TRENES ARGENTINOS
OPERACIONES

SOLUCIÓN DE SEGURIDAD INTEGRAL PARA REDES CON CARACTERÍSTICAS DE NEXT GENERATION FIREWALL (NGFW)

PLIEGO DE ESPECIFICACIONES TÉCNICAS

Artículo 1°. - OBJETO

El presente documento tiene como objeto establecer las características técnicas necesarias para la adquisición una Solución integral de seguridad para la red de datos perimetral y la segmentación interna de los TRES (3) Data Centers contingentes entre sí, toda la Solución deberá contar con licenciamiento por el término de TRES (3) años.

Con el objeto de mantener la seguridad de navegación en internet y para todas las capas de infraestructura de red en todas las redes de la Operadora Ferroviaria Sociedad del Estado (SOFSE).

Artículo 2°. - OFERTA TÉCNICA

El Oferente deberá incluir en su oferta una descripción pormenorizada de la Solución ofrecida, la cual contendrá todos los detalles que permitan evaluar el cumplimiento técnico de las mismas, indicando número de parte, descripción y cantidad.

Cabe aclarar que a lo largo del presente documento y para una mayor claridad técnica, algunos términos se han conservado en su lengua nativa o con sus acrónimos sajones.

La misma se integrará con:

a) Descripción técnica detallada.
b) Documentación en la que consten las características técnicas de los equipos y software que forman parte de la propuesta del Oferente
c) Antecedentes técnicos requeridos.

No se admitirá la especificación “según pliego" como identificación del equipamiento ofrecido.

Artículo 3°. – PLAZO Y LUGAR DE ENTREGA PARA EL EQUIPAMEINTO

El plazo de entrega para el equipamiento será de CIENTO VEINTE (120) días corridos como máximo, a partir de la notificación de la orden de compra.

El plazo de implementación de la Solución será de NOVENTA (90) días corridos como máximo, a partir de la entrega del equipamiento.

El lugar de entrega e implementación será:

DC 1: Dr. Ramos Mejía 1358 / Cabin 1 Retiro 1er piso, Estación Retiro Mitre, CABA

DC 2: Dr. Ramos Mejía 1358 / 2er piso, Estación Retiro Mitre, CABA

DC 3: Tte. Gral. Juan D. Perón 2800 1er Piso, Estación Once, CABA

Artículo 4°. - DESCRIPCIÓN TECNICA

Especificaciones Técnicas requeridas para la provisión de la Solución. La cual deberán cumplir con la totalidad de las siguientes características y requerimientos mínimos.

- La Solución deberá contar con características de Next Generation Firewall (NGFW) para la seguridad integral de la información que pasa por el perímetro y la segmentación interna de los Data Centers 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", como controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta.
- Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance.
- La Solución tiene que ser ofrecida en alta disponibilidad, se entiende por alta disponibilidad una Solución redundante de por lo menos 2 (dos) appliances que cada uno cumpla con las características mínimas mencionadas en estas especificaciones. Si el Oferente para poder cumplir con los requerimientos ofrece N appliance, para poder lograr la alta disponibilidad deberá ofertar N * 2 (dos) appliances.
- La Solución ofrecida debe contar con una plataforma de Seguridad, Orquestación, automatización y Respuesta de incidentes conocida por sus siglas en ingles de SOAR (Security, Orchestration, Automation and Response) y una plataforma integral de gestión de dispositivos IoT con capacidad de gestionar y manejar las vulnerabilidades y seguridad de estos integrada y del mismo fabricante que la plataforma de Next-Generation Firewall (NGFW)
- El fabricante debe estar en el cuadrante de líderes de Gartner para "Enterprise Firewall" o firewalls empresariales en los últimos 6 años.
- El fabricante debe estar como líder en el informe de Forrester de "Zero Trust eXtended (ZTX) Ecosystem Providers.
- El fabricante debe estar certificado para IPv6 en Firewall e IPS por NIST USGv6.
- Las soluciones requeridas deben poder interoperar sin necesidad de software o interacción de terceros.
- Todas las soluciones ofrecidas tienen que ser de un mismo fabricante y tener la posibilidad de orquestarlas entre si y compartir una misma base de inteligencia.

ARQUITECTURA Y SOLUCIONES SOLICITADAS

- La empresa cuenta actualmente con 3 (tres) Data Centers, los cuales cuentan con múltiples enlaces y brindando servicios activos en cada uno de estos Data Centers, por lo cual las soluciones de NGFW ofrecidos tienen que ser implementados en cada uno de los 3 (tres) Data Centers.
- Adicional a los equipos activos a implementar en los Data Centers, el Oferente tiene que proveer un equipo adicional en sitio del cliente (conocido por sus siglas en

ingles como OSS – On Site Spare) para remplazo rápido en caso de que unos de los NGFW presente una falla de hardware.

- La Solución de administración, reportes y gestión centralizada tiene que ser implementada de manera redundante, estando implementada la misma por lo menos en dos Data Center diferentes.
- La Solución de gestión, administraciones y manejo de seguridad de dispositivos IoT debe tener sensores en cada uno de los Data Center y poder brindar gestión centralizada de los dispositivos de toda la red.
- La Solución de SOAR tiene que poder orquestar no solo las tecnologías ofrecidas en el presente pliego, sino que también ser extensibles a toda la operación y herramientas que cuenta la organización y además integrarse con Cisco ISE y pxGrid, para automatizar la integración de los NGFW con la infraestructura de Networking que la compañía actualmente cuenta.

CAPACIDAD

Cada uno de los appliance (NGFW) ofrecidos de la plataforma de seguridad debe poseer las capacidades y características mínimas siguientes:

- Throughput no inferior a 37 Gbps medido con trafico real (no es valido tomar mediciones ideales o de laboratorio) con la funcionalidad de control de aplicaciones habilitada, para todas las firmas que el fabricante posea actualizadas con la última actualización disponible y log habilitado.
- Throughput no inferior a 23 Gbps medido con tráfico de real (no es valido tomar mediciones ideales o de laboratorio), con las siguientes funcionalidades habilitadas simultáneamente: Clasificación y control de aplicaciones, IPS, Control de navegación por URL, Antivirus y Antispyware, Control de amenazas avanzadas de día cero (Sandboxing). Para todas las firmas que la plataforma de seguridad posea totalmente activadas, actualizadas al día y con el mayor nivel de seguridad posible; considerando múltiples políticas de seguridad (por lo menos 100 políticas de seguridad aplicadas), y que tengan habilitado la generación de Logs y NAT aplicado a todas las reglas.
- Soporte no inferior a 8 Millones de conexiones simultaneas con todos los módulos de seguridad de capa 7 habilitados simultáneamente, en el mayor nivel de seguridad posible;
- Soporte no inferior a 390.000 nuevas conexiones por segundo;
- Capacidad de Desencripción de SSL de al menos 800.000 sesiones simultaneas.
- Fuente de energía redundante y hotswap
- Flujo de ventilación de Data Center del estilo “Front-to-back”
- Ventiladores redundantes y con la capacidad de remplazo hotswap.
- Capacidad de al menos 2Tb utilizable de almacenamiento sobre cada NGFW para almacenamiento de logs y reportes, etc. El espacio utilizable tiene que ser disponible para su uso luego de aplicar algún método de redundancia (mínimo RAID1 o superior).
- Disco Solid State Drive (SSD) como algún método de redundancia (mínimo RAID1 o superior) para el sistema y uso de la Solución.

A continuación, se detallan las Interfaces de red requeridas libres para su uso, es decir, disponer de las mismas luego del armado de la alta disponibilidad:

- Al menos 4 (cuatro) interfaces de red 100/1.000/10.000 sobre interfaces de cobre.
- Al menos 16 (dieciséis) interfaces de red 10 Gbps SFP+/SFP.
- Al menos 4 (cuatro) interfaces de red de 40/100 Gbps QSFP28;
- Interfaces de red para el armado de cluster de alta disponibilidad:
- Al menos 1 (una) interface de 100 Gbps QSFP28.
- Al menos 2 (dos) interfaces de 10 Gbps SFP+;
- Al menos 2 (dos) interfaces de 1 Gbps (cobre) dedicadas al armado de alta disponibilidad.
- Al menos 1 (una) interface de red 1 Gbps dedicada para administración;
- Al menos 1 (una) interface de tipo consola o similar;
- Soporte no inferior a 120 (ciento veinte) ruteadores virtuales;
- Soporte no inferior a 15.000 (quince mil) zonas de seguridad;
- Estar licenciada para soportar sin uso de licenciamiento adicional, al menos 15.000 (quince mil) clientes de VPN SSL y IPSec simultáneos del estilo cliente-servidor;
- Estar licenciada para soportar sin uso de licenciamiento adicional, al menos 4.000 (cuatro mil) túneles de VPN IPSEC simultáneos del estilo sitio-a-sitio;
- Debe soportar al menos 25 (veinticinco) sistemas virtuales lógicos (Contextos) sobre cada NGFW Físico y tener la posibilidad de expandir los mismos por lo menos hasta 100 (cien) sistemas virtuales lógicos (Contextos).
- Por el equipamiento que compone la plataforma de seguridad, se entiende como hardware y licenciamiento de software necesarios para su funcionamiento;
- Por consola de administración y monitoreo, se entiende el licenciamiento de software necesario para las dos funcionalidades, también como hardware dedicado para el funcionamiento de las mismas.
- La consola de administración y monitoreo puede residir en el mismo appliance de seguridad de red, desde que posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función;
- Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados en el site del fabricante como listas de end-of-life y end-of-sale.

CARACTERÍSTICAS GENERALES

- La Solución debe consistir en appliances de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), y consola de administración y monitoreo;
- Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- La plataforma debe ser optimizada para análisis de contenido de aplicaciones en Capa 7;
- El hardware y software que ejecuten las funcionalidades de seguridad de red y de administración y monitoreo, deben ser de tipo appliance. No serán aceptados equipamientos servidores y sistema operacional de uso genérico;
- La Solución ofrecida tiene que ser un Next Generation Firewall nativo de capa 7, es decir, con la capacidad de analizar en una única pasada todos los componentes de la sesión identificando la aplicación que se está utilizando, el usuario, el dispositivo y analizando en profundidad el contenido de cada paquete de trafico de red en una sola pasada de análisis con el objetivo de no degradar la performance de la red.

