

## CONCURSO DE PRECIOS N°04/2019

### PLIEGO DE BASES Y CONDICIONES GENERALES

**1. Normativa aplicable.** Para la presente contratación, rigen las disposiciones contenidas en el Pliego de Condiciones Generales, y en el REGLAMENTO PARA LA CONTRATACIÓN DE BIENES, OBRAS Y SERVICIOS aprobado por la COMISIÓN ARBITRAL DEL CONVENIO MULTILATERAL 18.08.77, vigente al momento de inicio del procedimiento de contratación.

**2. Objeto.** La presente contratación tiene por objeto la Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral, según el Anexo "A" Especificaciones Técnicas, que se adjunta al presente Pliego.

**3. Lugares y Plazos.** Tanto la recepción de las ofertas como el acto de apertura de los sobres se realizara en la sede de la Comisión Arbitral, departamento de Recursos Humanos y Materiales, sito en Esmeralda 672 piso 3°, Ciudad Autónoma de Buenos Aires.

La recepción de las ofertas será hasta las 11:00 hs del día 4 de junio de 2019.

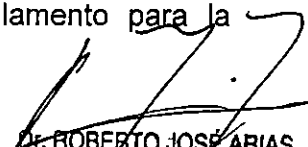
La apertura de las ofertas se realizara a las 11:30 hs del día 4 de junio de 2019.

**4. Requisitos formales para la presentación de las ofertas.** Las ofertas deberán cumplir los siguientes requisitos formales:

- a. Redactadas en idioma nacional en procesador de texto y/o a máquina, en formularios con membrete de la persona o firma comercial.
- b. Firmadas en todas sus hojas por el oferente, representante legal o apoderado debidamente acreditado.
- c. Enmiendas y raspaduras en partes esenciales, debidamente salvadas.
- d. Todas las fojas (incluida la documentación y folletería que se acompañe) debidamente compaginadas, numeradas y abrochadas o encarpetadas.
- e. Por duplicado y presentadas en sobre o paquete cerrado con indicación de número de contratación, fecha y hora de apertura.
- f. Tanto las ofertas como los presupuestos, facturas y remitos, deberán cumplir con las normas impositivas y previsionales vigentes.

Las infracciones, errores u omisiones no esenciales no invalidarán la oferta, sin perjuicio de las sanciones que pudiesen corresponder al infractor.

**5. Información y documentación que deberá presentarse junto con la Oferta.** Se estará a lo dispuesto por el art. 19 del Reglamento para la

  
Dr. ROBERTO JOSÉ ARIAS  
PRESIDENTE

contratación de bienes, obras y servicios de la Comisión Arbitral. A tal efecto, en el momento de presentar la oferta, se deberá proporcionar la información que en cada caso se indica. En todos los casos deberá acompañarse la documentación respaldatoria y las copias de escrituras, actas, poderes y similares deberán estar autenticadas por Escribano Público:

**a. Personas humanas y apoderados:**

1-Nombre completo, nacionalidad, profesión, domicilio real y constituido, tipo y número de documento de identidad.

2-Clave Única de Identificación Tributaria (C.U.I.T) y condición frente al Impuesto al Valor Agregado (IVA) y Regímenes de Retención vigentes.

**b. Personas jurídicas:**

1-Razón Social, domicilio legal y constituido, lugar y fecha de constitución y datos de inscripción registral.

2-Clave Única de Identificación Tributaria (C.U.I.T) y condición frente al Impuesto al Valor Agregado (IVA) y Regímenes de Retención vigentes

**c. En todos los casos, con la oferta deberá acompañarse:**

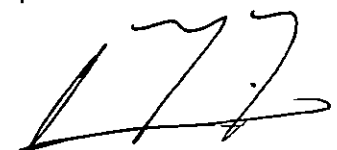
1-Copia autenticada del poder, en caso de que quien suscriba la oferta y el resto o parte de la documentación no sea la persona humana o el representante legal respectivo.

2-Declaración Jurada de que ni el oferente, ni los integrantes de los órganos de administración y fiscalización en su caso, se encuentran incurso en ninguna de las causales de inhabilidad para contratar con la Comisión Arbitral.

