ANEXO TÉCNICO

Los oferentes interesados en participar en el actual proceso se obligan para con la UPRA a cumplir y desarrollar cada una de las siguientes especificaciones técnicas mínimas.

1. NOMBRE DEL PRODUCTO:	Adquirir un firewall y licencias de antivirus para la protección de la red de datos perimetral y de los equipos endpoint que forman parte de la infraestructura tecnológica de la UPRA.
2. IDENTIFICACIÓN COMERCIAL DEL PRODUCTO:	**43222501:** Difusión de Tecnología de Información y Telecomunicaciones, Equipos o plataformas y accesorios de redes multimedia o de voz y datos, Equipo de seguridad de red, Equipo de seguridad de red cortafuegos (firewall). **43222644:** Difusión de Tecnología de Información y Telecomunicaciones, Equipos o plataformas y accesorios de redes multimedia o de voz y datos, Equipo de servicios de red, Controlador de tráfico de red. **43231513:** Difusión de Tecnología de Información y Telecomunicaciones, Software, Software funcional específico de la empresa, Software para oficinas **43233205:** Difusión de Tecnología de Información y Telecomunicaciones, Software, Software de seguridad y protección, Software de seguridad de transacciones y de protección contra virus. **81111801:** Servicios basados en ingeniería, investigación y tecnología, Servicios informáticos, Servicios de sistemas y administración de componentes de sistemas, Seguridad de los computadores, redes o internet. **81111805:** Servicios basados en ingeniería, investigación y tecnología, Servicios informáticos, Servicios de sistemas y administración de componentes de sistemas, Mantenimiento o soporte de sistemas patentados o autorizados. **81111820:** Servicios basados en ingeniería, investigación y tecnología, Servicios informáticos, Servicios de sistemas y administración de componentes de sistemas, Servicios de funcionalidad del sistema. **81112200:** Servicios basados en ingeniería, investigación y tecnología, Servicios informáticos, Mantenimiento y soporte de software, Mantenimiento de software de protección y seguridad.
3. CALIDAD:	N/A
4. GENERALIDADES:	N/A
5. REQUISITOS:	
5.1. Adquirir un firewall y licencias de antivirus para la protección de la red de datos perimetral y de los equipos endpoint que forman parte de la infraestructura tecnológica de la UPRA.	

FICHA TÉCNICA CARACTERÍSTICAS DE FIREWALL	
REQUISITOS ESPECÍFICOS CARACTERÍSTICAS	**DESCRIPCIÓN DEL REQUERIMIENTO MÍNIMO Y/O TIPO DE SERVICIOS**
Equipo de alta disponibilidad	Activo/Activo - Activo/En espera
Plataforma de gestión	Plataforma de seguridad integrada y robusta hardware y software tipo appliance.
NGFW	Equipo de seguridad perimetral con características de Next Generation Firewall.
Prevención de intrusos de nueva generación (NGIPS)	Visibilidad profunda, inteligencia de seguridad preeminente y protección superior avanzada contra nuevas amenazas.
Protección frente a Malware avanzado.	Detección, análisis y detección de malware y de amenazas emergentes.
Throughput	1 Gbps con la funcionalidad de control de aplicaciones habilitada para todas las firmas que el fabricante posea.
	790 Mbps con las funcionalidades activas de manera simultanea para control de aplicaciones, IPS, antivirus, antispyware y logging de eventos, asimismo para todas las firmas que la plataforma de seguridad posea.
Throughput de inspección completa.	Monitoreo del estado de sesiones activas y filtradas de comunicaciones intuitivo. Throughput de 1.8 Gbps para este tipo de inspecciones.
Conexiones	Soporte como mínimo de 128.000 conexiones simultaneas.
	Soporte como mínimo de 8300 nuevas conexiones por segundo.
Capacidad de almacenamiento.	Disco de estado sólido con una capacidad mínima de 240 GB para sistema y logs.
Conexiones	4 interfaces de red 100/1000/10000 base-TX.
	8 interfaces de red 1 Gbps SFP.
	1 (una) interfaz dedicada para alta disponibilidad a 1 Gbps.
	1 (una) interface de red 1 Gbps dedicada para administración.
	1 (una) interfaz de tipo consola o similar.
	Soporte como mínimo de 10 (diez) ruteadores virtuales.
	Soporte como mínimo de 20 (veinte) zonas de seguridad.
	Estar licenciada para soportar sin uso de licenciamiento 1024 (mil veinticuatro) clientes de VPN SSL simultaneos.
	Estar licenciada para soportar sin uso de licenciamiento, 2.000 (dos mil) túneles de VPN IPSEC simultáneos.
FUNCIONALIDAD DE SEGURIDAD DE RED	

