intrusos		
El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.		
Métodos de notificación: Alarmas mostradas en la consola de administración del appliance. Alertas vía correo electrónico. Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado. La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto. Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP		
Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir: 1. Protección contra botnets: Se deben bloquear intentos de conexión a servidores de Botnets, para ello se debe contar con una lista de los servidores de Botnet más utilizado. Dicha lista debe actualizarse de forma periodica por el fabricante. 2. Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una accion sobre el mismo.		

Prevención de Fuga de Información (DLP): Para esta amenaza y/o el aspecto de seguridad se debe anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.		
La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.		
Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.		
Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento,		
En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.		
La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo.		
La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.		

Se debe proveer la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se debe considerar como mínimo las siguientes: 1. Filtrado por tipo de archivo 2. Filtrado por nombre de archivo 3. Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos. 4. Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra. 5. Watermarking: Se insertará un "sello de agua" dentro del archivo considerado como confidencial. De acuerdo a esto se analizarán los archivos en busca de este sello de agua, este se detectará incluso si el archivo sufrió cambios.		

Control de Aplicaciones: Para esta amenaza y/o el aspecto de seguridad se debe anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.		
La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.		
Las solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.		
El listado de aplicaciones debe actualizarse periódicamente.		
Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.		
Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.		

Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.		
Preferentemente deben soportar mayor granularidad en las acciones.		

Inspección de Contenido SSL: Para esta amenaza y/o el aspecto de seguridad anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.		
La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).		
La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.		
Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.		
El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS		

Controlador Inalámbrico (Wireless Controller): Para esta amenaza y/o el aspecto de seguridad anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE

El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless		
En modo de Controlador de Wireless tendrá la capacidad de configurar múltiples puntos de acceso (Access Points: APs) reales de forma tal de que se comporten como uno solo. Cómo mínimo deberá controlar los SSID, roaming entre APs, configuraciones de cifrado, configuraciones de autenticación.		
Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection.		
El controlador de Wireless tendrá la capacidad de configurar la asignación de direcciones IP mediante DHCP a las estaciones de trabajo conectadas a los APs.		
Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs.		
La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el trafico wireless para detectar y reportar posibles intentos de intrusión.		
Debe contar con un sistema de aprovisionamiento de usuarios invitados para red wifi, que permita la creación sencilla de accesos para invitados, por medio de un portal independiente.		
El equipo debe tener capacidad de que estos usuarios invitados con acceso inalámbrico, tengan la opción de colocar o no contraseña, con tiempo limitado y configurable para la expiración de la cuenta.		
El controlador inalámbrico debe estar en la capacidad de balancear la carga entre los puntos de acceso (Access Points) soportando por lo menos los siguientes métodos de balanceo: Access Point Hand-off, Frequency Hand-off.		
Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma rubred.		

El dispositivo deberá ser capaz de administrar los dispositivos wireless AP de la misma plataforma, tanto en consola CLI como a través de una interfaz grafica (GUI)		
El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota.		
El dispositivo debe poder cifrar la información que se envía hacia los puntos de acceso de la misma plataforma, sobre los cuales se esté teniendo control y gestión.		
El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricos dentro del mismo segmento de red.		
El equipo debe tener la capacidad de reconocer y monitorear diferentes tipos de dispositivos de comunicación móvil como Smartphones Androide, Blackberry y Iphone; diferentes tipos de consolas de juego como Xbox, PS2, PS3, Wii, PSP; diferentes tipos de tabletas con SO Androide o tabletas Ipad,		
El equipo debe tener la capacidad de controlar el acceso a la red de los diferentes dispositivos antes mencionados a través de ACLs por MAC		
El equipo deberá permitir el crear diferentes niveles de acceso a la red en función del tipo de dispositivo que se conecte, siendo estos: Smartphones, Tabletas, Laptoos, PCs (tanto en Windows como en Linux)		
El equipo debe permitir la separación de redes al menos entre usuarios internos e invitados, permitiendo la colocación de reglas en función de los dispositivos móviles conectados.		