3-Certificado de inscripción en AFIP, donde se acredite la actividad que desarrolla y cuando corresponda, certificación de condición como "Agente de Retención" y/o certificado de exclusión de retención (Impuesto al valor Agregado, Impuesto a las Ganancias, Sistema Único de Seguridad Social -SUSS-).

4-Constancia de inscripción en el Impuesto a los Ingresos Brutos.

**6. Contenido de la oferta.** La presentación de las ofertas deberán contemplar la totalidad de los puntos solicitados bastando la falta de alguno de estos para que se desestime la oferta general. La presentación de la oferta significará de parte del oferente el pleno conocimiento del Reglamento de Contrataciones de Bienes, Obras y Servicios de la Comisión Arbitral y la aceptación de las cláusulas que rigen la contratación.



Dr. ROBERTO JOSÉ ARIAS  
PRESIDENTE

La oferta especificará por cada ítem en relación a la unidad solicitada o su equivalente: precio unitario, precio total; en pesos, con I.V.A. Incluido. El total general de la propuesta será expresado en letras y números con I.V.A. Incluido.

**7. Plazo de mantenimiento de la Oferta.** El plazo de mantenimiento de la oferta será de siete (7) días, en un todo de acuerdo a lo reglado por el art. 23 del Reglamento para la Contratación de Bienes, Obras y Servicios de la Comisión Arbitral.

**8. Efectos de la presentación de la oferta.** La presentación de la oferta, importa de parte del oferente el pleno conocimiento de toda la normativa que rige el llamado a contratación, la evaluación de todas las circunstancias, la previsión de sus consecuencias y la aceptación en su totalidad de las bases y condiciones estipuladas, sin que pueda alegar en adelante el oferente su desconocimiento.

**9. Análisis de las Ofertas.** Las ofertas serán evaluadas por un Comité de Preadjudicación, cuyos integrantes serán designados por el contratante, quienes emitirán el informe de evaluación de las ofertas.

**10. Adjudicación.** Se adjudicará el Concurso de Precios al oferente cuya propuesta se ajuste a lo establecido en el Pliego de Bases y Condiciones Generales, sea satisfactoria la documentación presentada y su oferta económica haya sido evaluada como la más conveniente. Dicha adjudicación se efectuara por monto global.

**11. Plazo de entrega.** El plazo de entrega será de 60 (sesenta) días, contados a partir de la fecha de recepción de la orden de compra.

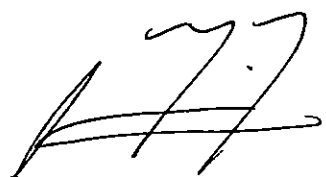
**12. Pagos.** El pago se efectuará con cheque oficial al día, de Banco Nación Argentina Sucursal Plaza de Mayo, contra entrega de la totalidad de los ítems.

**13. Penalidades y Sanciones.** Será de aplicación lo dispuesto por el Capítulo XII del Reglamento para la Contratación de Bienes, Obras y Servicios de la Comisión Arbitral.

**14. Impuesto al Valor Agregado.** A los efectos de la aplicación del Impuesto al Valor Agregado, la Comisión Arbitral reviste el carácter de consumidor final.

**15. Constitución de domicilio.** A todos los efectos legales, el oferente deberá constituir domicilio legal en la Ciudad Autónoma de Buenos Aires.

**16. Garantía.** Soporte y Licencias por 1 (un) año.

  
Dr. ROBERTO JOSÉ ARIAS  
PRESIDENTE

## **ANEXO “A” – Concurso del Precios 04/2019**

### **Especificaciones Técnicas**

**Detalles del Proyecto:** Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral que incluye filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware “Zero Day”, bien como controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta. Además se deberá complementar con un sistema de almacenamiento de Logs y Reportes. Por lo tanto, se requiere que la solución brinde una gestión simple, eficiente y permita la integración con la infraestructura existente.