REQUISITOS ESPECÍFICOS CARACTERÍSTICAS	DESCRIPCIÓN DEL REQUERIMIENTO MÍNIMO Y/O TIPO TECNOLOGÍA
VLAN	Soporte a 4094 VLAN Tags 802.1q.
Enlaces	Agregación de links 802.3ad.
Políticas	Basada en routing o forwarding.
Ruteo	Multicast (PIM-SM);
DHCP	Relay.
	Server.
Capacidad MTU	Soporte Jumbo Frames.
Creación de objetos de red	La plataforma debe tener la capacidad de realizar la configuración de las interfaces l3 la creación automática de objeto de direcciones de red que coincidan con la red de dicha interfaz ó Soporte la creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3
Interfaces lógicas	Soportar sub-interfaces ethernet lógicas.
Soporte NAT	Nat dinámico (Many-to-1).
	Nat dinámico (Many-to-Many).
	Nat estático (1-to-1).
	NAT estático (Many-to-Many).
	Nat estático bidirecional 1-to-1.
	NAT de Origen.
	NAT de Destino.
	Soportar NAT de Origen y NAT de Destino simultaneamente.
Servicios de monitoreo	Enviar log para sistemas de monitoreo externos simultaneamente.
	Soporte para envío de logs para los sistemas de monitoreo externos vía protocolo TCP y SSL.
	Seguridad contra anti-spoofing;
Capacidad de enrutamiento	Para IPv4, debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
	Para IPv6, debe soportar enrutamiento estático y dinámico (OSPFv3).
	Soportar OSPF graceful restart.
Balanceo	Soportar el balanceo de varios enlaces de internet sin el uso de políticas específicas, permitiendo aplicar una variedad de algoritmos distintos (round Robin, weighted, etc).
Soporte IPv6	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, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Activo/Activo, Activo/Pasivo, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.
Monitoreo de red	Los dispositivos de seguridad deben tener la capacidad de operar de forma simultanea mediante el uso de sus interfaces físicas en modo sniffer (monitoreo y análisis del tráfico de red), Capa 2 (I2) y Capa 3 (I3).
	Modo Sniffer, para inspección via 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 mixto de trabajo Sniffer, L2 e L3 en diferentes interfaces físicas.
Disponibilidad Activo/Pasivo y 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-criptografados, asociaciones de seguridad de las VPNs y tablas FIB.
	El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link.
Control de aplicaciones.	Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decryption, SSL Inspection 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.
Servicios embebidos.	La identificación de usuarios, el control de aplicaciones, filtrado de datos, VPN, QoS, NATs y GeoLocalización debe de estar embebido en el sistema operativo, sin necesidad de una licencia que active las mismas.
CONTROL POR POLÍTICA DE FIREWALL	
Controles	Soportar controles por zona de seguridad.
	Soportar controles de políticas por puerto y protocolo.
	Soportar 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.

	Soportar control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.
	Soportar control de políticas por código de País (Por ejemplo: BR, USA, UK, RUS).
	Soportar control, inspección, SSL Inspection y desencripción de SSL por política para tráfico de entrada (Inbound) y Salida (Outbound).
Bloque de tráfico	Soportar el bloqueo de de archivos bat, cab, dll, exe, pif, y reg.
	Soportar tráfico shaping QoS basado en Políticas (Prioridad, Garantía y Máximo).
QoS	Soportar QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones.
Soporte de protocolos y funcionalidades	Soportar objetos y Reglas IPV6.
	Soportar objetos y Reglas multicast.
	Soportar los atributos de agendamento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.
	Permitir la detección de portales de phishing estableciendo políticas que bloquee el acceso a los mismos.
Soporte zonas horarias	Soportar la creación de políticas que soliciten un segundo factor de autenticación basadas en el origen (Usuario / Zona / Direcciones) y destino del tráfico (Aplicativos / Zonas / IP).
Filtrado de URL basado en la reputación	Análisis preciso de URLs y asignación de puntuación, con un margen de 280 millones más url categorizadas
Monitor, gestor y reporte de amenazas.	Sistema de administración de amenazas.
Herramienta de gestión	Gráfica y por CLI.
Soporte y alto desempeño Dual Stack IPv4 - IPv6	La solución debe certificada para el soporte y alto desempeño IPv6 e IPS por USGv6 o certificada por IPV6 Ready. Soporte en el filtrado con Dual Stack para los protocolos IPv4 e IPv6
Suscripción total para actualizaciones	IDS, IPS, URL, Parches de seguridad
3 años de garantía con soporte 7x24.	Directamente con el fabricante
CONTROL DE APLICACIONES	
Funcionalidades	Reconocimiento de aplicaciones independiente del puerto y protocolo.
	Soportar la liberación y bloqueo de aplicaciones sin la necesidad de habilitar de puertos y protocolos.
	Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, mas no limitado: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de

