APC Colombia

ANEXO 2 “ALCANCE Y CONDICIONES TÉCNICAS”

# ESTUDIO DE MERCADO – ESTUDIOS PREVIOS

Ley 80 de 1993, Ley 1150 de 2007.

(Artículo 2.2.1.2.1.5.1. del Decreto 1082 de 2015)

# INCORPORAR UN FIREWALL DE NUEVA GENERACIÓN (NGFW) PARA REFORZAR LA PROTECCIÓN PERIMETRAL DE LA RED DE LA AGENCIA PRESIDENCIAL DE COOPERACIÓN INTERNACIONAL DE COLOMBIA, APC-COLOMBIA.

**2026**

## Tabla de contenido

1. ALCANCE ..... 3

1.1. Sede Única APC Colombia ..... 3

1. REQUERIMIENTOS TÉCNICOS DISPOSITIVOS DE SEGURIDAD PERIMETRAL PERÍMETRO. ..... 3

2. REQUERIMIENTOS TÉCNICOS SEGURIDAD ZERO TRUST. ..... 23

3. DECLARACIÓN DE ACEPTACIÓN DEL ALCANCE Y CONDICIONES TÉCNICAS DEL SERVICIO ..... 28

# 1. ALCANCE

## 1.1. Sede Única APC Colombia

| Número | Ubicación |
|---|---|
| Única Sede | Carrera 10 #97A - 13 Torre A - Piso 6, Edificio Bogotá Trade Center Bogotá D.C. |

## 1. REQUERIMIENTOS TÉCNICOS DISPOSITIVOS DE SEGURIDAD PERIMETRAL PERÍMETRO.

A continuación, se describen las características de Desempeño y Funcionalidad de los Firewall de Nueva Generación (Next Generation Firewall) requeridos por la entidad para su perímetro e interconexión Segura:

| CANTIDAD | ESPECIFICACIONES TECNICAS |
|---|---|
| **DOS (2) DISPOSITIVOS DE SEGURIDAD PERIMETRAL PERÍMETRO** | • Firewall Throughput (64 bytes) [Gbps]: 70<br>• Concurrent Sessions (TCP): 7500000<br>• New Sessions/Second (TCP): 500000<br>• IPsec VPN Throughput (512 byte) [Gbps]: 55<br>• Client-to-Gateway IPsec VPN Tunnels: 50000<br>• SSL-VPN Throughput [Gbps]: 3.6<br>• Concurrent SSL-VPN Users: 5000<br>• IPS Throughput (Enterprise Mix) [Gbps]: 12<br>• SSL Inspection Throughput (IPS, avg. HTTPS) [Gbps]: 8<br>• Application Control Throughput (HTTP 64K) [Gbps]: 28<br>• NGFW Throughput [Gbps]: 10<br>• Threat Protection Throughput [Gbps]: 9<br>• GE SFP Interfaces: 8<br>• 10GE SFP+ Interfaces: 8<br>• 5 GE RJ45 Interfaces: 8<br>• GE RJ45 Interfaces: 18 |