#### **Componentes de la solución:**

<b>Cantidad</b>	<b>Detalle</b>
<b>2</b>	Next Generation Firewall (NGFW) – Hardware Appliance
<b>1</b>	Sistema de Logs y Reportes Unificado

#### **Objeto 1: Next Generation Firewall**

Sistema de seguridad perimetral (“Firewall”) de tipo NGFW que deberá brindar ya incluidas y listas para ser utilizadas las funcionalidades de UTM o Unified Threat Management. Adicionalmente, debe contar con las siguientes funcionalidades detalladas a continuación:

##### **1. Generales**

- 1.1. La solución estará compuesta por Hardware y Software del mismo fabricante integrados en un Appliance de misión específica. No se aceptarán soluciones genéricas sobre servidores multipropósito.
- 1.2. El firewall deberá poseer aceleración por Hardware para las funciones de ruteo, firewall y tunelización de tráfico WiFi.
- 1.3. HA activo-pasivo y activo-activo, se requiere un cluster de dos 2 equipos iguales.
- 1.4. La configuración de alta disponibilidad debe sincronizar: Sesiones;
- 1.5. La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
- 1.6. La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;
- 1.7. La configuración de alta disponibilidad debe sincronizar: Tablas FIB;

- 1.8. En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
- 1.9. Debe soportar la creación de sistemas virtuales en el mismo equipo;
- 1.10. 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;
- 1.11. 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 áreas funcionales;
- 1.12. IPv6 en forma nativa (manteniendo la mismas características y rendimiento que IPv4)
- 1.13. Soporte a ruteo estático y dinámico (RIP, OSPF v2 y v3, ISIS y BGP)
- 1.14. Soporte a ruteo por política.
- 1.15. Soporte a protocolos de monitoreo como SNMP y sFlow
- 1.16. Soporte a Syslog, con capacidad de envío mediante TCP y SSL.
- 1.17. Debe permitir la creación de hasta 10 sistemas virtuales en el mismo equipo.
- 1.18. Soporte a VXLAN
- 1.19. Debe soportar Traffic Shaping con la posibilidad de aplicarlo, por usuario, IP, interface o aplicación detectada.
- 1.20. Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP.
- 1.21. Los dispositivos de protección de red deben soportar Jumbo Frames.
- 1.22. La solución debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de la solución.
- 1.23. El fabricante debe estar en el cuadrante de líderes de Gartner para "Enterprise Firewall" o firewalls empresariales al menos en los últimos dos años.
- 1.24. El fabricante debe tener la calificación para NGFW de "Recomendado" de acuerdo a la evaluación de NSS Labs al menos en los últimos tres años.

## **2. Firewall:**

- 2.1. Debe soportar la creación de zonas.
- 2.2. Aplicación de políticas por zona o interfaces, por usuarios, direcciones IP o tipos de dispositivo.
- 2.3. Debe ser compatible con NAT dinámica (varios-a-1);
- 2.4. Debe ser compatible con NAT dinámica (muchos-a-muchos);
- 2.5. Debe soportar NAT estática (1-a-1);
- 2.6. Debe admitir NAT estática (muchos-a-muchos);
- 2.7. Debe ser compatible con NAT estático bidireccional 1-a-1;
- 2.8. Debe ser compatible con la traducción de puertos (PAT);
- 2.9. Debe ser compatible con NAT Origen;
- 2.10. Debe ser compatible con NAT de destino;

- 2.11. Debe soportar NAT de origen y NAT de destino de forma simultánea;
- 2.12. Debe soportar NAT de origen y NAT de destino en la misma política
- 2.13. Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
- 2.14. Debe ser compatible con NAT64 y NAT46;
- 2.15. Debe implementar el protocolo ECMP;
- 2.16. VPN IPSec de sitio a sitio y para acceso remoto (sin límite de licencias)
- 2.17. La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI;
- 2.18. Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 2.19. Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
- 2.20. VPN SSL para acceso remoto
- 2.21. 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;
- 2.22. Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
- 2.23. Protecciones contra DoS (denegación de servicio)
- 2.24. Inspección de tráfico SSL (con la capacidad de descifrar el tráfico cifrado) entrante y saliente.
- 2.25. Posibilidad de armar políticas en base a objetos Geográficos
- 2.26. Base de datos de Servicios de Internet (actualizada dinámicamente) para el uso en políticas de seguridad.
- 2.27. Debe de funcionar como proxy web explícito y transparente.
- 2.28. Debe permitir la autenticación transparente (SSO) con sistemas de Active Directory.