	red, voip, áudio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail.
	Reconocer por lo menos aplicaciones como 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.
	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 RDP en el puerto 80 en vez del puerto 389.
	Aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis comportamental del tráfico observado, incluyendo Encrypted Bittorrent y aplicaciones VOIP que utilizan criptografía proprietária.
	Identificar el uso de tácticas evasivas para visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas via comunicaciones criptográficas, tales como Skype y ataques mediante el puerto 443.
	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 Yahoo Instant Messenger usando HTTP. La codificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo 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.
	Identificar el uso de tácticas evasivas via comunicaciones criptográficas.
	Actualizar la base de firmas de aplicaciones automáticamente.
	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.
	Identificar al usuario de red con integración al directorio activo, sin la necesidad de instalación de agentes en el controlador de dominio ni en las estaciones de trabajo de los usuarios finales.
	Soportar la agregación de control de aplicaciones en todas las Reglas de seguridad del dispositivo.

	Soportar múltiples métodos de identificación y clasificación de las aplicaciones, por lo menos chequeo de firmas, decodificación de protocolos y análisis heurístico.
	Soportar nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la própria interfaz gráfica de la solución, sin la necesidad de acción por parte del fabricante.
	Alertar al usuario sobre aplicaciones bloqueadas.
	El control de puertos debe ser aplicado a todas las aplicaciones.
	Posibilitar la diferenciación de tráficos Peer 2 Peer (Bittorrent, emule,Posibilitar la diferenciación de tráficos Peer2Peer (Bittorrent, emule, neonet o Morpheus, etc.) proveyendo granularidad de control/políticas para los mismos.
	Posibilitar la diferenciación de tráficos de mensajería instantánea (AIM, Gtalk, Facebook Chat, etc.) permitiendo la granularidad de control de políticas para los mismos.
	Posibilitar la diferenciación de aplicaciones Proxies (ghostsurf, freegate, etc.) permitiendo la granularidad de control de políticas para los mismos.
PREVENCIÓN DE AMENAZAS	
Ambiente contra ataques.	El equipo de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware integrados en el próprio 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 Antispyware deben operar en permanentemente, permitiendo 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 y Activo/pasivo.
	La ejecución simultanea de una o todas las funcionalidades (IPS, Antivirus y Antispyware), no debe entregar un rendimiento menor al solicitado por la entidad.
Ambiente de configuración y servicios.	Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo.
	La exclusiones por IP de origen o de destino deben ser posibles en las reglas de forma general y firma a firma.
	Debe soportar granularidad en las políticas de IPS Antivirus y Antispyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos items.

	Debe permitir el bloqueo de vulnerabilidades.
	Debe permitir el bloqueo de exploits conocidos.
	Debe incluir seguridad contra ataques de denegación de servicios.
Mecanismos de inspección IPS.	Análisis de patrones de estado de conexiones.
	Análisis de decodificación de protocolo.
	Análisis para detección de anomalías de protocolo.
	Análisis heurístico.
	Reensamblado de paquetes de TCP.
	Bloqueo de paquetes malformados.
	Capacidad para rechazar ataques básicos como Syn Flood, ICMP flood, UDP flood, etc.
	Detectar y bloquear el origen de port scans.
	Bloquear ataques efectuados por worms conocidos, permitiendo al administrador adicionar nuevos patrones.
	Soporte de firmas específicas para la mitigación de ataques DoS.
	Posea firmas para bloqueo de ataques de buffer overflow.
	Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
	Permitir el bloqueo de virus y spywares para por lo menos los protocolos HTTP, FTP, SMB, SMTP y 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.
Sistema de monitoreo y bloqueo.	Debe soporte captura de paquetes (PCAP), por política de protección, firma de IPS o AntiSpyware
	Debe permitir que en la captura de paquetes por firmas de IPS o AntiSpyware sea definido el número de paquetes a ser capturados.
	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 que se ejecuten a través de los protocolos: HTTP, FTP, SMB, SMTP y 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 involuntários usando HTTP de archivos ejecutables maliciosos.
	Búsqueda de virus en archivos 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.
ANÁLISIS DE MALWARES MODERNOS	
Funcionalidades para el análisis de tráfico o incidentes.	El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis "In Cloud" o local.
	El sistema automático de análisis "In Cloud" o local debe emitir información detallada del tipo de malware que tiene infectado el archivo inspeccionado.
	Seleccionar a través de la política de Firewall que tipos de archivos sufrirán este análisis.
	El sistema de análisis "In Cloud" o local debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuáles 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).
	Soportar el análisis como 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.
	Soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB.
	Debe permitir exportar el resultado de los análisis de malwares de día Cero en PDF y CSV a partir de la própria interfaz de administración.
	Debe permitir la descarga de los malwares identificados a partir de la própria interfaz de administración.
	Debe permitir visualizar los resultados de los análisis de malware de día cero 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 malwares de día cero a partir de la própria interfaz de administración.