Filtraje de tráfico VoIP, *Peer-to-Peer* y Mensajería instantánea: Para esta amenaza y/o el aspecto de seguridad anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE

Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).		
El dispositivo deberá técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella, KaZaa, Skype y WinNY para Peer-to-peer.		
En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual.		
La solución debe contar con un ALG (Application Layer Gateway) de SIP		
Debe poder hacerse inspección de encabezados de SIP		
Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP.		
La solución debe soportar SIP HNT (Hosted NAT Transversal).		
La solución deberá integrar la inspección de tráfico basado en flujo utilizando un motor de IPS dentro del mismo dispositivo para escaneo de paquetes		
Deberá ser capaz de hacer inspección tráifco SSH en modo proxy explicito		
La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explicito con las funcionalidades de IPS, Antivirus, Filtrado Web, Control de Aplicaciones y DLP, todo en un mismo dispositivo		
El dispositivo tendrá la opción para configurar sus interfaces integradas en modo Sniffer con funcionalidades de Filtrado Web, Control de Aplicaciones, Antivirus e IPS		

Optimización WAN y Web Caching: Para esta amenaza y/o el aspecto de seguridad anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
La solución deberá permitir la creación de perfiles para la aplicación de Optimización WAN e indicar bajo que protocolos se ejecutara		
Deberá ser capaz de activar en modo transparente dentro de los perfiles de Optimización WAN y seleccionar un determinado grupo de usuarios para autenticación de acceso		
El dispositivo deberá soportar la desfragmentación dinámica de paquetes para detectar fragmentos persistentes de distintos archivos o datos adjuntos dentro del trafico bajo protocolos desconocidos		
La solución debe ser capaz de generar y aplicar perfiles de Optimización WAN para los usuarios		
El dispositivo de seguridad podrá integrar contenido de inspección dentro de sus políticas de seguridad con Optimización WAN		
La solución integrara dentro de cada interface la capacidad de hacer túneles de Optimización WAN		
Deberá ser capaz de configurar Optimización WAN en modo Activo/Pasivo		
Solución capaz de aplicar web cache a tráfico HTTP y HTTPS dentro de las políticas de seguridad incluyendo también Optimización WAN y web proxy cache		
Dispositivo capaz de habilitar el almacenamiento en caché web tanto en el lado del cliente y del lado de la solución		
La solución podrá recibir el tráfico HTTPS en nombre del cliente, abrirá y extraerá el contenido del tráfico cifrado para inspeccionar y almacenar en cache para el envío al usuario final		

El dispositivo tendrá la opción de integrar un certificado SSL determinado para la recifrado de tráfico		
La solución capaz de configurar el cache de trafico HTTP y HTTPS bajo distintos puertos a los predeterminados (80 y 443)		
La solución debe ser capaz de habilitar opciones para depurar la funcionalidad de Web Cache a determinadas URL		

Alta Disponibilidad: Para esta amenaza y/o el aspecto de seguridad anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6		
Alta Disponibilidad en modo Activo-Pasivo		
Alta Disponibilidad en modo Activo-Activo		
Posibilidad de definir al menos dos interfaces para sincronía		
El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red		
Será posible definir interfaces de gestión independientes para cada miembro en un clúster.		

Características de Administración: Para esta amenaza y/o el aspecto de seguridad anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE

Interfase gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfase debe soportar SSL sobre HTTP (HTTPS)		
La interfase gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario.		
Interfase basada en línea de comando (CLI) para administración de la solución.		
Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.		
Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet)		
El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales.		
Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.		
El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS.		
El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.		
Soporte de SNMP versión 2		

Soporte de SNMP versión 3		
Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos		
Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL.		
Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.		
Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.		
Debe ser posihle definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.		
Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.		
Contar con facilidades de administración a través de la interfaz grafica como listas de edición a través de click derecho.		
Contar con facilidades de administración a través de la interfaz grafica como ayudantes de configuración (setup wizard).		
Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa.		

Contar con herramientas graficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.		

Virtualización - Para esta amenaza y/o el aspecto de seguridad anexar certificación del fabricante.

DESCRIPCIÓN	CUMPLE	NO CUMPLE
El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains"		
La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus		
Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer.		
Cada instancia virtual debe poder tener un administrador independiente		
La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.		
Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red		
Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual		
Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.		
Debe ser posible definir y modificar los mensajes mostrados por el		

dispositivo de forma independiente para cada instancia virtual.		
Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente.		