### **3. SDWAN:**

- 3.1. Balanceo de vínculos a Internet, VPNs y enlaces WAN (ej: MPLS)
- 3.2. Balanceo Round Robin, Balanceo por peso, cantidad de sesiones, ancho de banda y derrame.
- 3.3. Definición de políticas de SDWAN por Aplicación, Servicio de internet, usuarios, IPs o Interfaces/zonas.
- 3.4. Soporte a más de 5 vínculos a Internet.
- 3.5. Aplicación de Traffic Shaping a las interfaces que utilizan SDWAN basado en aplicaciones, origen, destino, servicio o categoría de URL.

### **4. Control de Aplicaciones:**

- 4.1. Control de Aplicaciones en capa 7, para la detección de tráfico sin importar el puerto que utilicen.
- 4.2. Reconocer al menos 3000 aplicaciones diferentes
- 4.3. Debe inspeccionar el contenido del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas independiente de puerto y protocolo que usen;

- 4.4. Debe permitir la creación de firmas de aplicación manuales.
- 4.5. Debe soportar la creación de firmas manuales.

#### **5. Prevención de Amenazas:**

- 5.1. Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus, anti-spyware y Sandboxing);
- 5.2. La aplicación de controles de IPS y Antimalware deben ser aplicadas a través de las reglas de seguridad.
- 5.3. Debe incluir motores heurísticos, Sandboxing bajo servicio en la nube, detección de anomalías de protocolo y antibotnet.
- 5.4. Debe contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- 5.5. Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- 5.6. 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;
- 5.7. Debe incluir el servicio de Sandbox en la nube, con la capacidad de enviar hasta 20 muestras por minuto y 28.000 por día. Adjuntar documentación que demuestre los alcances del servicio.
- 5.8. El servicio de Sandbox en la nube deberá poder identificar y analizar distintas extensiones de archivos de la suite MS Office, avi, mpeg, mp3, mp4, zip, rar, tar, 7Z, entre otros. Para archivos PDF debe soportar el escaneo de archivos de al menos 1MB de tamaño con el fin de prevenir estrategias de evasión.

#### **6. Filtrado de URL**

- 6.1. Tener por lo menos 60 categorías de URL, actualizadas dinámicamente por el fabricante de la solución.
- 6.2. Permitir página de bloqueo personalizadas;
- 6.3. Los filtros URL deben poder aplicarse por política de seguridad.
- 6.4. Debe permitir la definición de listas negras y blancas de URL.
- 6.5. 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;
- 6.6. Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- 6.7. 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;
- 6.8. Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).

## **7. Identificación de Usuarios**

- 7.1. Las políticas de seguridad deben permitir la integración con servicios de Active Directory, LDAP, y base de datos local.
- 7.2. Debe permitir crear reglas por grupos de usuario o usuarios individuales.
- 7.3. Debe tener integración con RADIUS.
- 7.4. Debe incluir portal captivo para autenticación explícita de los usuarios.
- 7.5. Debe soportar métodos de autenticación como NTLM y Kerberos.
- 7.6. Debe ser integrable con entornos de Citrix XenApp/XenDesktop y Terminal Services.

## **8. DLP**

- 8.1. Permite la creación de filtros para archivos (por tipo y tamaño) y datos predefinidos.
- 8.2. Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);
- 8.3. Soportar la identificación de archivos comprimidos y cifrados.
- 8.4. Permitir identificar y opcionalmente prevenir la transferencia de información sensible