	Debe soportar el análisis de archivos ejecutables, DLLs, ZIP y criptografiados en SSL en el ambiente controlado.
	Debe permitir el envío de archivos para análisis en el ambiente controlado via web y de forma automática vía API.
FILTRO DE CONTENIDO	
Funcionalidades de filtro URL.	Debe permite especificar la política por tiempo, horário o determinado período (día, mes, año, dia de la semana y hora).
	Debe ser permitir crear políticas por usuario, grupo de usuário, IPs, redes y zonas de seguridad.
	Debe incluir la característica de creación de políticas basadas en la visibilidad y control de quién está utilizando cual URLs a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, EDirectory y base de datos local.
	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL.
	Debe bloquear el acceso a imagenes e información no debida sobre sitios de búsqueda (Google, Bing y Yahoo) en el caso de que la opción de Safe Search este deshabilitada o habilitada en el navegador. Si Safe Search esta deshabilitada este debe exhibir una página de bloqueo dando instrucciones al usuario de como habilitar dicha función o simplemente forzar la búsqueda segura de manera transparente al usuario.
	Debe soportar una caché local de URL en el appliance, evitando el delay de comunicación/validación de las URLs.
	Debe poseer al menos 60 categorías de URLs.
	Debe soportar la creación de categorías URL personalizadas.
	Debe soportar la exclusión de URLs del bloqueo por categoría.
	Debe permitir la personalización de la página de bloqueo.
	Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuários.
IDENTIFICACIÓN DE USUARIOS	
Control y gestión de usuarios.	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 soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x y soluciones NAC via syslog o radius, para la identificación de direcciones IP y usuarios.
	Debe permitir bloquear él envió de credenciales del dominio a sitios catalogados como comprometidos y/o Phishing.
	Soporte de autenticación Kerberos.
	Debe soportar la identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuário sobre el uso de las aplicaciones que tiene estos servicios.
	Debe ofrecer la posibilidad de identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente.
CALIDAD DE SERVICIO QoS	
Gestión de tráfico	Debe permitir bloquear aplicaciones como youtube, ustream, etc y/o controlar el consumo de ancho a través de políticas aplicadas a usuarios o grupos de usuarios.
Gestión de políticas.	Por dirección de origen.
	Por dirección de destino.
	Por usuario y grupo de LDAP/AD.
	Por aplicaciones, incluido servicios como Skype, Bittorrent, Youtube y Azureus o Vuze
	Por puerto.
Gestión de clases.	Ancho de banda garantizado.
	Ancho de banda máximo.
	Cola de prioridad.
	Soportar priorización RealTime 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 estatísticas RealTime para clases de QoS.
	Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuário.
FILTRO DE DATOS	

Gestión de tráfico	Debe permitir la creación de filtros para archivos y datos predefinidos.
	Debe permitir identificar archivos por extensión y firmas.
	Debe soportar la identificación de archivos compactados y las aplicaciones de políticas sobre el contenido de esos tipos de archivos;
	Debe permitir identificar y opcionalmente prevenir la transferencia de información sensible como datos bancarios, permitiendo la creación de nuevos tipos de datos via expresión regular.
	Debe permitir listar el número de aplicaciones soportadas para control de datos.
	Debe permitir listar el número de tipos de archivos soportados para el control de datos.
	Debe permitir la detección de portales de phishing estableciendo políticas que eviten el envío de credenciales válidas de usuarios a sitios no autorizados.
	Debe permitir la creación de políticas que soliciten un segundo factor de autenticación basadas en el origen (Usuario / Zona / Direcciones) y destino del tráfico (Aplicativos / Zonas / IPs).
	Opcional: debe aplicar etiquetas de manera automática a una IP origen (o destino) cuando un log es generado en el firewall, y que la etiqueta pueda formar parte de políticas existentes que puedan aplicar controles de manera dinámica.
GEOLOCALIZACIÓN	
Características.	Debe soportar la creación de políticas por geolocalización, permitiendo que el tráfico de determinado País/Países sean bloqueado.
	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.
SERVICIOS VPN	
Funciones.	Soportar VPN Site-to-Site y Client-To-Site.
	Soportar IPSec VPN.
	Soportar SSL VPN.
VPN IPSec.	3DES.
	Soporte para autenticación MD5 y 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).