- La performance de la Solución tiene que ser predecible y no tiene que verse degradada por la habilitación de módulos de seguridad o firmas de seguridad de la Solución.
- Todos los equipamientos ofrecidos deben ser adecuados para montaje en rack 19”
- El software deberá ser ofrecido en su versión más estable y/o más avanzada;
- La arquitectura de procesadores utilizado por la Solución tiene que ser procesadores reprogramables, tipo FPGA, para garantizar que con futuras actualizaciones el equipo no quede obsoleto.
- Los dispositivos de seguridad de red deben poseer por lo menos las siguientes funcionalidades:
    - Soporte de 4094 VLAN Tags 802.1q, tanto por dispositivo como en una sola interfaz;
    - Agregación de links 802.3ad;
    - Policy based routing o policy based forwarding;
    - Ruteo multicast (PIM-SM);
    - DHCP Relay;
    - DHCP Server;
    - Jumbo Frames;
    - Soporte a creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3;
    - Soportar sub-interfaces ethernet lógicas.
      Debe soportar los siguientes tipos de NAT:
    - Nat dinamico (Many-to-1);
    - Nat dinámico (Many-to-Many);
    - Nat estático (1-to-1);
    - NAT estático (Many-to-Many);
    - Nat estático bidireccional 1-to-1;
    - Traducción de porta (PAT);
    - NAT de Origen;
    - NAT de Destino;
    - Soportar NAT de Origen y NAT de Destino simultáneamente;
    - Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
    - Enviar log para sistemas de monitoreo externos, simultáneamente;
    - Debe tener la opción de enviar logs para los sistemas de monitoreo externos vía protocolo TCP y SSL;
    - Debe permitir configurar certificado caso necesario para autenticación del sistema de monitoreo externo de logs;
    - Seguridad contra anti-spoofing;
    - Para IPv4, debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2);
    - Debe soportar MP-BGP
    - Para IPv6, debe soportar enrutamiento estático y dinámico (OSPFv3)
    - Soportar OSPF *graceful restart*;
    - Debe ser capaz de balancear varios enlaces de internet sin el uso de políticas específicas, permitiendo aplicar una variedad de algoritmos distintos (round Robin, weighted...)
    - Soportar BFD (bidirectional forward detection)
    - Soportar LACP/LLDP Pre-negotiation
    - Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Desencripción SSL y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Activo/Activo, Activo/Pasivo, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones;

- Debe contar con una herramienta para poder optimizar políticas de seguridad, detectar cuáles no se esten usando y por cuánto tiempo; poder aprender de las políticas aplicadas y sugerir que aplicaciones deberían aplicarse a las políticas en el NGFW. Dar estadísticas de uso, ancho de banda por aplicación, último hit de las aplicaciones, sobre cada política, con el objetivo de optimizar y mejorar la configuración del NGFW.
- Los dispositivos de seguridad deben tener la capacidad de operar de forma simultanea mediante el uso de sus interfaces físicas en los siguientes modos dentro del mismo firewall, sin necesidad de tener que hacer uso de contextos virtuales: Modo sniffer (monitoreo y análisis del tráfico de red), Capa 2 (L2), Capa 3 (L3) y modo Transparente;
- Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red;
- Modo Capa – 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación;
- Modo Capa – 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default Gateway de las redes protegidas;
- Modo Transparente, para poder inspeccionar de datos en línea y tener visibilidad del control de trafico en nivel de aplicación sobre 2 puertos en modo bridge/Transparente.
- Modo mixto de trabajo Sniffer, Transparente, L2 e L3 simultáneamente en diferentes interfaces físicas del mismo equipo;
- En el modo Transparente, debe poder soportar al menos 256 interfaces (físicas y/o virtuales) sobre cada sistema virtual lógico (Contexto).
- Soporte a configuración de alta disponibilidad Activo/Pasivo e Activo/Activo:
- En modo transparente;
- En layer 3;

- La configuración en alta disponibilidad debe sincronizar:
  - Sesiones;
  - Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QOS y objetos de red;
  - Certificados de desencripción;
  - Asociaciones de Seguridad de las VPNs;
  - Tablas FIB;
  - El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link.
- Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
- Debe poder inspeccionar protocolos como:
  - GRE
  - IPSEC no encriptado (NULL o AH)

CONTROL POR POLÍTICA DE FIREWALL

- Deberá soportar controles por zona de seguridad
- Controles de políticas por puerto y protocolo.
- Control de políticas por aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.
- Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.
- Control de políticas por código de País (Por ejemplo: AR, BR, USA, UK, RUS).

- Control, inspección y desencripción de SSL por política para tráfico de entrada (Inbound) y Salida (Outbound).
- Debe soportar offload de certificado en inspección de conexiones SSL de entrada (Inbound);
- Debe desencriptar tráfico Inbound y Outbound en conexiones negociadas con TLS v1.1, v1.2 y v1.3;
- Debe desencriptar tráfico que use certificados ECC (como ECDSA)
- Control de inspección y desencripción de SSH por política;
- La plataforma de seguridad debe implementar copia del tráfico desencriptado (SSL y TLS) para soluciones externas de análisis (Forense de red, DLP, Análisis de Amenazas, entre otras);
- Se permite el uso de appliance externo, específico para la desencripción de (SSL y TLS), con copia del tráfico desencriptado tanto para el firewall, como para otras soluciones de análisis externas.
- La Solución deberá contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL / TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de trafico, el mismo tiene que tener varios estados de trobleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del trafico.
- Bloqueos de los siguientes tipos de archivos: bat, cab, dll, exe, pif, y reg
- Traffic shaping QoS basado en políticas (Prioridad, Garantía y Máximo)
- QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones.
- Al crear o editar políticas de seguridad, se debe poder forzar el uso de una descripción, tag o comentario de auditoria. Esto con el fin de garantizar buenas practicas de documentación, organización y auditoria.
- Soporte a objetos y Reglas IPV6.
- Soporte a objetos y Reglas multicast.
- Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.

CONTROL DE APLICACIONES

- Los dispositivos de seguridad de red deberán poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo, con las siguientes funcionalidades:
    - Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.
    - Reconocer por lo menos 3500 aplicaciones diferentes, incluyendo, más no limitado: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail;
    - Reconocer por lo menos las siguientes aplicaciones: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;
    - Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también

debe determinar si una aplicación está utilizando su puerto default o no, incluyendo, más no limitando a RDP en el puerto 80 en vez del 389;
- Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis comportamental del tráfico observado, incluyendo, más no limitado a Encrypted Bittorrent y aplicaciones VOIP que utilizan cifrado propietario;
- Identificar el uso de tácticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones cifradas, tales como Skype y ataques mediante el puerto 443.
- Para tráfico Cifrado (SSL y SSH), debe permitir la desencripción de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante;
- Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo, incluyendo, más no limitado a Yahoo! Instant Messenger usando HTTP. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo, más no limitado a la compartición de archivos dentro de Webex. También debe detectar el archivo y otros contenidos que deben ser inspeccionados de acuerdo a las Reglas de seguridad implementadas;
- Debe Identificar el uso de tácticas evasivas vía comunicaciones cifradas;
- Debe Actualizar la base de firmas de aplicaciones automáticamente;
- Debe Reconocer aplicaciones en IPv6;
- Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD;
- Los dispositivos de seguridad de red deben poseer la capacidad de identificar al usuario de red con integración al Microsoft Active Directory, sin la necesidad de instalación de agente en el Domain Controller, ni en las estaciones de los usuarios;
- Debe ser posible adicionar control de aplicaciones en todas las Reglas de seguridad del dispositivo, o sea, no limitándose solamente a la posibilidad de habilitar control de aplicaciones en algunas Reglas;
- Debe soportar múltiples métodos de identificación y clasificación de las aplicaciones, por lo menos chequeo de firmas, decodificación de protocolos y análisis heurístico;
- Para mantener la seguridad de la red eficiente, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas;
- Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interface gráfica de la Solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la empresa;

- La creación de firmas personalizadas debe permitir el uso de expresiones regulares, contexto (sesiones o transacciones), usando la posición en el payload de los paquetes TCP y UDP y usando decoders de por lo menos los siguientes protocolos:
  - HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP y File body.
- El fabricante debe permitir la solicitud de inclusión de aplicaciones en la base de firmas de aplicaciones;
- Debe alertar al usuario cuando una aplicación fuera bloqueada
- Debe posibilitar que el control de puertos sea aplicado para todas las aplicaciones;
- Debe posibilitar la diferenciación de tráficos Peer2Peer (Bittorrent, emule, neonet, etc.) proveyendo granularidad de control/políticas para los mismos;
- Debe posibilitar la diferenciación de tráficos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) proveyendo granularidad de control/políticas para los mismos;

- Debe posibilitar la diferenciación y control de partes de las aplicaciones como por ejemplo permitir Gtalk chat y bloquear la transferencia de IM (mensajería instantánea);
- Debe posibilitar a diferenciación de aplicaciones Proxies (ghostsurf, freegate, etc.) proveyendo granularidad de control/políticas para los mismos;
- Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:
    - Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
    - Nivel de riesgo de las aplicaciones.
    - Categoría y sub-categoría de aplicaciones.
    - Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda, etc.
- Debe poder monitorear aplicaciones SaaS (Software as a service) tanto via GUI como en reporte predefinido.
- Las políticas de seguridad tienen que poder ser creadas en base a las aplicaciones y no en base a puertos TCP/UDP.
- La aplicación de seguridad tiene que ser 100% en base a aplicaciones pudiendo aplicar reglas especificas a cada aplicación, ejemplo si dos aplicaciones utilizan el mismo puerto de comunicaciones, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles de seguridad diferentes a cada aplicación.
- Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz grafica debe sugerir y permitir agregar las políticas dependientes de la seleccionada, para poder permitir el uso correcto de la aplicación.