## **9. Wireless Controller**

- 9.1. Deberá gestionar de manera centralizada los puntos de acceso del mismo fabricante de la solución ofertada.
- 9.2. Debe generar túneles cifrados hacia los AP para la gestión de los mismos.
- 9.3. Soporte al cifrado de tuneles entre la controladora y el punto de acceso inalámbrico para el tráfico de las redes WiFi
- 9.4. Debe permitir elegir si el tráfico de cada SSID se enviará hacia la controladora por un túnel o directamente por la interfaz de punto de acceso en una determinada VLAN.
- 9.5. Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS (via 802.1x), con la posibilidad de usar un portal captivo interno.
- 9.6. Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows
- 9.7. Permitir la visualización de los dispositivos inalámbricos conectados por usuario; IP, tipo de autenticación, canal, ancho de banda utilizado, potencia de la señal, tiempo de asociación.
- 9.8. Para la autenticación de los usuarios y dispositivos deberá soportar WPA y WPA2 con 802.1x o Preshared key, WEP y un portal cautivo Web, así como con listas negras y blancas basadas en MAC
- 9.9. La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal.
- 9.10. La configuración de los puntos de acceso debe ser Zero Touch.
- 9.11. Debe contar con un módulo de WIDS.
- 9.12. 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.
- 9.13. Debe tener un mecanismo de ajuste automático de potencia de la señal y de balanceo de usuarios entre puntos de acceso.
  - 9.14. Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados.
  - 9.15. Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID específico mediante protocolo RADIUS o VLAN pooling
  - 9.16. El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming.
  - 9.17. La controladora inalámbrica debe soportar protocolo LLDP.
  - 9.18. Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos;
  - 9.19. La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado.
  - 9.20. Debe proporcionar la capacidad de crear varias claves pre-compartidas de acceso protegido WiFi (WPA-PSK) para que no sea necesario compartir PSK entre dispositivos.
  - 9.21. Gestión de firmware desde el controlador centralizado.

## **10. Switch Controller**

- 10.1. Deberá gestionar de manera centralizada switches del mismo fabricante de la solución ofertada.
- 10.2. Configuración y replicación de VLANs en todos los switches controlados de forma automática.
- 10.3. Gestión de estado de los puertos, VLANs (nativas o permitidas), POE, DHCP blocking, IGMP snooping, Spanning Tree, Loop Guard y Edge Port desde la consola central.
- 10.4. Gestión y aplicación de 802.1X desde el Controlador central a todos los switches gestionados.
- 10.5. Diagrama gráfico en tiempo real de la interconexión de los Switches
- 10.6. Gestión de LLDP desde el controlador centralizado.
- 10.7. Configuración de QoS de forma centralizada.
- 10.8. Gestión y creación de puertos trunk estáticos, LACP pasivo o activo.
- 10.9. Posibilidad de asignar nombres y descripciones a los switches y puertos gestionados.
- 10.10. Gestión de firmware desde el controlador centralizado.
- 10.11. Operación para reinicio y apagado centralizado de los Switches administrados.

### **Licenciamiento y actualizaciones**

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

La vigencia del soporte para actualizaciones de software, soporte del fabricante y soporte de hardware debe proveerse por al menos 1 año bajo el esquema 24x7.

### **Desempeño / Conectividad**

El equipo debe por lo menos ofrecer las siguientes características de desempeño y conectividad

Número de Interfaces Requeridas	8x GE RJ45, 8x GE SFP 2 x 10GE SFP+
Fuentes Redundantes	Sí
Throughput de Firewall (con paquetes de 1518/512/64 Bytes)	36 Gbps/36 Gbps/22 Gbps
Latencia de firewall (con paquetes de 64 byte)	2 $\mu$ s
Throughput de VPN IPsec (con paquetes de 512 byte)	20 Gbps
Throughput de NGFW	5 Gbps
Threat Prevention Throughput	4.5 Gbps
Throughput de Inspección SSL	5.5 Gbps
Políticas de Firewall admitidas	10.000
Tuneles gateway to gateway	2.000
Tuneles client to gateway	50.000
Tuneles SSL	500
Throughput VPN SSL	5 Gbps
Sesiones Concurrentes Máximas	7.5 Millones

Nuevas sesiones / segundo	270.000
AP soportados / AP en modo tunnel	400 / 250
Switches Soportados	40
VDOMs incluidos	10

### **Objeto 3: Solución de Análisis y Reportería**

Con el fin de lograr una visualización completa de las soluciones requeridas se solicita un sistema que permita recibir los logs de la solución de NGFW y permita ver en un único panel de control las distintas variables destacables de seguridad y rendimiento de las soluciones mencionadas, para que a posteriori permita elaborar reportes estándar y personalizables de acuerdo a los requerimientos.