	Autenticación vía certificado IKE PKI.
	Debe ser compatible con la Suite B de protocolos de NSA.
VPN SSL	Debe permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operacional del equipamiento o por medio de interfaz WEB.
	Servicio de soporte sin que requiera el uso de agentes.
	Soportar 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.
	Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus y 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.
	Soporte para 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).
	Debe permitir la aplicación de políticas de seguridad y visibilidad 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 distribuído 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.
	El agente de VPN SSL client-to-site debe ser compatible al menos con: Versiones de Windows que actualmente soporta Microsoft.
	Debe poseer la capacidad de identificar el origen de conexion de VPN si es interna o externa.
CONSOLA DE ADMINISTRACIÓN Y MONITOREO	
Funcionalidades.	Debe centralizar la administración de Reglas y políticas del cluster, usando una única interfaz de administración.
	Soporte acceso vía SSH, cliente WEB (HTTPS) y API, abierta compatible con Windows y Linux.
	Soporte para la creación y administración de políticas de firewall y control de aplicaciones.

	Soporte para la creación y administración de políticas de IPS y Anti-Spyware.
	Soporte para la creación y administración de políticas de filtrado de URL.
	Soporte para el monitoreo de logs.
	Herramientas de investigación de logs, debugging, captura de paquetes.
	Soporte para el acceso concurrente de administradores.
	Debe tener un mecanismo de búsqueda de comandos de administración vía SSH que facilite su su localización.
	Debe permitir usar palabras claves 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 client-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 simultáneo de dos o más administradores.
	Debe permitir la definición de perfiles de acceso a la consola con permisos granulares como el 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 realizar copias de respaldo de las configuraciones y restauración de configuración salvada que se requiera.
	Debe permitir crear reglas con fecha de expiración.
	Debe soportar el Rollback de Sistema operativo para la última versión local.
	Debe poseer la habilidad del upgrade via 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 permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó fecha y el horario de la modificación.
	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 red lan.
	Debe proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Anti Spyware) 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 y Antispyware) 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 acesso.
	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 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 simultáneas.
	Debe poder mostrar el estado de las interfaces.
	Debe poder mostrar el uso de CPU.

	Debe mostrar un resumen gráfico de las aplicaciones utilizadas.
	Debe presentar gráficamente las aplicaciones por utilización de ancho de banda de entrada y salida.
	Debe presentar gráficamente las principales aplicaciones por tasa de transferencia en bytes.
	Debe presentar gráficamente los principales hosts por número de amenazas identificadas.
	Debe presentar gráficamente las 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 horário, donde debe ser posible definir un rango de tiempo como criterio de búsqueda.
	Debe generar alertas automáticas vía email, SNMP y Syslog.
	La plataforma de seguridad o de gestión debe permitir a través de API-XML o Rest-API o JSON-API (Application Program Interface) la integración con sistemas existentes en el ambiente de contratación de forma que posibilite que aplicaciones desarrolladas por la entidad o por terceros, 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.

FICHA TÉCNICA CARACTERÍSTICAS DE SOFTWARE ENDPOINT

REQUISITOS ESPECÍFICOS CARACTERÍSTICAS	DESCRIPCIÓN DEL REQUERIMIENTO MÍNIMO Y/O TIPO DE SERVICIOS
Identificación de ataques de exploits	Detección del mecanismo de identificación de propiedades de un sistema por parte de un exploit kit, sin necesidad de utilizar firmas, patrones o heurísticas.
Prevención contra exploits.	Detección de técnicas de explotación sin necesidad de utilizar firmas, patrones o heurísticas, enfocadas principalmente en la prevención de exploits lógicos, procesos vulnerables y exploits del sistema operativo, para sistemas Microsoft Windows.
	Mitigación de vulnerabilidades conocidas, desconocidas y día cero.
	Soporte de técnicas de explotación de vulnerabilidades distintas, entre las que se encuentran Return Oriented Programming, Heap Spray, Jit Spray, Shell link, Structured Exception Handler, etc).
	Protección de aplicaciones contra las técnicas de explotación de manera predeterminada y "out-of-the-box".

