1. **REQUERIMIENTOS TÉCNICOS DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL**

La Universidad Militar Nueva Granada desea adquirir una solución de protección de red con características de Next Generation Firewall (NGFW) que cuenten con sistema seguridad de la información perimetral para las sedes de Calle 100 y Cajicá en alta disponibilidad para cada sede que incluya 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", así 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.

El fabricante debe haber permanecido en la clasificación de los "Cuadrantes de Gartner" para "Enterprise Firewall" o firewalls empresariales en los últimos 3 años.

Las características deben ser confirmadas mediante documentación oficial de acceso público (guías de administración, manuales y/o guías técnicas). No se aceptarán documentos generados expresamente para este proceso (ad-hoc).

El un requisito obligatorio que la solución incluya y se integre con su solución de seguridad perimetral. Para la evaluación de la propuesta es fundamental que los equipos cumplan las siguientes características técnicas.

Básicas

a. No debe ser un firewall basado en UTM (Puerto / Protocolo / IP). La Universidad Militar requiere un firewall de última generación que permita la inspección de paquetes a nivel de aplicación (Capa 7 del modelo OSI).
b. Gartner es una empresa especializada en consultoría e investigación de tecnologías de la información que cuenta con una alta trayectoria, reputación, credibilidad e imparcialidad sobre los reviews de soluciones y/o dispositivos encontrados en el mercado. Por tal motivo la solución de seguridad perimetral ofertada debe estar posicionada en el cuadrante de gartner correspondiente a "Magic Quadrant for Enterprise Network Firewalls". Ello garantiza que la solución a implementar es una plataforma de calidad y por lo tanto garantiza que ha sido probada en muchas empresas a nivel mundial.

c. Para garantizar su continuidad el chasis debe contar con fuente redundante
d. Debe poderse integrar a la actual arquitectura de directorio activo presente en la Universidad Militar en el caso de que se deseen crear filtros específicos más estrictos.

Firmas / Actualizaciones

a. Las firmas o actualizaciones mínimas que debe ofrecer la solución es:

i. Ataques de día cero
ii. Antimalware
iii. Phishing / Control de contenido web por categorías
iv. Análisis e identificación de aplicaciones (Funcionalidad de firewall de capa 7)

b. Las actualizaciones deben actualizarse de manera automática con una periodicidad mínima de 2 (dos) días.
c. El fabricante de la solución de seguridad debe estar en capacidad de ofrecer un sistema de ticket's, o atención telefónica en español con horario de atención 7x24 para la atención de fallas o de escalamiento

Sobre ancho de banda - Networking

a. La solución de seguridad perimetral debe garantizar un rendimiento de ancho de banda (througput) a nivel constante del procesamiento de paquetes o requerimientos sin importar la cantidad de módulos o funcionalidades activas en el equipo.
b. Debe ser compatible con el protocolo de Link Aggregation Protocol (Enlaces agregados)

Redundancia / Alta disponibilidad

A pesar de que lo ideal es tener un nodo activo/activo o activo/pasivo para ofrecer alta disponibilidad cuando ocurra una falla, queda a potestad del oferente ofrecerlo (o no). Se debe tener en cuenta que debe estar incluido dentro del presupuesto asignado al proyecto.