PREVENCION DE AMENAZAS

- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware integrados en el propio appliance de Firewall
- Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware);
- Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
- Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo;
- Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Anti-Vírus y Antispyware habilitadas simultáneamente.
- Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo;
- Excepciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma por firma;
- Debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems.
- Debe permitir el bloqueo de vulnerabilidades.
- Debe permitir el bloqueo de exploits conocidos.
- Debe incluir seguridad contra ataques de negación de servicios.
- Deberá poseer los siguientes mecanismos de inspección de IPS:

- Análisis de parones de estado de conexiones;
- Análisis de decodificación de protocolo;
- Análisis para detección de anomalías de protocolo;
- Análisis heurístico;
- IP Defragmentation;Re ensamblado de paquetes de TCP;
- Bloqueo de paquetes malformados.
- Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;
- Detectar y bloquear el origen de portscans;
- Bloquear ataques efectuados por worms conocidos, permitiendo al administrador adicionar nuevos patrones;
- Soportar los siguientes mecanismos de inspección contra amenazas de red: análisis de patrones de estado de conexiones, análisis de decodificación de protocolo, análisis para detección de anomalías de protocolo, análisis heurístico, IP Defragmentation, re ensamblado de paquetes de TCP y bloqueo de paquetes malformados;
- Posea firmas específicas para la mitigación de ataques DoS;
- Posea firmas para bloqueo de ataques de buffer overflow;
- Posea firmas de C2 (Comando y control) generadas de forma automática.
- Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
- Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- Soportar bloqueo de archivos por tipo;
- Identificar y bloquear comunicaciones como botnets;
- Debe soportar varias técnicas de prevención, incluyendo Drop y tcp-rst (Cliente, Servidor y ambos);
- Debe soportar referencia cruzada como CVE;
- La Solución ofrecida a partir de los logs debe poder generar indicadores “tags” para IP de equipos a partir de las detecciones de amenazas con el objetivo de poder utilizar los mismos en grupos dinámicos y aplicarlos a otras políticas. Esta funcionalidad tiene que poder efectuarse localmente en el mismo NGFW o bien poder una vez detectado generar el Tag en un firewall remoto o en la consola de gestión para poder aplicar los grupos dinámicos local, remoto o a todos los NGFW de la organización.
- La funcionalidad de Indicadores/Tags mencionada en el punto anterior tiene que poder utilizarse para poder agregar o quitar tags a la IP de origen o destino de una detección efectuada.
- Registrar en la consola de monitoreo las siguientes informaciones sobre amenazas identificadas:
- Debe soportar la captura de paquetes (PCAP), por firma de IPS y Antispyware;
- Debe permitir que en la captura de paquetes por firmas de IPS y Antispyware sea definido el número de paquetes a ser capturados. Esta captura debe permitir seleccionar, como mínimo, 50 paquetes;
- Debe poseer la función reSolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos;
- Permitir el bloqueo de virus, por al menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- Los eventos deben identificar el país de donde partió la amenaza;
- Debe incluir seguridad contra virus en contenido HTML y JavaScript, software espía (spyware) y worms.
- Seguridad contra downloads involuntarios usando HTTP de archivos ejecutables. maliciosos.

- Rastreo de virus en pdf.
- Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.)
- Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques basados en políticas del firewall considerando Usuarios, Grupos de usuarios, origen, destino, zonas de seguridad, etc, o sea, cada política de firewall podrá tener una configuración diferente de IPS, siendo esas políticas por Usuarios, Grupos de usuario, origen, destino, zonas de seguridad.
- Capacidad de poder re-direccionar el trafico de consultas de DNS a un servidor del tipo sinkhole para poder identificar equipos comprometidos con spyware o actividad de command and control dentro de la red corporativa.

ANALISIS DE MALWARE MODERNO

- Poseer la capacidad de análisis de amenazas no conocidas;
- Debido a los Malware hoy en día se debe ser muy dinámicos y un antivirus común no es capaz de detectar los mismos a la misma velocidad que sus variaciones son creadas, la Solución ofertada deber poseer funcionalidades para análisis de Malware no conocidos incluidas en la propia herramienta
- El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis "In Cloud" o local, donde el archivo será ejecutado y simulado en un ambiente controlado;
- Seleccionar a través de la política de Firewall que tipos de archivos sufrirán este análisis;
- Soportar el análisis de por lo menos 60 (sesenta) tipos de comportamientos maliciosos para el análisis de la amenaza no conocida;
- Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP y Windows 7;
- Debe soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB;
- El sistema de análisis “In Cloud” o local debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo Malware y proveer informaciones sobre el usuario infectado (su dirección ip y su login de red);
- El sistema automático de análisis "In Cloud" o local debe emitir relación para identificar cuales soluciones de antivirus existentes en el mercado poseen firmas para bloquear el malware;
- Debe permitir exportar el resultado de los análisis de malware de día Zero en PDF y CSV a partir de la propia interfaz de administración;
- Debe permitir la descarga de los malware identificados a partir de la propia interfaz de administración;
- Debe permitir visualizar los resultados de los análisis de malware de día Zero en los diferentes sistemas operacionales soportados;
- Debe permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día Zero a partir de la propia interfaz de administración.
- Soportar el análisis de archivos ejecutables, DLLs, ZIP y encriptados en SSL en el ambiente controlado;
- Soportar el análisis de archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), email link, flash, archivos de MacOSX (mach-o, dmg, pkg) y Android APKs en el ambiente controlado;

- Poseer SLA de, como máximo, 5 minutos para actualización de la base de vacunas contra malware desconocidos identificados en el ambiente controlado;
- Permitir el envío de archivos para análisis en el ambiente controlado vía web y de forma automática vía API.
- Debe poder dar veredictos distintos, como mínimo:
  - Malicioso
  - Grayware
  - Benigno
  - Phising
- En caso de detectar una forma de evasión de maquina virtual, debe poder enviar de forma automática a revisión en modo Bare Metal (maquinas físicas)
- Capacidad de poder aplicar técnicas de aprendizaje de maquina (Machine Learning) localmente sobre los NGFW para poder identificar amenazas desconocidas y bloquear la mismas durante la descarga de los archivos por parte de los usuarios.

PROTECCION AVANZADA DE DNS

- La Solución debe ser capaz de proteger contra decenas de millones de dominios maliciosos identificados con análisis en tiempo real sin depender de firmas estáticas.
- La protección de DNS debe ser alimentada exponencialmente por un servicio de inteligencia global.
- El servicio de protección de DNS debe alimentarse de telemetría provista por clientes a nivel mundial y fuentes de inteligencia de amenazas de terceros.
- La Solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (por sus siglas en ingles conocido como DGA – Domain Generation Algoritm).
- Aprendizaje automático para detectar dominios DGA nuevos y nunca antes vistos mediante el análisis de las consultas de DNS a medida que se realizan.
- Debe utilizar machine learning o inteligencia artificial para detectar nuevos dominios nunca antes vistos autogenerados por algoritmos DGA.
- Debe poseer políticas para bloquear dominios DGA o interrumpir las consultar de DNS a dichos dominios.
- Debe detectar e interrumpir robo de datos ocultos o enviados mediante túneles en trafico DNS.
- Debe analizar las consultas de DNS, incluyendo las tasas de consultas y patrones, entropía, frecuencia, análisis de dominios, etc. para detectar posibles intentos de tunelización de DNS.

IDENTIFICACION DE USUARIOS

- Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de quien está utilizando cuales aplicaciones a través de la integración como servicios de directorio, autenticación vía ldap, Active Directory, E-directory y base de datos local.
- Debe poseer integración con Microsoft Active Directory para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
- Debe poseer integración con Radius para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
- Debe poseer integración con TACACS+
- Debe posea integración con Ldap para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios.

- Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x y soluciones NAC vía syslog, para la identificación de direcciones IP y usuarios
- Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal).
- Soporte a autenticación Kerberos.
- Soporte SAML 2.0
- La Solución ofrecida debe soportar e incluir múltiples factores de autenticación (como por ejemplo usuario y password + 2FA hard token + 2FA soft token + portal cautivo) para poder utilizarlo tanto en aplicación web como en aplicaciones cliente servidor.
- Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tiene estos servicios
- Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.

QOS

- Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, ustream, etc) y tener un alto consumo de ancho de banda, se requiere que la Solución, a la vez de poder permitir o negar ese tipo de aplicaciones, debe tener la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto de audio como de vídeo streaming.
- Soportar la creación de políticas de QoS por:
    - Dirección de origen
    - Dirección de destino
    - Por usuario y grupo de LDAP/AD.
    - Por aplicaciones, incluyendo, más no limitando a Skype, Bittorrent, YouTube y Azureus;
    - Por puerto;
- El QoS debe permitir la definición de clases por:
    - Ancho de Banda garantizado
    - Ancho de Banda Máximo
    - Cola de prioridad.
- Soportar priorización Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
- Soportar marcación de paquetes Diffserv, inclusive por aplicaciones;
- Disponer de estadísticas Real Time para clases de QoS.
- Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario.

FILTRO DE DATOS

- Permite la creación de filtros para archivos y datos predefinidos;
- Los archivos deben ser identificados por extensión y firmas;
- Permite identificar y opcionalmente prevenir la transferencia de varios tipos de archivos (MS Office, PDF, etc) identificados sobre aplicaciones (P2P, InstantMessaging, SMB, etc);

- Soportar la identificación de archivos compactados y las aplicaciones de políticas sobre el contenido de esos tipos de archivos;
- Permitir identificar y opcionalmente prevenir la transferencia de informaciones sensibles, incluyendo, más no limitando al número de tarjetas de crédito, permitiendo la creación de nuevos tipos de datos vía expresión regular;
- Permitir listar el número de aplicaciones soportadas para control de datos;
- Permitir listar el número de tipos de archivos soportados para el control de datos;
- Debe poder integrarse son soluciones de punto final de terceros para mejorar la política de DLP.
- Debe traer por efecto al menos dos perfiles de bloqueo predefinidos.

GEO-LOCALIZACION

- Soportar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sean bloqueados.
- Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
- Debe posibilitar la creación de regiones geográficas desde la interfaz gráfica y crear políticas utilizando las mismas.