Análisis de seguridad y almacenamiento de Logs:

1. La solución de seguridad debe contar con un equipo de propósito específico appliance que permita la centralización de reportes, análisis de tráfico, almacenamiento de logs, generación de reportes gerenciales del tráfico que fluye a través ***del dispositivo sistema de seguridad informática perimetral o de borde*** incluidos en dichos reportes de funcionalidades como: Web Filter, AntiSpam, Antivirus, IPS, Control de Aplicaciones, DLP, Eventos, Autenticación, VPN, entre otros.

2. Para la implementación de buenas prácticas de este sistema de administración de logs se requiere que el sistema de gestión de eventos cuente con la opción de selección de niveles de logs (0 – Emergency, 1 - Alert, 2- Critical, 3- Error, 4 – Warning , 5- Notification, 6 – Information) para evitar siempres guardar logs en el disco que sean muy frecuentes por un periodo de tiempo largo que causa un desgaste excesivo en el disco duro y puede causar fallas prematuras también que se pueda escoger la opción de Overwrite Oldest Logs para que si se llena el disco, sobrescriba los archivos de logs.

3. Permitir Monitoreo y alertas en tiempo real que permita descubrir y resolver las vulnerabilidades que se manifiestan entre el sistema de seguridad perimetral o de borde. el esfuerzo requerido para monitorear y mantener políticas de uso aceptables, identifica Patrones de ataque y descubrir a los atacantes, y así poder estar dentro de regulaciones gubernamentales en cuanto a la privacidad y confidencialidad de los recursos informáticos.

4. Este sistema de gestión de eventos también debe proveer funciones de administración de seguridad avanzadas como archivos de cuarentena, correlación de eventos, análisis de vulnerabilidades, análisis de tráfico y archivo de contenido que permita controlar en tiempo real con diferentes mecanismos de alertas los problemas potenciales.

5. El sistema de gestión de eventos debe poder manejar las Alertas Correlacionadas: Correlación de alertas manejada por plantillas, permite la creación y definición de

cualquier número de reglas y alertas que reduzcan falsos positivos, identifiquen ataques combinados y brechas en la seguridad o anomalías y patrones de identidad

6. Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis.

GESTIÓN Y ANÁLISIS:

1. Simplificación de la administración centralizada de logs.
2. Tráfico y visibilidad de aplicaciones.
3. Asegurar el registro organizado de retención.
4. Monitoreo en tiempo real y alertas.
5. Personalizada y preconfiguradas presentaciones de informes.
6. Análisis de tráfico.
7. Copia de seguridad consistente y actualizaciones.

CARACTERÍSTICAS CLAVES

Tablero de control: Sistema y registro de widgets, además de monitores en tiempo real le permiten ver exactamente lo que está pasando dentro de tu red en cualquier momento.

Visor de registro: Visualización de registros en tiempo real con los filtros en cualquier asunto potencial o evento sospechoso.

Análisis de usuario: Profundizar y analizar la actividad de red para una visibilidad granular de la actividad.

Generador de informes: Creación de informes en diferentes formatos, incluyendo PDF a medir política de cumplimiento o ilustrar los patrones de uso de la red.

Actualizaciones de plataforma

DESCRIPCIÓN	CUMPLE	NO CUMPLE
La solución contara con el servicio de actualización de firmas para dispositivos sobre BYOD		
El dispositivo tendrá la opción de conectarse a los servidores NTP de los Laboratorios de Investigación y Actualización propietarios del mismo fabricante para actualización del horario		

de sistema local		
Sera capaz de hacer consultas a los servidores DNS de los Laboratorios de Investigación y Actualización del mismo fabricante para resolución y categorización de sitios web dentro de los perfiles para Filtrado Web		
Tendrá la capacidad de hacer consultas a los servidores DNS de los Laboratorios de investigación y Actualización mismos del fabricante sobre reputación de direcciones IP		

Lieenciamiento y actualizaciones

*** Tamaño de licencia**

El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.

*** Vigencia de licencia de actualización**

La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos 3 años.

Desempeño / Conectividad THROUGHPUT MINIMO Y OTRAS ESPECIFICACIONES QUE DEBE SATISFACER LA SOLUCION OFERTADA.