CARACTERÍSTICAS FÍSICAS Y DE RENDIMIENTO				
A. Características Técnicas Mínimas Obligatorias (s/g bien, servicio u obra)				
Ítem 1. Solución de seguridad perimetral sede calle 100	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
Throughput de 10 Gbps con la funcionalidad de control de aplicaciones habilitada para todas las firmas que el fabricante posea				
Throughput de 5 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la plataforma de seguridad posea debidamente activadas y actuando: control de aplicaciones IPS, Antivirus e Antispyware				
Soporte a, como mínimo, 2.000.000 de conexiones simultáneas				
Soporte a, como mínimo, 100.000 nuevas conexiones por segundo				
Fuente 120/240 AC redundante y hot-swappable				
Disco Solid State Drive (SSD) de, como mínimo, 200 GB				
12 (doce) interfaces de red 10/100/1000 base-TX				
8 (ocho) interfaces de red 1 Gbps SFP				
4 (cuatro) interfaces de red 10Gbps SFP+				
2 (dos) Gbps interfaces dedicadas para alta disponibilidad				
1 (una) interface de red 1 Gbps dedicada para administración				
1 (una) interface de tipo consola o similar				
Soporte a, como mínimo, 100 (cien) ruteadores virtuales				
Soporte a, como mínimo, 400 (cuatrocientas) zonas de seguridad				
Estar licenciada para soportar sin uso de licenciamiento, 10.000 (diez mil) clientes de VPN SSL simultáneos				
Estar licenciada para soportar sin uso de licenciamiento, 4.000 (cuatro mil) túneles de VPN IPSEC simultáneos				
Debe soportar, no mínimo, 25 sistemas virtuales lógicos (Contextos) en el firewall Físico				
Los contextos virtuales deben las funcionalidades nativas del gateway de seguridad incluyendo: Firewall, IPS, Antivirus, Anti-Spyware, Filtro de Datos, VPN, Control de Aplicaciones, QOS, NAT e Identificación de usuarios				
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 no puede residir en el mismo appliance de seguridad de red, así 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 podrán estar listados en el site del fabricante como listas de end-of-life y end-of-sale				

Ítem 2. Solución de seguridad perimetral sede Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
Throughput de 4 Gbps con la funcionalidad de control de aplicaciones habilitada para todas las firmas que el fabricante posea				
Throughput de 2 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la plataforma de seguridad posea debidamente activadas y actuando: control de aplicaciones IPS, Antivirus e Antispyware				
Soporte a, como mínimo, 500.000 de conexiones simultaneas				
Soporte a, como mínimo, 50.000 nuevas conexiones por segundo				
Fuente 120/240 AC redundante y hot-swappable				
Disco Solid State Drive (SSD) de, como mínimo, 100 GB				
8 (ocho) interfaces de red 10/100/1000 base-TX				
8 (ocho) interfaces de red 1 Gbps SFP				
2 (dos) interfaces de red 10Gbps SFP+				
2 (dos) Gbps interfaces dedicadas para alta disponibilidad				
1 (una) interface de red 1 Gbps dedicada para administración				
1 (una) interface de tipo consola o similar				
Soporte a, como mínimo, 10 (diez) ruteadores virtuales				
Soporte a, como mínimo, 40 (cuarenta) zonas de seguridad				
Estar licenciada para soportar sin uso de licenciamiento, 2.000 (mil) clientes de VPN SSL simultáneos				
Estar licenciada para soportar sin uso de licenciamiento, 2.000 (mil) túneles de VPN IPSEC simultáneos				
Debe permitir expansión futura a hasta 6 sistemas virtuales lógicos (Contextos) en el firewall Físico				
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 podrán estar listados en el site del fabricante como listas de end-of-life y end-of-sale				

Ítem 3. Funcionalidades Mínimas para sedes calle 100 y Cajicá	CUMPLE		FOLIO	OBSERVACIONES
	SI	NO		
La solución debe consistir de un appliance 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				
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				
Los dispositivos de seguridad de red deben poseer por lo menos las siguientes funcionalidades: Soporte a 4094 VLAN Tags 802.1q; 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 dinámico (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 puertos (PAT); NAT de Origen; NAT de Destino; Soportar NAT de Origen y NAT de Destino simultáneamente; 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);				

Para IPv6, debe soportar enrutamiento estático y dinámico (OSPFv3); Soportar OSPF graceful restart; Debe ser compatible con LACP;				
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				
Los dispositivos de seguridad deben tener la capacidad de operar de forma simultanea mediante el uso de sus interfaces físicas en los siguientes modos: Modo sniffer (monitoreo y análisis del tráfico de red), Capa 2 (l2) y Capa 3 (l3); 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 mixto de trabajo Sniffer, L2 e L3 en diferentes interfaces físicas				
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, mas no limitado a políticas de Firewall, NAT, QOS y objetos de red; Certificados de-criptografados; Asociaciones de Seguridad de las VPNs; Tablas FIB;				
El sistema de 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				