VPN

- Soportar VPN Site-to-Site y Cliente-To-Site;
- Soportar IPSec VPN;
- Soportar SSL VPN;
- La VPN IPSEc debe soportar:
  - DES y 3DES;
  - Autenticación MD5 e SHA-1;
  - Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
  - Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
  - AES 128, 192 e 256 (Advanced Encryption Standard)
  - Debe permitir SSO via Kerberos
  - Autenticación vía certificado IKE PKI.
  - Debe ser compatible con la Suite B de protocolos de NSA
- Debe poseer interoperabilidad como los siguientes fabricantes:
  - Cisco;
  - Checkpoint;
  - Juniper;
  - Palo Alto Networks;
  - Fortinet;
  - Sonic Wall
- Las VPN SSL deben soportar:
  - Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operacional del equipamiento o por medio de interfaz WEB;
  - Las funcionalidades de VPN SSL deben ser atendidas con o sin el uso de agente;
  - La asignación de dirección IP en los clientes remotos de VPN;
  - La asignación de DNS en los clientes remotos de VPN;
  - Debe haber la opción de ocultar el agente de VPN instalado en el cliente remoto, tornando el mismo invisible para el usuario;
  - Deber permitir criar políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN SSL;
  - Las VPN SSL deben soportar proxy arp y el uso de interfaces PPPOE;
  - Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;

- Permite establecer un túnel VPN client-to-site del cliente a la plataforma de seguridad, proveyendo una Solución de single-sign-on a los usuarios, integrándose como las herramientas de Windows-logon;
- Soporte de lectura y verificación de CRL (certificate revocation list);
- Permite la aplicación de políticas de seguridad y visibilidades para las aplicaciones que circulan dentro de los túneles SSL;
- El agente de VPN a ser instalado en los equipamientos desktop y laptops, debe ser capaz de ser distribuido de manera automática vía Microsoft SMS, Active Directory y ser descargado directamente desde su propio portal, en el cual residirá el centralizador de VPN;
- El agente deberá comunicarse con el portal para determinar las políticas de seguridad del usuario,
- Debe permitir que las conexiones como VPN SSL sean establecidas de las siguientes formas:
  - Antes del usuario autenticarse en la estación;
  - Después de la autenticación del usuario en la estación;
  - Bajo demanda del usuario;
- Deberá mantener una conexión segura con el portal durante la sesión.
- El agente de VPN SSL client-to-site debe ser compatible al menos con: Windows XP, Vista, Windows 7, Windows 8, Windows 10, MacOS X; Apple iOS, Android, Linux, Windows 10 UWP y Google Chrome OS 45 superior
- El portal de VPN debe enviar al cliente remoto la lista de gateways VPN activos para el establecimiento de la conexión, los cuales deben poder ser administrados centralizadamente
- Debe haber una opción en el cliente remoto de escoger manualmente el Gateway de VPN y de forma automática a través de la mejor respuesta entre los gateways disponibles con base al más rápido.
- Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa

- Debe soportar VPN SSL sin el uso de cliente
  - Esta función no debe estar basada en Java
- Debe poder integrarse con soluciones MDM de terceros (por ejemplo, AirWatch).
- Debe permitir configurar Split Tunel inteligente, que permita seleccionar el tráfico a enrutar en base a la aplicación y dominio de internet. Por ejemplo, la navegación a Salesforce que viaje por el túnel VPN, pero no todo el resto de tráfico de internet.
- Debe permitir aislar el dispositivo de la red y mantenerlo en cuarentena de forma dinámica, en caso se detecte alguna actividad maliciosa
- Debe permitir la configuración de políticas de seguridad de VPN basado en las características del equipo, por lo menos se deberá recopilar las siguientes características: sistema operativo, dominio de red, versión de parche, software antivirus, software DLP y software de cifrado de disco. De tal forma que si el equipo no cumple cierta condición basado en esas características (Perfilamiento y Postura), no permita el acceso a la VPN o le otorgue acceso de mayores restricciones.
- El Perfilamiento y postura mencionado en el punto anterior, tiene que poder efectuarse inclusive dentro de la red, entre dos o mas segmentos de red que controle el firewall, sin necesidad de armar un túnel de VPN, sino solamente utilizando el perfilamiento y postura del equipo de punto final sobre las políticas de seguridad del NGFW.

SOLUCION DE SEGURIDAD PARA DISPOSITIVOS DE IOT

- La Solución deberá contar con un módulo de monitoreo, descubrimiento, identificación y clasificación de dispositivos IoT (Internet de las Cosas) como

teléfonos IP, cámaras de vigilancia, consolas de videojuegos, impresoras, dispositivos médicos, equipos industriales, entre otros.

- Por cada dispositivo IoT identificado deberá mostrar la marca del fabricante, tipo de dispositivo, serial number, sistema operativo, dirección IP, dirección MAC.
- Debe descubrir y mantener un inventario de dispositivos IoT de forma automática, el cual deberá basarse en al menos dos mecanismos de descubrimiento como Firmas, Machine Learning u otro, con el objetivo de brindar mayor fiabilidad.
- Debe identificar dispositivos que posean software o hardware desactualizado y vulnerable, junto con su respectivo identificador CVE.
- Mostrar el nivel de riesgo de cada dispositivo IoT clasificando su severidad por nivel Bajo, Medio, Alto y Crítico o una clasificación equivalente.
- Mostar los ataques e intentos de ataques hacia los dispositivos IoT.
- Mostrar la actividad en la red de los dispositivos IoT, a nivel de tráfico entrante y saliente. Adicionalmente deberá mostrar la aplicación, protocolo y puerto utilizado para dicha actividad de red.
- Deberá contar con un mapa geográfico que facilite el monitoreo de la actividad de red del dispositivo IoT.
- Deberá estar integrado nativamente a la plataforma Next Generation Firewall, con el objetivo de que la política de seguridad se pueda realizar directamente en base al Dispositivo IoT, en lugar de usar Direcciones IP.
- Esta funcionalidad deberá poder ser ofrecida sin necesidad de instalar hardware adicional.

CONSOLA DE ADMINISTRACION y MONITOREO

- Debe tener una Solución de administración centralizada, posibilitando dicha administración para varios equipos.
- La Solución de consola de administración, monitoreo seguridad y reportes tiene que ser implementada de manera redundante.
- La plataforma de gestión centralizada, reportes, monitoreo y centralización de logs tiene que ser escalable y poder soportar gestionar por lo menos de 10 (diez) soluciones de IPS/NGFW
- La administración de la Solución debe posibilitar un conjunto de estadísticas de todo el tráfico que pasa por los equipos de la plataforma de seguridad.
- Debe controlar todos los dispositivos de la plataforma de seguridad en una única consola, con administración de roles, privilegios y funciones
- La administración centralizada deberá ser entregada como appliance físico o bien como appliance virtual, pero cumpliendo los requerimientos mencionados. En caso de ser equipo físico debe ser compatible con un rack 19” y tener todos los accesorios necesarios para su instalación
- Debe tener al menos 16 Tb utilizables, luego de aplicar algun método de redundancia (RAID) para almacenamiento de Logs y reportes y estar licenciado para poder soportar ese almacenamiento.
- Esta Solución debe estar montada en un servidor con fuentes de energía redundantes y con la posibilidad de trabajar en hotswap
- Debe tener al menos 4 interfaces 10/100/1000 Base T
- Debe poder separar funciones entre las distintas interfaces, como por ejemplo separar logs de administración.
- Debe permitir el control global de las políticas para todos los dispositivos que componen la plataforma de seguridad.
- Debe soportar organizar los dispositivos administrados en grupos: los sistemas virtuales deben ser administrados como dispositivos individuales, los grupos pueden ser geográficos, por funcionalidad (por ejemplo, IPS), y distribuidos.

- Debe permitir la creación de objetos y políticas compartidas.
- Debe consolidar logs y reportes de todos los dispositivos administrados;
- Debe permitir exportar backups de configuración automáticamente vía programación;
- Debe permitir realizar RBAC (Rol based administration) desde el directorio activo
- Debe generar una estructura jerárquica para poder diferenciar políticas generarles y locales y así mejorar la administración global de la compañía.
- Debe poder diferenciar la administración de los distintos Sistemas Virtuales de los equipos configurados y poder separar los logs y reporteria de cada Sistemas Virtuales
- Debe centralizar la administración de Reglas y políticas del cluster, usando una única interfaz de administración
- Debe poder recibir logs de soluciones del mismo fabricante, como por ejemplo endpoint
- Debe soportar una arquitectura de plug-in para integración con terceros
- Debe tener capacidad de análisis analíticos de logs de por lo menos 60 dias.
- La administración de la Solución debe soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta;
- En el caso de que sea necesaria la instalación de cliente para administración de la Solución, el mismo debe ser compatible con sistemas operacionales Windows y Linux;
- La administración debe permitir/hacer:
    - Creación y administración de políticas de firewall y control de aplicaciones;
    - Creación y administración de políticas de IPS y Anti-Spyware;
    - Creación y administración de políticas de filtro de URL
    - Monitoreo de logs;
    - Herramientas de investigación de logs;
    - Debugging;
    - Captura de paquetes.
    - Debe permitir el acceso concurrente de administradores;
    - Debe tener un mecanismo de búsqueda de comandos de administración vía SSH, facilitando la localización de los comandos;
    - Debe permitir usar palabras clave y distintos tags de colores para facilitar la identificación de Reglas;
    - Debe permitir monitorear vía SNMP fallas en el hardware, inserción o remoción de fuentes, discos y ventiladores, uso de recursos por número elevado de sesiones, número de túneles establecidos de VPN cliente-to-site, porcentaje de utilización en referencia al número total soportado/licenciado y número de sesiones establecidas;
    - Debe permitir el bloqueo de alteraciones, en el caso de acceso simultaneo de dos o más administradores;
    - Debe permitir la definición de perfiles de acceso a la consola con permisos granulares como: acceso de escritura, acceso de lectura, creación de usuarios, alteración de configuraciones;
    - Debe permitir la autenticación integrada con Microsoft Active Directory y servidor Radius;
    - Debe permitir la localización de donde están siendo utilizados objetos en: Reglas, dirección IP, Rango de IPs, subredes u objetos
    - Debe poder atribuir secuencialmente un número a cada regla de firewall, NAT, QOS y Reglas de DOS;
    - Debe permitir la creación de Reglas que estén activas en un horario definido;
    - Debe permitir la creación de Reglas con fecha de expiración;
    - Debe poder realizar un backup de las configuraciones y rollback de configuración para la última configuración salvada;