	Entre las aplicaciones predeterminadas se encuentran: Firefox, Internet Explorer, Microsoft Word, Microsoft Excel, versiones de Flash Player, Microsoft Silverlight entre otras.
	Capacidad de utilizar los módulos de protección contra técnicas de explotación en cualquier aplicación, incluyendo aquellas desarrolladas internamente.
	Opcional: capacidad de crear un snapshot de forma automática de la memoria RAM al momento de prevenir la ejecución de una técnica de explotación, con la finalidad de proporcionar datos forenses sobre el evento.
	Posibilidad para configurar perfiles de protección en modo de prevención o monitoreo.
	Opcional: capacidad para la eliminación del proceso en el cual fue identificado el intento de ejecución de una técnica de explotación.
	Prevención de técnicas de explotación que utilizan ROP para Mac OS.
	Prevención de técnicas de explotación que utilizan JIT para Mac OS.
	Prevención de técnicas de explotación que buscan secuestrar el flujo de control de un proceso mediante el monitoreo de intentos de enumeración de la distribución de la memoria para sistemas operativos Linux.
	Prevención de técnicas de explotación que buscan redireccionar los flujos de entrada y salida estándares a sockets de red para sistemas operativos Linux.
	Prevención de técnicas de explotación que utilizan return-oriented programming para sistemas operativos Linux.
	Prevención del uso de áreas de memoria que son utilizadas para almacenar el payload de un ataque utilizando técnicas de heap spray, para sistemas operativos Linux.
	Capacidad para prevenir técnicas de explotación, así como de compatibilidad, de manera predeterminada, con la finalidad de mejorar la experiencia del usuario final y reducir la creación de falsos positivos.
	Capacidad de proporcionar la protección contra la explotación de vulnerabilidades sin necesidad de tener una conexión a la consola.
Identificación de ataques post-explotación.	Identificación y prevención de intentos de escalamiento de privilegios a nivel de Kernel. Esta protección debe de poder ser utilizada en agentes Windows, Mac y Linux.
	Detección y terminación de comportamientos considerados como maliciosos mediante el análisis continuo de los eventos que sucedan en un endpoint. Esta detección debe considerar varios

	eventos y no sólo un evento. La detección debe utilizar varias reglas preconfiguradas, las cuales deben de tener la capacidad de analizar varios eventos y no sólo un evento.
	La protección no debe depender de una conexión a la consola de administración.
Prevención contra malware.	Soporte para la creación de hashes de procesos en ejecución y verificación de veredictos en una nube de inteligencia de amenazas.
	Envío de ejecutables desconocidos para su análisis en un sandbox ubicado en la nube, con la finalidad de determinar si son maliciosos o benignos. Esta protección debe estar disponible para sistemas operativos Windows, Mac, Linux y Android.
	Capacidad de prevenir contra shells reversos (reverse shell) para sistemas operativos Linux.
Prevención de malware conocido y desconocido.	Debe poseer un modelo matemático generado a partir de aprendizaje de máquina para comparar aproximadamente 300 características de un archivo ejecutable, de manera estática, para determinar si es malicioso. Esta protección debe estar disponible al menos para sistemas operativos Windows y Mac.
	Capacidad de identificar si la macro contenida en un documento de Word o Excel es maliciosa, sin necesidad de tener que ejecutar la macro ni observar su comportamiento o ejecución, para determinar si es maliciosa.
	Capacidad de proporcionar protección contra malware sin necesidad de tener una conexión a la consola.
	Capacidad de proporcionar protección contra malware sin necesidad de contar con firmas, patrones y/o heurísticas.
	Prevención de ejecución de procesos utilizando su hash, de manera que el administrador puede determinar qué aplicaciones pueden ser ejecutadas.
	Es posible configurar las políticas en modo de prevención o monitoreo.
Escaneo de archivos ejecutables.	Debe permitir realizar el escaneo de archivos ejecutables sin la necesidad de firmas.
	Debe permitir programar el escaneo de archivos de manera semanal o mensual.
	Debe permitir definir el día y la hora en la cual se iniciará el escaneo.
	El consumo de recursos al momento de realizar el escaneo no debe impactar en la experiencia del usuario.
	Permite habilitar el escaneo de dispositivos de almacenamiento removible.
	Permite crear listas blancas de carpetas para que sean excluidas del proceso de escaneo.