Ítem 3.1. Control por política de firewall para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
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: 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 des encriptar tráfico Inbound y Outbound en conexiones negociadas con TLS 1.2				
Debe poder generar claves RSA de hasta 2048 bits en el tráfico saliente para inspección Control de inspección y desencripción de SSH por política				
La plataforma de seguridad debe implementar duplicación de tráfico des encriptando (SSL e TLS) para soluciones externas de análisis (Forense de red, DLP, Análisis de Amenazas, entre otras);				
Es permitido el uso de appliance externo, específico para la desencripción de (SSL y TLS), con copia del tráfico desencripción tanto para el firewall, como para las soluciones de análisis				
Bloqueos de los siguientes tipos de archivos: bat, cab, dll, exe, pif, reg, encrypted - doc, docx, pdf, ppt, pptx, zip, rar, Flash, ISO, Mp3, Mp4, PNG, AVI, bmp,email – link				
Traffic shaping QoS basado en Políticas (Prioridad, Garantía y Máximo				
QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones				
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				
En los logs debe presentar la razón de fin de sesión en el tráfico				

Ítem 3.2. Control de aplicaciones para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
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 2000 aplicaciones diferentes, incluyendo, mas 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, mas no limitando a RDP en el puerto 80 en vez del 3389				
Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis comportamental del tráfico observado, incluyendo, mas no limitado a Encrypted Bittorrent y aplicaciones VOIP que utilizan criptografía propietaria				

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 criptografiadas, tales como Skype y ataques mediante el puerto 443				
Para tráfico criptografados (SSL y SSH), debe desencripción 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, mas no limitado a Yahoo! Instant Messenger usando HTTP. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo, mas 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 criptografiadas				
Debe Actualizar la base de firmas de aplicaciones automática y periódicamente				
Debe Reconocer aplicaciones en IPv6				
Limitar el ancho de banda (Down load/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				
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 del órgano				
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 archivos				
Debe posibilitar a diferenciación de aplicaciones de evación de politicas tipo Proxy (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 malwares, como transferencia de archivos y/o uso excesivo de ancho de banda, etc				

Ítem 3.3. Prevención de amenazas para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
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-Virus y Antispyware habilitadas simultáneamente				
Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo				
Exenciones 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 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 explicar los mecanismos de inspección de IPS				
Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood, 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				
Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto				

Permitir el bloqueo de virus y spywares 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				
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				
Rastreamiento 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				

Ítem 3.4. Análisis de malwares modernos para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
Poseer la capacidad de análisis de amenazas no conocidas				
Debido a los Malwares hoy en día hay que 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 Malwares 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 sufrirá este análisis				
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 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 malwares de día Zero en PDF y CSV a partir de la propia interfaz de administración				
Debe permitir la descarga de los malwares 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 malwares de día Zero a partir de la propia interfaz de administración				
Soportar el análisis de archivos ejecutables, DLLs, ZIP y criptografados en SSL en el ambiente controlado				
Soportar el análisis de archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), open office, flash, archivos java (.jar e class), Android APKs y enlaces URL en correos, en el ambiente controlado				
Poseer SLA de, como máximo, 40 minutos para actualización de la base de vacunas contra malwares 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				

Ítem 3.5. Filtro de URL para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
La plataforma de seguridad debe poseer las siguientes funcionalidades de filtro de URL				
Permite especificar la política por tempo, horario o determinado período (día, mes, año, día de la semana y hora)				
Debe ser posible crear políticas por usuario, grupo de usuario, IPs, redes y zonas de seguridad				
Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quien está utilizando cual Urls a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, E-Directory y base de datos local				
Debe permitir poder publicar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio				
Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL				
Debe bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo!) en el caso de que la opción de Safe Search este deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de como habilitar dicha función				
Debe soportar una cacheé 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 custom				
Debe soportar la exclusión de Urls del bloqueo por categoría				