- Debe soportar el Rollback de Sistema operativo para la última versión local;
- Debe poseer la habilidad del upgrade vía SCP, TFTP e interfaz de administración;
- Debe poder validar las Reglas antes de las aplicaciones;
- Debe permitir la validación de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing);
- Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas.
- Debe posibilitar la integración con otras soluciones de SIEM del mercado (third-party SIEM vendors)
- Debe permitirá la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo y el horario de la alteración;
- Deberá tener la capacidad de generar un gráfico que permita visualizar los cambios en la utilización de aplicaciones en la red en lo que se refiere a un período de tiempo anterior, para permitir comparar los diferentes consumos realizados por las aplicaciones en el tiempo presente con relación al pasado;
- Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la institución;
- Debe proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Antispyware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes;
- La administración de la Solución debe posibilitar la recolección de estadísticas de todo el tráfico que pasa por los dispositivos de seguridad;
- Debe proveer resúmenes de utilización de los recursos por aplicaciones, amenazas (IPS, Anti-Spyware y antivirus de la Solución), etc;
- Debe proveer de una visualización sumarizada de todas las aplicaciones, amenazas (IPS, Antivirus e Anti-Spyware) y URLs que pasan por la Solución;
- Debe poseer un mecanismo "Drill-Down" para navegación por los resúmenes en tiempo real;
- En las listas de "Drill-Down", debe ser posible identificar el usuario que ha determinado el acceso;
- Debe ser posible exportar los logs en CSV;
- Deberá ser posible acceder al equipamiento a aplicar configuraciones durante momentos donde el tráfico sea muy alto y la CPU y memoria del equipamiento este siendo totalmente utilizada.
- Debe tener rotación de logs;
- Debe tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto):
- Debe mostrar la situación del dispositivo y del cluster;
- Debe poder mostrar las principales aplicaciones;
- Debe poder mostrar las principales aplicaciones por riesgo;
- Debe poder mostrar los administradores autenticados en la plataforma de seguridad;
- Debe poder mostrar el número de sesiones simultaneas;
- Debe poder mostrar el estado de las interfaces;
- Debe poder mostrar el uso de CPU;

- Generación de reportes. Como mínimo los siguientes reportes deben poder ser generados:
  - Resumen gráfico de las aplicaciones utilizadas;
  - Principales aplicaciones por utilización de ancho de banda de entrada y salida;
  - Principales aplicaciones por tasa de transferencia en bytes;
  - Principales hosts por número de amenazas identificadas;

    - Actividades de un usuario específico y grupo de usuarios del AD/LDAP, incluyendo aplicaciones accedidas y amenazas (IPS, y Anti-Spyware), de red vinculadas a este tráfico;
    - Debe permitir la creación de reportes personalizados;
- En cada criterio de búsqueda del log debe ser posible incluir múltiples entradas (ej. 10 redes e IP's distintas; servicios HTTP, HTTPS y SMTP), excepto en el campo horario, donde debe ser posible definir un rango de tiempo como criterio de búsqueda;
- Generar alertas automáticas vía:
    - Email;
    - SNMP;
    - Syslog;
- El equipo deberá soportar el envío de logs a un servidor externo syslog según RFC 3164.
- La plataforma de seguridad debe permitir a través de API-XML (Application Program Interface) la integración con sistemas existentes en el ambiente de contratación de forma que posibilite que aplicaciones desarrolladas por el cliente puedan interactuar en tiempo real con la Solución permitiendo así que Reglas y políticas de seguridad puedan ser modificadas por estas aplicaciones con la utilización de scripts en lenguajes de programación como Perl o PHP.

REQUERIMIENTOS DE LA SOLUCION DE SOAR

- La Solución debe soportar investigaciones interactivas que permitan la colaboración, la revisión histórica y la documentación en tiempo real de todas las acciones.
- La Solución debe soportar flujos de trabajo y secuencias de comandos modulares

- **Automatización**
    - La herramienta de SOAR debe automatizar las tareas básicas de respuesta a incidentes, haciendo que sus analistas sean más eficientes y efectivos.
    - La plataforma debe soportar investigaciones interactivas que permitan colaboración, revisión histórica y ejecución en tiempo real y documentación de todas las acciones.
    - Para cualquier acción de seguridad, debe ofrecer flexibilidad para automatizar o manualmente ejecutar en tiempo real según los requisitos del caso de uso.
    - La automatización se debe lograr utilizando flujos de trabajo modulares y scripts.
    - Las tareas automatizadas se deben visualizar en flujos de trabajo basados en interfaz gráfica y ser impulsadas por scripts de automatización en el backend.
    - Cualquier script puede ser adjunto a una tarea automatizada dentro de flujos o playbooks visuales.
    - Los flujos de trabajo que la plataforma de SOAR utilza para automatizar y ejecutar acciones deben ser compatible al menos con Python y JavaScript, debe tener la capacidad de exportar paquetes de Python a Dockers para que librerias de Python existentes puedan ser reutilizadas.
    - Debe incluir una función "BYOI" o similar que permita a los analistas escribir sus propias integraciones a través de un SDK interno y un wizard.

- La Solución debe incluir nuevas integraciones de productos y automatizaciones automáticas como parte de actualizaciones de contenido.
- La Solución debe integrar las funciones de TIM (Threat intelligence Management). Deberá Automatizar y Orquestar las labores de un equipo de Threat Intel.

- **Integraciones**
  - Herramientas forenses: Debe integrarse con un mínimo de 20 herramientas de anti-malware y forense, entre ellas Any.Run, CheckPoint Sandblast Appliance, CheckPoint Sandblast Cloud Services, McAfee Advanced Threat Defense, Palo Alto Networks WildFire, Rekall, VMRay, etc.
  - Herramientas TI: Debe integrarse con un mínimo de 30 servicios de TI, incluidos Box, Cisco Meraki, EasyVista, McAfee Web Gateway, Skyinformation.
  - Herramientas Colaboración: Debe integrarse con un mínimo de 20 herramientas de colaboración incluidas ActiveMQ, Cisco Webex Teams, EWS, FCM PushNotificaciones, Kafka, etc.
  - Herramientas SIEMs: Debe tener integraciones bidireccionales con APIs de SIEM terceros, la herramienta debe recolectar incidentes desde los SIEM, buscar alertas del SIEM durante una investigación y actualizar el SIEM de ser necesario. Debe integrarse con al menos 30 soluciones de SIEM o analítica de logs, entre ellos ArcSight, RSA Netwitness, IBM Qradar, Securonix, Exabeam, LogRythm, Splunk, JASK, ELK, McAfee ESM y AlienVault
  - Endpoint Security: Debe integrarse con soluciones de punto final, incluidas McAfee, Symantec, Trend, FireEye, Crowdstrike, Cortex XDR, Cylance, Sentinel One, Cisco AMP, CybeReason y muchos más. Debe utilizar los APIs de las soluciones para hacer consultas en los productos, desencadenar nuevos incidentes, y activar acciones como parte de las acciones de respuesta (como por ejemplo aislar al punto final o matar procesos).
  - Seguridad de red: Debe integrarse con productos de seguridad de Red a través de API bi-direccionales pararealizar acciones de prevención tales como agregar reglas y desplegar IOCs. Los productos compatibles deben incluir marcas líderes del mercado como, Check Point, Forcepoint, Cisco, Palo Alto Networks, Fortinet y otros. Debe ofrecer la capacidad de agregar mas productos de ser necesario.
  - Directorio Activo: Debe proveer todas las acciones permitidas por Directorio Activo via API. Debe incluir consultar info acerca de usuarios, maquinas, contraseñas que expiran, control de afiliaciones a grupos, etc. Debe integrarse con servidores de email, permitiendo leer los buzones de correo entrante como enviar correos, actualizar usuarios, pedir aprobaciones, ejecutara tareas basadas en respuestas a correos, etc.
  - Threat Intelligence: Debe contar con más de 70 integraciones para enriquecimiento de datos y Inteligencia de amenazas, incluidas todas las principales plataformas de inteligencia de amenazas, incluidos AlienVault, AWS Sagemaker, Anomali, Cisco Umbrella, Palo Alto Networks Autofocus, etc
  - Análisis de malware dinámico: Debe integrarse con productos relacionados con análisis de malware. Debe incluir Lastline, MISP, CrowdStrike, Falcon Sandbox, Palo Alto Networks WildFire y otros.
  - Análisis de Vulnerabilidades: Debe ser compatible con soluciones de assesment de vulnerabilidades como Nssus, Rapid7 y Qualys para proveer enriquecimiento de la información y para disparar acciones de parchado de vulnerabilidades. Debe incluir integraciones con herramientas de monitoreo

de nube, como GuardDuty, AWS Security Hub, servicios de compliance como Palo Alto Networks Prisma, servicios de TI (S3, EC2), loggign (CloudTrail, CloudWatch) y otros.
    - Sistemas Desarrollados localmente: Debe permitir crear integraciones propias o customizadas con soluciones locales (home-grown) (ej. portales internos y sistemas de tickets de soporte).