	Permite poner en cuarentena los archivos identificados como maliciosos, si es que la política está configurada de esta manera.
Protección contra el robo de contraseñas.	Proporciona una protección predeterminada en memoria contra el uso de la herramienta de extracción de contraseñas Mimikatz.
Restricciones de ejecución.	Debe restringir la ejecución de archivos a partir de cierta carpeta.
	Debe restringir la ejecución de archivos a partir de recursos compartidos.
	Debe restringir la ejecución de archivos a partir de dispositivos USB o CD/DVD.
	Debe permitir restricciones granulares de ejecución de procesos hijo definiendo el proceso padre y los procesos hijo a restringir o permitir.
	Debe permitir restricciones granulares de ejecución de procesos hijo sin necesidad de contar con una conexión a la consola de administración.
	Debe contar con políticas de restricción de creación de procesos hijo configuradas de manera predeterminada.
	Debe tener la capacidad de crear excepciones para permitir la ejecución de archivos a partir de ciertas carpetas.
	Debe tener la capacidad de crear excepciones para permitir la creación de procesos hijo.
	Debe tener la capacidad de crear excepciones para permitir la ejecución de archivos a partir de carpetas dentro de los dispositivos de almacenamiento removibles.
	Debe tener la posibilidad de configurar perfiles en modo de prevención o monitoreo.
Acciones de respuesta.	La consola debe permitir aislar un endpoint para que sólo exista comunicación con ella.
	La consola debe permitir definir otros dispositivos a los cuales se pueda conectar el endpoint, además de la consola.
	La consola debe permitir poner en cuarentena, bajo demanda, archivos maliciosos que hayan sido detectados o reportados, pero no bloqueados por las políticas de prevención definidas.
	La consola debe permitir eliminar bajo demanda los procesos que hayan sido reportados o detectados, pero no bloqueados, por las políticas de prevención definidas.
Administración y revisión de eventos.	La solución debe permitir la administración de políticas centralizadas, a través de una consola Web.
	La consola debe distinguir los eventos de prevención y notificación, y para cada uno de estos dos grupos debe clasificar los eventos en intentos de ejecución de exploits, intentos de ejecución de malware, violaciones a las políticas de restricciones e intentos de violación a las políticas de restricción.

	La consola debe clasificar los eventos en tres niveles de acuerdo a su severidad, bajo, medio y alto.
	La consola de administración debe identificar claramente los eventos que han sido reportados y/o bloqueados, y aquellos que han sido detectados.
	La consola debe tener la capacidad para clasificar el estado de las alertas en tres distintas categorías, nuevas, investigando y cerradas.
	La consola debe proporcionar información detallada bajo demanda de los eventos identificados como exploits.
Servicio de actualización y desinstalación del agente a partir de la consola.	Debe contar con integración con Active Directory para la gestión de computadoras y configuración de políticas.
	Debe permitir la creación de perfiles granulares.
	Debe permitir crear políticas basadas en los perfiles creados.
	Debe tener la capacidad de poder aplicar políticas a usuarios, grupos, computadoras o unidades organizaciones de Active Directory.
	Debe tener la capacidad de crear grupos virtuales que pueden alimentarse de forma estática y dinámica.
	Los eventos de prevención o notificación deben tener información básica como tipo de evento, módulo que realizó la prevención, detalles de ese módulo, nombre de la computadora, nombre del usuario, sistema operativo, versión del agente, proceso que generó el evento de prevención, ruta de ejecución del proceso que generó el evento de prevención, horario y fecha del evento.
	La consola deberá ser proporcionada bajo un esquema software as a service.
	Debe contar con un tablero de control donde se muestran los eventos de seguridad que no han sido atendidos (clasificados de acuerdo a su criticidad en alta, media y baja), la cantidad de endpoints que tienen instalado el agente (clasificados por su plataforma), la cantidad de licencias disponibles y la versión del agente.
	Debe contar con un tablero control donde se describen las características de los eventos de seguridad que se han generado. Este tablero debe permitir analizar a mayor detalle el evento de seguridad, incluyendo los reportes generados por el agente.
	Debe permitir la integración con una plataforma de ciberseguridad la cual incluya una nube de inteligencia y contextualización de amenazas.
	Debe permitir gestionar las excepciones en una pantalla específica, clasificándolas por excepciones de ejecución de

	archivos, excepciones a ejecución de procesos (exploits y procesos hijo) y excepciones de soporte.
Características del agente.	Agente con un footprint mínimo que no impacte la experiencia de usuario.
	El almacenamiento en disco debido ser mínimo y no debe almacenar firmas, patrones y/o heurísticas.
	Debe soportar sistemas operativos Windows para 32 y 64 bits para usuarios finales y para servidores incluyendo Windows Server Datacenter Edition y las versiones Windows Server 2012, además de sistemas operativos MAC, Linux, y ambientes virtualizados en VMware ESX, Citrix XenServer, Oracle Virtualbox, Microsoft Hyper-V.
Gestión de usuarios.	La consola permitir administrar los usuarios mediantes asignación roles.
	La consola debe permitir asignar roles a los diferentes usuarios para la gestión de la de consola de administración.
	Los roles preconfigurados tienen las siguientes características:
	Super Admin. Cuenta con todos los permisos, puede cambiar los roles asignados a otros usuarios, pero no puede cambiar su propio rol.
	Viewer. Cuenta con acceso de sólo lectura. Puede exportar datos.
	Security Admin. Cuenta con permisos para gestionar los perfiles, políticas y eventos de seguridad. Tiene acceso de sólo lectura a las tareas de despliegue.
	IT Admin. Cuenta con acceso a las tareas de despliegue. Tiene acceso de sólo lectura a los perfiles, políticas y eventos de seguridad.
	No Access. Sin acceso.
	Deployment Admin. Cuenta con acceso a las tareas de despliegue, pero no tiene acceso a los perfiles, políticas y eventos de seguridad.
Reportes.	Debe permitir generar reportes bajo demanda o programados en formato PDF.
	La consola debe mantener un historial de los reportes que han sido generados para su posterior consulta.
	La frecuencia para la generación de los reportes programados podrá ser diaria, semanal o mensual.
	La generación de reportes automatizada debe ser administrable.
	La consola debe permitir gestionar las cuentas de correo para la notificación de alertas.
	Los reportes deben presentar el resumen de seguridad de los endpoint, tendencia de amenazas bloqueadas y detalles de seguridad.