#### **1. Funcionalidades Generales**

- 1.1. Debe soportar acceso vía SSH, WEB (HTTPS) y Telnet para la gestión de la solución
- 1.2. La solución podrá estar compuesta por un Aplicación que podrá ser montada en un servidor virtualizado.
- 1.3. Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.
- 1.4. Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
- 1.5. Soporte SNMP versión 2 y 3
- 1.6. Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
- 1.7. Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
- 1.8. Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH y Telnet.
- 1.9. Autenticación de usuarios de acceso a la plataforma vía Radius
- 1.10. Generación de informes en tiempo real de tráfico, ya sea en mapas geográficos y en tablas.
- 1.11. Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
- 1.12. Autenticación de usuarios de acceso a la plataforma vía Microsoft Active Directory
- 1.13. 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.
- 1.14. Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
- 1.15. Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado

- 1.16. Contar con mecanismos de borrado automático de logs antiguos.
- 1.17. Permitir la importación y exportación de reportes
- 1.18. Debe contar con la capacidad de crear informes en formato HTML
- 1.19. Debe contar con la capacidad de crear informes en formato PDF
- 1.20. Debe contar con la capacidad de crear informes en formato XML
- 1.21. Debe contar con la capacidad de crear informes en formato CSV
- 1.22. Debe permitir exportar los logs en formato CSV
- 1.23. Generación de logs de auditoria, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
- 1.24. 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.
- 1.25. La solución debe contar con reportes predefinidos
- 1.26. Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución
- 1.27. Debe ser posible la duplicación de reportes existentes para su posterior edición.
- 1.28. Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
- 1.29. 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.
- 1.30. 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.
- 1.31. Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
- 1.32. Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
- 1.33. Debe permitir descargar de la plataforma los archivos de logs para uso externo.
- 1.34. Tener la capacidad de generar y enviar reportes periódicos automáticamente.
- 1.35. Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
- 1.36. Permitir el envío por email de manera automática de reportes.
- 1.37. Debe permitir que el reporte a enviar por email sea al destinatario específico.
- 1.38. Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
- 1.39. Debe ser posible visualizar gráficamente en tiempo real el consumo de disco y la tasa de generación de logs por cada dispositivo gestionado.
- 1.40. Debe permitir el uso de filtros en los reportes.
- 1.41. Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
- 1.42. Permitir que los reportes creados sean en idioma Español

- 1.43. Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
- 1.44. Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
- 1.45. Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para su en gráficas y tablas en reportes.
- 1.46. 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.
- 1.47. 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.
- 1.48. 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.
- 1.49. Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
- 1.50. La solución debe servir como un servidor Syslog y aceptar logs de diferentes fabricantes
- 1.51. Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
- 1.52. Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
- 1.53. Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos
- 1.54. Debe permitir visualizar en tiempo real los logs recibidos

## **2. Reportes**

- 2.1. Debe permitir la creación de Dashboards personalizados para visualizar tráfico de aplicaciones, categorías de URL, amenazas, servicios, países, origen y destino.
- 2.2. Debe poder contar con un Indicador de Compromisos (IoC), 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.
- 2.3. Debe contar con reporte de cumplimiento de PCI DSS
- 2.4. Debe contar con reporte de utilización de aplicaciones SaaS
- 2.5. Debe contar con reporte de prevención de pérdida de datos (DLP)
- 2.6. Debe contar con reporte de VPN
- 2.7. Debe contar con reporte de Sistema de prevención de intrusos (IPS)
- 2.8. Debe contar con reporte de reputación de cliente
- 2.9. Debe contar con reporte de análisis de seguridad de usuario
- 2.10. Debe contar con reporte de análisis de amenaza cibernética
- 2.11. Debe contar con reporte de cumplimiento PCI de Wireless.

- 2.12. Debe contar con reporte de AP's y SSID's autorizados, así como clientes WiFi
- 2.13. Debe contar con reporte de vulnerabilidades de solución gestionada de seguridad de equipo terminal.
- 2.14. Debe contar con análisis de seguridad y uso de web, si se tiene plataforma de Cache
- 2.15. Debe contar con reporte de aplicaciones web, si se cuenta con plataforma de seguridad web

### ***Licenciamiento y actualizaciones***

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

La vigencia del soporte para actualizaciones de software, soporte del fabricante debe proveerse por al menos 1 año y bajo el esquema 24x7.

### ***Capacidades / Conectividad***

Almacenamiento Diario de Logs p/Analítica	1GB
Capacidad de Almacenamiento Total	500 Gbps
Cantidad Máxima de Dispositivos Soportados	10.000
Cantidad de Interfaces Soportadas	4
Cantidad de Virtual CPU's o vCPU's (Mínimo)	4
Memoria Requerida (Mínimo)	8GB