- **Indicadores de compromiso**
    - La Plataforma debe poder admitir formatos de código abierto estándar como OpenIOC, Yara, STIX 1.0, STIX 1.2, STIX 2.0, XML, CSV, JSON
    - La Plataforma debe tener la capacidad de mapear datos de origen al modelo interno de datos TIP y clasificar los datos con una combinación de valores de hash, incluidos MD5, SHA1, SHA256 y SHA512
    - La plataforma debe poder mapear los IOC que ingiere al TTP, y puede mapear el TTP a grupos APT para reducir a cero los grupos APT dirigidos a su organización.
    - La plataforma debe facilitar la atribución de amenazas con nombre: mapeo de TTP a actores de amenazas, grupos, y el marco de Mitre Att&ck
    - La plataforma debe poder admitir indicadores personalizados como IBAN, tarjetas de crédito, números de teléfonos celulares y números de identificación
    - La plataforma deberá recopilar indicadores de compromiso de muchas fuentes diferentes y deducir, según el valor de cada indicador, manteniendo el contexto de cada fuente.
    - Debe permitir al analista buscar indicadores en función de campos como etiquetas, estado o tipo de indicador para llevar a cabo acciones determinada
    - La plataforma debe automatizar la consolidación de la normalización tanto desde herramientas internas como externas para responder a los ataques en tiempo real
    - La plataforma debe realizar la des duplicación automática de indicadores
    - La plataforma debe admitir la inclusión de indicadores internos como IP y URL en la lista blanca, para garantizar que no sean marcados como maliciosos

- **Flujos o playbooks de automatización**
    - La herramienta debe contar con un mínimo de 200 casos de usos y playbooks de respuesta a incidentes
    - Los playbooks deben ser de código abierto y están alojados en GitHub o un repositorio público.
    - Debe permitir crear playbooks copiando flujos existentes, debe poseer una interface sencilla de utilizar que permita realizar drag-and-drop de acciones u otros flujos/playbooks
    - Debe permitir embeber un playbook dentro de otro, de forma de que este sea reutilizado continuamente
    - Un playbook puede contener acciones totalmente automatizadas o tareas manuales, tareas de collection de datos o tareas condicionadas
    - Los playbooks pueden ser ejecutadas automáticamente al crear un incidente y asociando al playbook correspondiente
    - Los playbooks deben poder ser ejecutados como tareas y también ejecutados en tiempo real
    - La ejecución de los playbooks y la actividad relacionada por en analista debe ser automáticaente documentada para cada incidente de seguridad

- La herramienta debe de tener la capacidad de ejecutar flujos/playbooks en modo debug, de tal forma que permita observar la ejecución paso a paso del mismo y resolver cualquier inconveniente de ser necesario
- Las acciones de los playbooks deben ser totalmente personalizables por el usuario y deben poder utilizarse para adherirse a cualquier requisito de proceso organizacional o industrial.
- Debe poseer la capacidad de asignar a cualquiera de los usuarios disponibles en el
- sistema basado en las capacidades RBAC.
- La herramienta debe tener un API capaz de ejecutar las mismas funciones que la interfaz gráfica

- **Gestión de Incidentes**
  - La herramienta debe integrarse con sistemas de ticketing de TI, debe ser compatible con Jira, ServiceNow, HP Service Manager, Remedy, etc).
  - Los usuarios pueden hacer comunicación bi-direccional con estas herramientas para iniciar acciones de creación de notificaciones (tickets) como también buscar y actualizar notificaciones(tickets) con información de investigación
  - La herramienta debe proveer con una herramienta de ticketing de propósito específico de respuesta a incidentes
  - La herramienta debe soportar la asignación de tickets a usuarios o equipos de trabajo a través de roles de capacidad. Los incidentes pueden ser asignados a un equipo a través de un rol de grupo.
  - La herramienta debe estandarizar o escalar la administración de SLAs
  - Debe manejar campos obligatorios a ser llenados antes de cerrar un incidente de seguridad
  - Debe enviar notificaciones mediante herramientas de integración de mensajes tales como Okta, Slack y correos sobre cambios en incidentes changes, alertas sla, etc.
  - La notificación debe poder enviarse como parte de los pasos del playbook.
  - La herramienta debe poder enviar recordatorios para las tareas mientras se crea el playbook. Debe poder fijar SLA y usuario mientras se crea el playbook
  - Los incidentes pueden ser generados usando fetch trigger en cualquiera de los productos integrados o usando un modelo de push mediante Rest API, adicionalmente también pueden ser creados manualmente.
  - Debe ser posible conectar o marcar incidentes como duplicados. Debe poseer un aprendizaje automático para calcular la similitud de incidentes basado en datos de investigación.
  - Debe ofrecer una visión optimizada de como se relacionan los ataques en el tiempo, personalizar esa visión para adecuarse a su línea de trabajo, y codificar sus perspectivas para abordar de una mejor manera incidentes similares en el futuro.
  - Debe poseer la capacidad de asignar tags o características personalizables a los incidentes, estas características deberán poder utilizarse para distintos usos, entre ellos medir KPIs, medir estadísticas, ejecutar atomizaciones basadas en ellas, etc.
  - La Solución debe permitir la delegación de tareas a otro usuario y asignar SLAs

- **Documentación**

- La herramienta debe incluir una instancia donde usuarios puedan ver evidencia y documentación de incidentes anteriores, la herramienta debe agregar información de investigaciones pasadas
- Debe incluir un War Room donde los incidentes se auto-documenten, ofreciendo una vista detallada de registros basada en una línea de tiempo con cada actividad realizada durante la investigación de un incidente
- La herramienta debe detectar alertas redundantes y agregar incidentes duplicados en uno solo, desplegando los datos de la agregación realizada
- Como parte de un incidente, la herramienta debe documentar cualquier cambio, los analistas parte del incidente, tareas terminadas, comandos de interacción, evidencia, chats, notas y tareas de playblooks
- Los usuarios pueden marcar resultados de comandos o notas como evidencia, o automatizar la recolección de evidencia dentro de un playbook.
- Toda la información recolectada debe ser inmutable y no debe ser modificada, la documentación debe ser exportable para producir un documento de cadena de custodia
- Los analistas deben poder ver todos los indicadores de compromiso y el detalle alrededor de ellos deben poder asociados a las distintas fases del ataque o kill chain
- Los avalistas deben ser capaces de utilizar campos customizados para por ejemplo atribuir indicadores a campañas de ataque

- **Colaboración**
  - El producto debe proveer herramientas de colaboración en tiempo real entre usuarios, debe agrupar a todos los usuarios asociados a un incidente dentro del mismo o en un cuarto de guerra
  - Debe integrarse con Slack, para que los usuarios de Slack puedan interactuar con los analistas de forma sencilla y ágil
  - Los analistas deberán poder colaborar uno con otro usando la línea de comando dentro de la investigación de un incidente
  - La colaboración puede ser extendida a grupos o equipos de trabajo terceros, como usuarios internos, grupos de recursos humanos, PR, o terceros.
  - Las tareas realizadas dentro de incidentes deben de ser respaldadas para que sirvan de documentación para entrenar a nuevos analistas
  - La herramienta debe incluir un Canvas o mapa de investigación, el cual mediante machine learning pueda crear un mapa de ataques en tiempo real
  - Los resultados de los canvas deben ser exportados y compartidos por equipos ejecutivos e interesados

- **Repositorio de indicadores**
  - El producto debe correlacionar bidireccionalmente indicadores e incidentes. Los usuarios deben poder ver todos los indicadores de un incidente y viceversa
  - La plataforma debe incluir playbooks de threat hunting, que puedan ser ejecutados utilizando indicadores de compromiso
  - Debe ser posible importar y exportar indicadores en archivos STIX y JSON
  - Debe poseer la capacidad de customizar la estructura de la información de los indicadores
  - La plataforma debe poder crear whitelist so listas blancas de indicadores

- **Machine Learning**

- La Solución debe incluir aprendizaje dinámico de los IOCs e incidentes que se investigan y ayudar a los analistas a identificar incidentes que pueden estar relacionados
- La Solución debe se capaz de sugerir próximos pasos de acuerdo con el aprendizaje de máquina realizado durante investigaciones previas.
- Debe ser capaz de aprender qué analistas son contactados usualmente por tipo de incidente y puede sugerir a los nuevos analistas a quien ellos pueden querer contactar para recibir ayuda.

- **Arquitectura y administración**
  - La Solución debe soportar un despliegue on-premise permitiendo que toda la data que se produzca en la organización no salga de las premisas
  - La Solución debe soportar un despliegue en nube, capaz de conectarse a las premisas del cliente
  - La Solución debe ofrecer Control de Acceso Basado en Rol (RBAC por sus siglas en idioma inglés) así como también el mapeo de roles a los grupos en el Directorio Activo o SAML. Los roles se corresponden con permisos granulares con inclusión de leer/escribir, leer solamente, y acceso denegado a varias áreas de la Solución
  - Debe soportar multi-tenancy, donde una cuenta maestra puede administrar y ver a todos los tenants, mientras que cada tenant trabaja de forma autónoma y no puede ver los datos de otros tenants.
  - Debe incluir la capacidad de generar informes de incidentes, informes de estadísticas (tales como MTTR – tiempo medio de reSolución) y los resúmenes o informes por incidente.
  - Debe soportar informes programados y asociarse a una lista de distribución de correos, y el motor de informes debe ser compatible con formatos PDF, DOC y CSV.
  - Debe ofrecer monitoreo y gráficos enfocados tanto a los analistas, así como a los incidentes, con el objetivo de que los CISOs y gerentes puedan medir la salud del SOC, productividad de los analistas y severidad y alcance de incidentes
  - La Solución debe ser Multi-tenant, asegurando que cada tenant tenga su propia infraestructura y que sus datos no se mezclen entre si.
  - La plataforma no limita el número de acciones, tareas, incidentes, indicadores, playbooks u otra acción operativa. La licencia debe basarse en sólo en Usuarios Nombrados.
  - La plataforma debe realizar procesos automáticos preventivos y proactivos. Estos procesos deben ejecutarse con una frecuencia programada y sin necesidad de que un incidente se manifieste como tal.
  - La función de Live Backups debe ser soportada.
  - Con el fin de realizar desarrollos de manera segura la Solución deberá contar con un ambiente de desarrollo ajeno al ambiente de producción.