Debe permitir la customizacion de la página de bloqueo				
Debe permitir o bloquear y continuar (habilitando que el usuario acceda a un sitio potencialmente bloqueado informándole del bloqueo y habilitando el botón de "continuar" para permitirle seguir a ese site)				
Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios				
Debe permitir loguear el campo de HTTP header para análisis forenses				

Ítem 3.6. Identificación de usuarios para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
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 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 (Tipo Captive Portal /Portal Cautivo)				
Soporte a autenticación Kerberos				
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				

Ítem 3.7. QOS para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
Como la finalidad de controlar aplicaciones y trafico 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 ves 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 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 estadísticas RealTime para clases de QoS.				
Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario				

Ítem 3.8. Filtro de Datos para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
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, Instant Messaging, 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, mas 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				

Ítem 3.9. Geo-localización para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
Soportar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sea 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				

Ítem 3.10. VPN para sedes calle 100 y Cajicá	CUMPLE		FOLIO	OBSERVACIONES
	SI	NO		
Soportar VPN Site-to-Site y Cliente-To-Site				
Soportar IPSec VPN				
Soportar SSL VPN				
Las vpns IPSec debe soportar: 3DES; Autenticación MD5 e SHA-1; Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encryption Standard) Autenticación vía certificado IKE PKI.				
Debe poseer interoperabilidad como los siguientes fabricantes: Cisco; Checkpoint; Juniper; Palo Alto Networks; Fortinet; Sonic Wall				
Deben 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 crear 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 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 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: Sistemas operativos Microsoft vigentes en el mercado (Windows 7, 8, 8.1, 10), y sistemas operativos Linux y MacOS				
El cliente de VPN SSL cliente to site también debe soportar dispositivos móviles (IOS y Android)				
Debe poseer mecanismos de chequeo de conformidades del dispositivo remoto				
Este chequeo debe permitir verificar como mínimo las siguientes informaciones Sistema operacional y nivel de parcheo Antivirus y versión instalada Firewall de host Encripcion de disco Agente DLP instalado Backup de disco Llaves en el registro Procesos activos Debe ser posible la creación de perfiles customizados de conformidades con al menos las siguientes opciones: Sistema operacional y nivel de parcheo Antivirus y versión instalada Firewall de host Encripcion de disco Agente DLP instalado Backup de disco Llaves en el registro				
El proponente debe explicar cómo se soporta VPN				

Ítem 3.11. Consola de administración y monitoreo para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
Debe tener una solución de administración centralizada, posibilitando dicha administración para varios equipos				

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				
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 centralizar la administración de Reglas y políticas del clúster, usando una única interfaz de administración				
La administración de la solución debe soportar acceso vía SSH, cliente WEB (HTTPS)				
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 simultáneo 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				
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 auditoría detallados, informando de la configuración realizada, el administrador que la realizó 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 clúster				
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				
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 IPs 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				

Ítem 4. Otros Requerimientos para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
1 año de Garantía de fábrica				
3 Años en modalidad 7x24x4 de Tiempo de Servicios de reposición de partes y piezas (Hardware)				
El oferente deberá adjuntar en su propuesta una hoja de vida de un ingeniero especialista en networking para que lidere las actividades de instalación e integración con la red actual, con certificación técnica a nivel de especialización (Cisco CCIE, HP MASE, Juniper JNCIE-ENT). Esto con el fin de garantizar la calidad en la integración de los productos ofrecidos.				
El oferente debe ser partner Silver o nivel superior, además de estar autorizado en Colombia por el fabricante de los equipos ofertados y estar en capacidad técnica de configurar mantener y dar soporte técnico de los equipos. En consecuencia el oferente deberá presentar documentación que lo acredite como partner de la marca, documento que debe ser expedido por el fabricante de los equipos ofertados.				
El contratista deberá realizar capacitaciones oficiales (impartidas por fabricante) del producto ofrecido, dichas capacitaciones deberán contemplar los niveles de administración básico y avanzado, cada capacitación deberá ser independiente y el plan de estudio deberá ser aprobado por la entidad				