Los equipos deben por lo menos ofrecer las siguientes características de desempeño y conectividad:

PERFORMANCE Y CAPACIDAD	MÍNIMO SOLICITADO	OFRECIDO
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	45 / 45 / 23 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	45 / 45 / 23 Gbps	
Firewall Latency (64 byte, UDP)	2 µs	
Firewall Throughput (Packet per Second)	39.5 Mpps	

Concurrent Sessions (TCP)	10 Million	
New Sessions/Second (TCP)	250000	
Firewall Policies	80000	
IPsec VPN Throughput (512 byte)	20 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	1500	
Client-to-Gateway IPsec VPN Tunnels	8000	
SSL-VPN Throughput	2.6 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum)	9000	
IPS Throughput	6 Gbps	
Antivirus Throughput	2.5 Gbps	
CAPWAP Clear-text Throughput (HTTP)	7 Gbps	
Virtual Domains (Default / Maximum)	10	
Maximum Number of APs (Total / Tunnel)	1000 / 450	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

Solución almacenamiento y gestion de logs

PERFORMANCE Y CAPACIDAD	MINIMO SOLICITADO	OFRECIDO
GB/Day of Logs	10	
Sustained Log Rate (Standalone Mode)	150	
Peak Log Rate (Standalone Mode)*	600	
Devices/VDOMs/ADOMs (Maximum)	150	

Total Interfaces	4x GE	
Storage Capacity	4 TB (2x 2 TB)	
RAID Levels Supported	RAID 0/1	
Safety Certifications Se deberá acreditar un flujo de caja operativo positivo en los últimos seis (6) meses (mes a mes) del año 2014	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	

MIGRACIÓN DESDE LOS FIREWALL 620B EXISTENTE AL NUEVO FIREWALL.

El proponente al que finalmente se le adjudique el contrato de suministro e instalación de la solución de infraestructura y de seguridad perimetral, deberá realizar la migración de todo lo implementado hasta la fecha, en el firewall Fortinet 620B existente, como son políticas, reglas, filtros, Nat's, Pat's, VPN'S IPsec, SSL Apertura y cierre de puertos, permisos, usuarios, etc., garantizando el desempeño óptimo y de acuerdo a lo ofertado.

El equipo 620 se debe instalar y configurar con la funcionalidad de Firewall en la granja de servidores e integrarse con el nuevo equipo a adquirir.

Dicha migración, deberá ser transparente para todos los usuarios, internos y externos de nuestra plataforma de red, en este sentido, el proponente seleccionado deberá presentar un plan de migración para ejecutar en 45 días hábiles, para que éste se lleve a cabo sin ningún tipo de traumatismos que deterioren el desempeño del tráfico de información de nuestra red.

Atentamente,

_____

Representante Legal

ANEXO No 4

INVITACION A COTIZAR No _____- 2015

FORMULARIO ESTADO FINANCIERO

RAZÓN SOCIAL: _____

NIT O C.C: _____

FECHA DE CORTE 31 DE DICIEMBRE DE 201___

ACTIVO		**PASIVO**	
ACTIVO CORRIENTE (AC)		PASIVO CORRIENTE (PC)	
PROPIEDAD PLANTA Y EQUIPO		PASIVO MEDIANO Y LARGO PLAZO (PM)	
OTROS ACTIVOS			
ACTIVO TOTAL (AT)		**PASIVO TOTAL (PT)**	
		PATRIMONIO (P)	
		TOTAL PASIVO MAS PATRIMONIO	
TOTAL INGRESOS		**TOTAL GASTOS**	
UTILIDAD ANTES DE IMPUESTOS		UTILIDAD NETA	

RAZONES FINANCIERAS

CAPITAL DE TRABAJO (CT) AC - PC =	
NIVEL DE ENDEUDAMIENTO (E) PT / AT =	
* RELACIÓN PATRIMONIAL (RP)	

_____
REPRESENTANTE LEGAL
C.C.

NOMBRE:

_____
FIRMA CONTADOR
C.C.
T.P.
NOMBRE:

FIRMA REVISOR FISCAL
NOMBRE:
T.P. N°

NOTAS

* La relación patrimonial es igual a la razón entre el Valor Total de la Propuesta Económica y el Patrimonio (P)

- La Universidad de Caldas se reserva el derecho de confirmar los datos suministrados por los proponentes.
- Toda la información deberá presentarse en pesos colombianos.