- **Modulo de gestión de Inteligencia de Amenazas (TIM)**
  - La Solución de SOAR deberá contar con un módulo que gestione la ingesta de indicadores de amenazas conocidos comúnmente como Feeds. La plataforma deberá contar con playbooks capaces recibir estos indicadores y procesarlos de manera automática. De esta manera los indicadores se encontrarán fusionando de inmediato una ves recibido.
  - La plataforma de SOAR deberá proporcionar una fuente de amenazas de alta calidad propia e integrar fuentes de terceros.
  - El módulo de Threat Intelligence deberá:

- Hacer control sobre la ingesta de fuentes de amenazas y puntuación de amenazas: La combinación del módulo de TIM con SOAR deberá proporcionar a los usuarios la capacidad de hacer que los datos de amenazas sean procesables para búsqueda y respuesta.
- Personalizar la visualización de los indicadores: Deberá proporcionar formas escalables y personalizables para ver los datos de información sobre amenazas, permitiendo a los usuarios obtener un contexto de datos procesables.
- Integraciones abiertas y extensibles: La plataforma deberá permitir a los usuarios editar integraciones de productos de terceros existentes, así como agregar nuevas integraciones por sí mismos.
- Convergencia de incidentes y datos de indicadores: la plataforma deberá grabar y capturar automáticamente todos los indicadores presentes en los incidentes ingeridos.

- La integración del módulo de Threat Intelligence y la plataforma de SOAR deberá ser cien por ciento integrable. Deberá trabajar coordinadamente con mínimo esfuerzo por parte del Analista y máximo beneficio.
- A continuación, se enumeran las características debidas y deseables en relación con las funciones de inteligencia de amenazas de SOAR.

- **Automatización**
  - La plataforma permitirá ejecutar playbooks frente a un conjunto de indicadores especificados por el usuario. La plataforma también permitirá a los clientes dirigir indicadores hacia dispositivos de seguridad de tercero
  - La Plataforma permitirá a los clientes ejecutar playbooks personalizadas ante indicadores nuevos/editados/quitados
  - La plataforma proporcionará diversos playbooks listos para usar, para análisis de inteligencia de amenazas. Por ejemplo, análisis de indicadores en masa.
  - La plataforma permitirá ver y personalizar todos los códigos fuente de automatizaciones, en caso de ser necesario

- **Ingesta y Fuentes**
  - La plataforma debe permitir a los usuarios filtrar el listado de integraciones basadas en sus funcionalidades
  - La Plataforma deberá soportar formatos estructurados como JSON, CSV, STIX 1.X & STIX 2.X, etc. Y además deberá soportar formatos no estructurados como correo electrónico, noticias, fuentes RSS, entre otras.
  - La Plataforma deberá recopilar fuentes de amenazas de una combinación de fuentes comerciales, de código abierto, creadas por el usuario y de intercambio de la Comunidad.
  - La Plataforma Threat Intelligence deberá contar con la capacidad de crear incidentes en la plataforma SOAR, lo cual permita al usuario responder usando la plataforma SOAR. SOAR & TI deberán combinarse en una sola plataforma que permita que diferentes equipos de seguridad (SOC, IR, TI) trabajen en una plataforma en común
  - La paltaforma deberá soportar distintos tipos de datos. A modo de referencia se citan algunos de ellos: STIX, JSON, datos de tarjetas, IBAN, contactos, correos electrónicos, etc.
  - Cuentas, puntuación CVE, CVSS, dominios, FQDN, corros electrónicos, scripts para mejora de archivos, host, nombre de host, IP, clave del registro,

reputación de la ruta de acceso del registro, archivo, URL, nombre de usuario, CIDR, IPv6, IPv6 CIDR
- La plataforma de Threat Intelligence deberá proporcionar integraciones de fuentes listas para usar para HTTP, TAXII, CSV, etc. La plataforma también admitirá múltiples técnicas de autenticación, como autenticación básica, certificada, clave API, etc.
- La Plataforma deberá admitir formatos de código abierto estándar como OpenIOC, Yara, STIX 1.0, STIX 1.2, STIX 2.0, XML, CSV, JSON, etc
- La Plataforma deberá tener la capacidad de mapear datos de origen al modelo interno de datos Treath Intelligence. Deberá contar con un indicador de “archivo” que combina múltiples valores de hash, incluidos MD5, SHA1, SHA256 y SHA512.
- La plataforma podrá mapear los IOC que ingiere al TTP, y puede mapear el TTP a grupos APT para reducir a cero los grupos APT dirigidos a su organización.
- La plataforma admitirá indicadores personalizados como IBAN, tarjetas de crédito, números de teléfonos celulares y números de identificación
- La plataforma deberá contar con una sección que resuma todos los datos sobre un indicador a modo de resumen.
- La plataforma recopilará indicadores de compromiso de muchas fuentes diferentes y deducirá, según el valor de cada indicador, mientras mantiene el contexto de cada fuente. De esa forma, los indicadores se podrán enviar a herramientas de terceros para bloquear/alertar flujos de trabajo.
- La plataforma recopilará indicadores de compromiso de muchas fuentes diferentes y deducirá, según el valor de cada indicador, mientras mantiene el contexto de cada fuente. De esa forma, los indicadores se pueden enviar a herramientas de terceros para bloquear/alertar flujos de trabajo.

SERVICIO DE IMPLEMENTACIÓN

- Deberán incluir la Instalación, Configuración, Puesta en Marcha y Prueba de la SOLUCIÓN DE INTEGRAL para los TRES (3) Centros de Datos
- Luego del perfeccionamiento contractual, se convocará al Oferente a una REUNIÓN DE INICIO DEL PROYECTO, donde:
  - Se especificará las prioridades, validaciones y aprobaciones técnicas de los entregables del proyecto.
  - Se acordará en detalle la metodología de trabajo y el uso de las Herramientas de seguimiento y control.
  - Los acuerdos establecidos en las reuniones deberán quedar debidamente documentados, firmados y aprobados por todos los participantes.

Plan de instalación

- Dentro de los SIETE (7) días del perfeccionamiento contractual, el Oferente deberá presentar un PLAN DE INSTALACIÓN, que deberá aprobar SOFSE, el mismo deberá cubrir todas las tareas a llevar a cabo hasta la puesta en marcha de los bienes, tales como:

a) Instalación de los equipos y software ofertados.
b) Instalación de programas y dispositivos.
c) Conexión de los equipos.
d) Configuración de los equipos y software ofertados.
e) Procedimientos de backup y recovery.
f) Procedimientos de verificación y de testeo.
g) Documentación para entregar.
h) Toda otra actividad que sea conveniente planificar.

- En dicho plan se deberán establecer plazos mínimos y máximos para cada una de las tareas a cumplir, debiéndose discriminar las que deberá cumplir SOFSE, el Oferente en forma exclusiva, y las que deberán asumir en forma compartida.
- Juntamente con el PLAN DE INSTALACIÓN, el Oferente deberá presentar un detalle de las especificaciones técnicas a cumplir por las instalaciones físicas necesarias para el montaje y correcto funcionamiento de los equipos y/o programas a instalar. De surgir algún inconveniente en la instalación de los bienes originada por una incorrecta especificación técnica, SOFSE no aceptará reclamos ni justificará fallas en los equipos y/o programas instalados, por lo que de producirse alguna de estas situaciones, resultarán de automática aplicación las disposiciones que por atrasos, fallas, etc., se establezcan a esos efectos**.**

Puesta en marcha

- Se entenderá por Puesta en Marcha, la ejecución exitosa por parte del Oferente (con la colaboración activa del personal de SOFSE), de las siguientes tareas:
  a) Instalaren el rack respectivo, conectar a los sistemas de alimentación eléctrica, de tierra y configurar los equipos que conforman la Solución de NGFW y que deberán ser instalados por el Oferente.
  b) Configurar los equipos de acuerdo con las especificaciones entregadas por SOFSE con anterioridad a la puesta en marcha, incluyendo la configuración de una política básica en una aplicación.
  c) Realizar el Backup de todos los sistemas y bases de datos que corresponda, con prueba de restauración.

Prueba de la Solución

- El Oferente deberá facilitar los medios necesarios para que SOFSE pueda verificar el correcto funcionamiento de la totalidad del equipamiento ofrecido y el cumplimiento de todas las especificaciones referidas en el presente pliego.
- SOFSE realizará las pruebas necesarias para constatar que los bienes entregados (hardware y software) recibidos se ajustan en su totalidad a las especificaciones técnicas y prestaciones adicionales ofrecidas por el Oferente en su oferta.

SERVICIO DE CAPACITACIÓN

- Se deberán incluir el Servicio de Capacitación de la Solución.
- El Servicio de Capacitación deberá incluir cursos aprobados por el fabricante de la Solución.
- Finalizada la capacitación se entregará un certificado de asistencia firmado por el Oferente
- El Servicio de Capacitación deberá incluir prácticas en plataformas.
- El Servicio de Capacitación deberá permitir, que el personal de SOFSE posea los conocimientos suficientes para efectuar en tiempo y forma y sin ayuda externa, las siguientes tareas para la totalidad de la Solución:

a) Instalación
b) Configuración y parametrización
c) Administración y puesta a punto
d) Operación y mantenimiento
e) Generación y prueba de backup

- Para fortalecer la Transferencia Integral de Conocimientos, el personal de SOFSE participará activamente en la instalación y configuración inicial de la Solución de NGFW adquirida, aun cuando la responsabilidad total de esta tarea se mantiene en el Oferente.
- Los cursos deberán ser dictados en idioma castellano, por profesionales certificados por las empresas desarrolladoras del software contratado.
- Si en el marco de la Emergencia Sanitaria COVID-19 no fuera posible la capacitación en modalidad presencial, a pedido de SOFSE se deberá dictar en modalidad virtual.
- Asistentes: DIEZ (10) agentes
  - Duración Mínimo de CUARENTA (40) horas.
- Temario
  - Temario mínimo:
    a) Arquitectura y diseño de los equipos provistos.
    b) Instalación física de los equipos suministrados en la provisión.
    c) Administración del Software de los equipos suministrados en cuanto a Sistema Operativo, imágenes de Software requeridas para su funcionamiento, file systems, systems logs, etc.
    d) Configuración de todas las funcionalidades existentes en los equipos provistos.
    e) Optimización del funcionamiento (tunning), Solución de inconvenientes (troubleshooting), sistemas de calidad de servicio, etc.
    f) Manejo integral del sistema de administración y de los equipos y su utilización en la determinación de problemas.
- Las fechas de los cursos serán coordinadas por SOFSE en conjunto con el Oferente.