	Deben incluir la cantidad global de archivos que fueron analizados, la cantidad global de eventos de explotación de vulnerabilidades prevenidos, la cantidad global de archivos maliciosos que fueron bloqueados.
	Deben mostrar los usuarios que han generado la mayor cantidad de eventos haciendo una diferencia entre malware, exploits y el número total de eventos registrados.
	Deben mostrar las computadoras, sin importar el usuario, que más eventos de seguridad han generado haciendo una diferencia entre malware, exploits y el número total de eventos registrados.
	Deben mostrar los archivos maliciosos que más prevalencia han presentando, incluyendo su hash calculado con el algoritmo SHA256, el número de veces que ha sido bloqueado y si fue o no identificado mediante un escaneo.
	Deben mostrar los procesos que más eventos de prevención de explotación de vulnerabilidades han presentado.
	Deben mostrar las técnicas de explotación de vulnerabilidades que fueron más utilizadas durante los ataques que fueron prevenidos.
	Deben mostrar un detalle de los endpoints que pueden potencialmente estar comprometidos incluyendo nombre, nombre del archivo malicioso y la primera vez que fue identificada su ejecución.
	Deben mostrar un detalle de los exploits que potencialmente fueron exitosos en su ejecución incluyendo el nombre del endpoint y el proceso cuya vulnerabilidad fue explotada.
	Debe mostrar el número de licencias utilizadas de manera global y por sistema operativo.
	Debe mostrar por cada sistema operativo, el número de licencias utilizadas en cada versión.
	Debe mostrar el número de licencias y el estado del agente asociado.
	Debe mostrar el número de licencias y versión del agente.
Capacidades de detección, investigación y respuesta.	Debe tener la capacidad de utilizar los datos capturados por el agente que se utiliza para realizar las tareas de detección e investigación, sin necesidad de utilizar un segundo agente.
	Deberá de contar con un tablero de control que permita visualizar alertas generadas de distintas fuentes.
	La plataforma de administración debe mostrar información detallada de los equipos, así como las amenazas detectadas en cada uno de ellos.
	Las columnas del tablero de control deben ser configurables tanto en su contenido como en su ancho y alto, para poder seleccionar las que sean de interés para el analista y que su vista sea cómoda.

	Las alertas deberán de poder ser filtradas utilizando parámetros de ID de la alerta, timestamp, nombre del host, IP del host, nombre de usuario, severidad, frente de la alerta, si la alerta constituye una detección o un bloqueo, categoría, nombre de la alerta, descripción, proceso que lo inició, línea de comando del proceso que lo inició, firma del proceso que lo inició, nombre de la entidad que firmó el proceso, tipo de evento, nombre del proceso que generó la alerta, comando del proceso que generó la alerta, firma del proceso que generó la alerta, nombre de la entidad que firmó el proceso que generó la alerta, CID, ruta del archivo, valor MD5 del archivo, valor SHA256 del archivo, valor del registro, llave completa del registro, IP local, puerto local, host remoto.
	Debe mostrar el número total de alertas, incluyendo la cantidad de alertas que resultan de aplicar un filtro.
	Debe implementar un menú contextual que permita analizar de manera detallada la alerta, generar una línea de tiempo, editar una regla, eliminar una alerta, copiar el URL de una alerta y copiar la alerta.
	Debe permitir exportar los datos contenidos en el tablero de control, incluso si se han aplicado filtros, a un archivo separado por pestañas para poder ser analizado por un analista fuera del producto.
	Debe contar con un gestor de columnas para que el usuario pueda libremente modificar el orden, teniendo la opción de volver a restaurar su configuración predeterminada.
	Debe permitir al analista copiar toda la información de la actividad identificada, por cada renglón.