Artículo 5°. - SERVICIOS CONEXOS DE SOPORTE TÉCNICO Y GARANTIA

- Todos los servicios necesarios para cumplir con lo solicitado a continuación se considerarán integrados a la oferta y no se admitirán adicionales por ningún concepto.
- El Soporte Técnico y Garantía ofrecido para la Solución deben tener vigencia de TRES (3) años en la modalidad 7x24.
- Los servicios que requieran asistencia presencial, deberán ser prestados en los sitios determinados para la instalación de los equipos, de acuerdo a la solicitud de la prestación del servicio.
- El servicio de Soporte Técnico será integral.
- Los servicios requeridos alcanzan a cualquier tipo de desperfecto, funcionamiento anormal, o fuera de servicio total o parcial, que ocurra sobre los bienes objeto de la presente, durante el plazo previsto y cualquiera fuese la causa que origine el desperfecto, funcionamiento anormal, o fuera de servicio, total o parcial.
- Entiéndase por desperfecto, funcionamiento anormal, o fuera de servicio, total o parcial, a cualquier tipo y clase de evento que no permita que los bienes requeridos, en forma conjunta o separada, puedan cumplir el desempeño deseado según las especificaciones técnicas realizadas.
- Todo el trabajo realizado por el Oferente será ejecutado con razonable habilidad y cuidado, y al menos con los niveles de habilidad y cuidados esperables de

diseñadores y programadores competentes experimentados en los lenguajes de programación, herramientas y aplicaciones prácticas.

- El servicio requerido no deberá caducar, extinguirse, o modificarse bajo ningún concepto debido a la manipulación o reemplazo de partes, operación o administración del sistema por parte de la SOFSE.
- En caso de que el Oferente no pudiera concretar la reparación de los bienes dentro de los plazos estipulados deberá solucionar el inconveniente mediante el reemplazo de los bienes afectados por otros en condiciones de buen funcionamiento, sin que esto implique costo alguno para la SOFSE.
- La cantidad de incidentes a reportar y resolver deberá ser ilimitada.
- Solicitudes de servicio de soporte técnico
  - Soporte técnico On- line software y hardware
  - Tiempo de reparación/reSolución: El plazo para la reSolución del problema reportado, deberá responder al siguiente detalle, de acuerdo con la criticidad reportada y definida exclusivamente por la SOFSE:

NIVEL DE CRITICIDAD	TIEMPO MÁXIMO DE REPARACIÓN	IMPACTO	DETALLE DEL IMPACTO
1	DOS (2) horas corridas	MUY ALTO	Solución detenida, fallas de componentes vitales o de al menos dos componentes redundantes del sistema que produzcan indisponibilidad o falla del mismo.
2	OCHO (8) horas corridas	ALTO	Solución no detenida, falla en componentes vitales solucionable en forma transitoria y no definitiva.
3	VEINTICUATRO (24) horas corridas	MEDIO	Solución no detenida, falla de componentes no vitales que requieren Solución no inmediata
4	SIETE (7) días corridos	BAJO	Problemas en nuevos componentes o funciones no utilizables aún en el ambiente de producción
5	VEINTE (20) días corridos	MUY BAJO	Consultas por nuevos componentes o funciones no utilizables aún en el ambiente de producción

  - Por reparación se entiende que el bien reparado, cualquiera fuese su especie, funcione u opere en las mismas condiciones que las exigidas en estas especificaciones, incluyéndose la puesta en operación del software, de ser necesario.
  - SOFSE podrá efectuar solicitudes de servicio a los efectos de garantía y soporte técnico durante las 24 horas los 365 días del año.
- En relación con el RMA el fabricante debe contar con depósito de partes, o equipos completos con presencia local en el país y poder ofrecer mínimamente remplazo de partes en el próximo día hábil, conocido por las siglas en ingles NBD (next business day), para poder garantizar el funcionamiento de la Solución.
  - El Sistema de Reclamos deberá:
    a) Asignar automáticamente un número de reclamo único por cada solicitud. Realizar la colocación y el seguimiento del estado de

reclamos por inconvenientes.

b) Registrar cada evento relacionado con cada uno de los reclamos efectuados. Por cada evento permitirá conocer el personal y área interviniente, fecha y hora, tarea efectuada, hora de derivación.
c) Actualizar las acciones adoptadas en tiempo real, permitiéndole al administrador de la SOFSE el seguimiento de dicho reclamo.
d) Permitir que el Oferente efectúe el cierre de los reclamos (previa conformidad de personal de la SOFSE, una vez recibido el aviso por parte del Oferente, debiendo quedar constancia). Si el problema fue solucionado, se tomará como hora de cierre, la del aviso del Oferente, caso contrario seguirán corriendo los tiempos desde la apertura del reclamo.

- En el caso de proveer una interfaz web, la misma deberá:
  a) Permitir controlar el acceso al mismo a través de usuarios y contraseñas, con distintos niveles de usuario. Las contraseñas podrán ser cambiadas por personal de la SOFSE cuando éstos lo consideren necesario. deberá poseer acceso mediante interfaces de cliente HTML sin limitación en la cantidad de usuarios simultáneos.
  b) Contar con un sistema de auditoría, el cual podrá ser consultado por personal de la SOFSE autorizado.
  c) Tener la posibilidad de exportar los registros de los eventos a un formato texto con delimitadores.

Artículo 6°. - REQUISITOS DE LOS BIENES OFERTADO:

Si se dejara de comercializar el bien durante el periodo entre la presentación de la Oferta y su correspondiente entrega, la empresa adjudicataria deberá reemplazar por el comercializado, el que deberá poseer características técnicas iguales o superiores al ofertado. Sin costo adicional para Sofse.

Ese reemplazo deberá ser previamente autorizado por quien realice el dictamen técnico.

Artículo 7°. – CONFIDENCIALIDAD DE LA INFORMACION:

La empresa adjudicataria se compromete a no divulgar la información no publicada o de carácter confidencial a la que haya tenido acceso con motivo de la ejecución de las obligaciones emanadas de la presente licitación.

Todo acceso a la infraestructura tecnología de información que la adjudicataria requiera para cumplir con la prestación establecida en el presente pliego será otorgado de acuerdo a normas y procedimientos establecidos por SOFSE y sujeto al análisis, aprobación y supervisión del personal especializado de la Gerencia de Tecnologías de la Información e Innovación y Telecomunicaciones “GTIIT”

La adjudicataria declara observar el cumplimiento de la Ley de Protección de Datos Personales, así como el régimen Legal de la Propiedad Intelectual y todas las normas

legales aplicables en el marco de la ejecución de las obligaciones establecidas en la presente licitación.

Artículo 8°. – CERTIFICACION:

Está previsto realizar certificaciones parciales tomando como referencia el cumplimiento total de cada HITO solicitado en la apertura de costos “ANEXO B”.

Artículo 9°. - REQUISITOS DEL OFERENTE:

El Oferente debe acreditar experiencia para la oferta a proveer, para ello deberá:

- Acreditar documentalmente estar radicado en la República Argentina, con no menos de TRES (3) años de antigüedad previos a la presentación de la oferta.

- Acreditar documentalmente que el oferente es canal certificado de la marca solicitada presentando una nota del Fabricante que los acredite como Reseller Certificado para comercializar los productos de la marca y mencionando esta licitación en particular.

- Informar, en carácter de declaración jurada, al menos DOS (2) participaciones en ofertas similares, de la misma marca propuesta, con el siguiente detalle por cada cliente: razón social, contacto, teléfono, mail y equipos ofertados.

- El Oferente deberá presentar los antecedentes de los ingenieros que realizaran la instalación debiendo estar certificados por el fabricante.

En todos los casos la documentación que se acompañe deberá estar redactada en idioma nacional. En caso de que la documentación esté redactada en idioma extranjero SOFSE podrá solicitar la correspondiente traducción, realizada por traductor publico matriculado.

ANEXO “A” - PLANILLA DE COTIZACION

TRENES ARGENTINOS
OPERACIONES

OPERADORA FERROVIARIA S. E. – SOFSE -

SOLUCIÓN DE SEGURIDAD INTEGRAL PARA REDES CON CARACTERÍSTICAS DE NEXT GENERATION FIREWALL (NGFW)

PLANILLA DE COTIZACIÓN

RAZON SOCIAL:	FECHA
CUIT:	PRESUPUESTO N°
DIRECCION – CIUDAD – C.P:	MONEDA
EMAIL – CONTACTO:	CONDICION DE PAGO (*)

RENGLON		U.M	CANT.	VAL. UNIT. S/IVA	VAL. TOT. S/IVA
1	SOLUCIÓN DE SEGURIDAD INTEGRAL PARA REDES CON CARACTERÍSTICAS DE NEXT GENERATION FIREWALL (NGFW)	C/U	1		
				SUBTOTAL	
				IVA___%	
				TOTAL	

Celdas que deben ser completadas por el oferente

CARGO/ FIRMA Y ACLARACION

El oferente deberá presentar junto con la “Planilla de cotización” una planilla de apertura de costos en la cual deberá agrupar los mismos en cuatro Hitos, indicando los totales cada por uno. En todos los casos los precios deberán expresarse discriminando el impuesto al valor agregado

* Equipamiento.

* Licenciamiento.

* Servicios profesionales de implementación.

* Servicios de Capacitación.

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2022-47591596-APN-GTIIYT#SOFSE

CIUDAD DE BUENOS AIRES
Jueves 12 de Mayo de 2022

Referencia: PET - SOLUCION INTEGRAL NGFW

El documento fue importado por el sistema GEDO con un total de 35 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.05.12 13:13:10 -03:00

Federico Baseggio
Supervisor Técnico
Gerencia Tecnología de la Información e Innovación y Telecomunicaciones
Operadora Ferroviaria Sociedad del Estado

Digitally signed by Gestion Documental Electronica
Date: 2022.05.12 15:10:09 -03:00

Leonel Hernan Miglioli
Gerente
Gerencia Tecnología de la Información e Innovación y Telecomunicaciones
Operadora Ferroviaria Sociedad del Estado

Digitally signed by Gestion Documental Electronica
Date: 2022.05.12 15:10:10 -03:00