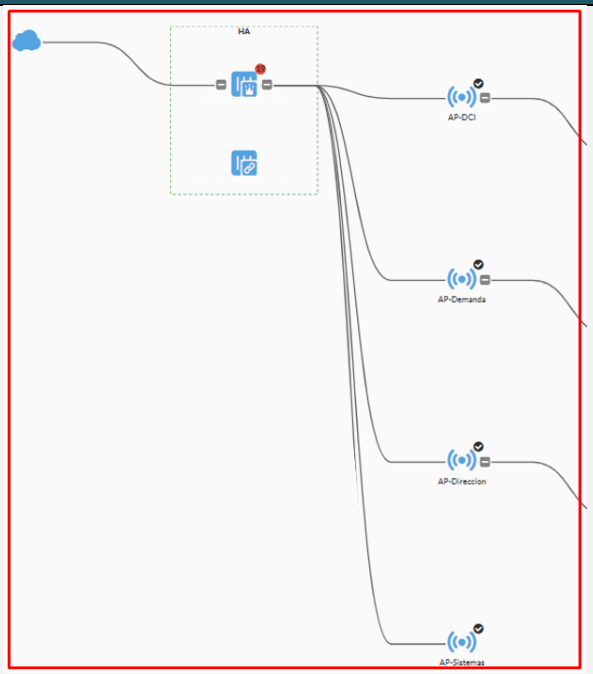
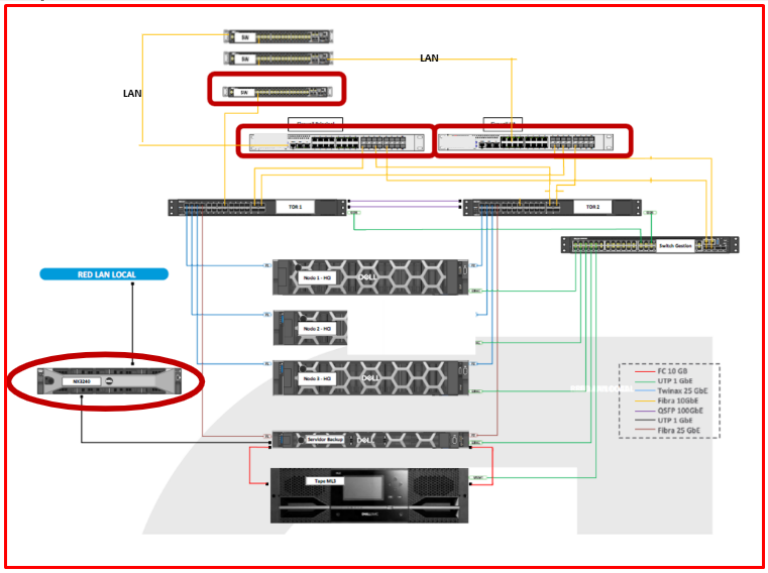
| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| **GENERAL** | • La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.<br>• Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos<br>• Las funcionalidades de protección de red que conforman la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.<br>• La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7<br>• Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación<br>• La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red<br>• Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q<br>• Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP<br>• Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding<br>• Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM)<br>• Los dispositivos de protección de red deben soportar DHCP Relay<br>• Los dispositivos de protección de red deben soportar DHCP Server<br>• Los dispositivos de protección de red deben soportar sFlow<br>• Los dispositivos de protección de red deben soportar Jumbo Frames |

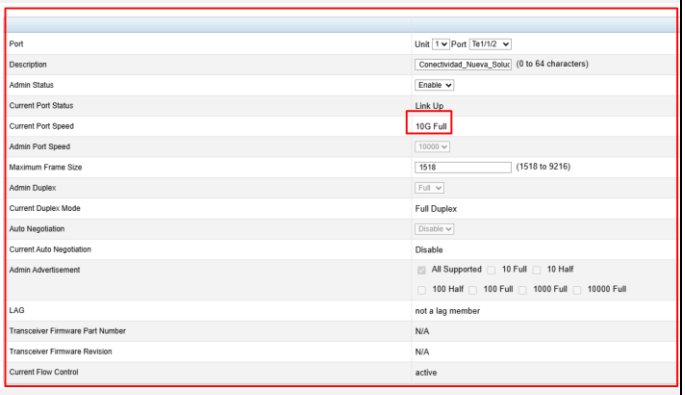
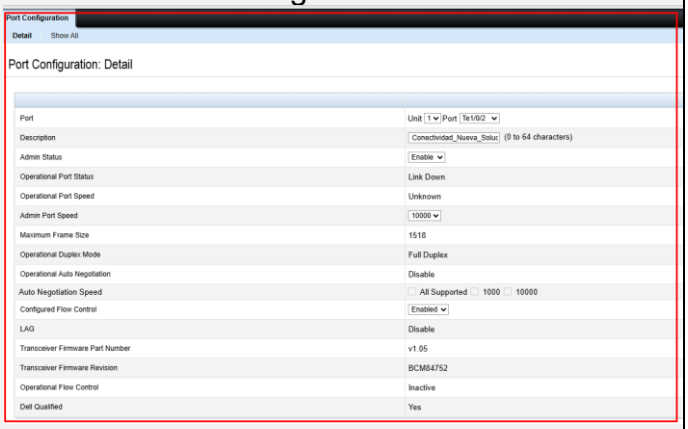
| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | • Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas<br>• Debe ser compatible con NAT dinámica (varios-a-1)<br>• Debe ser compatible con NAT dinámica (muchos-a-muchos)<br>• Debe soportar NAT estática (1-a-1)<br>• Debe admitir NAT estática (muchos-a-muchos)<br>• Debe ser compatible con NAT estático bidireccional 1-a-1<br>• Debe ser compatible con la traducción de puertos (PAT)<br>• Debe ser compatible con NAT Origen<br>• Debe ser compatible con NAT de destino<br>• Debe soportar NAT de origen y NAT de destino de forma simultánea<br>• Debe soportar NAT de origen y NAT de destino en la misma política<br>• Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico<br>• Debe ser compatible con NAT64 y NAT46;<br>• Debe implementar el protocolo ECMP;<br>• Debe soportar SD-WAN de forma nativa<br>• Debe soportar el balanceo de enlace hash por IP de origen;<br>• Debe soportar el balanceo de enlace por hash de IP de origen y destino;<br>• Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;<br>• Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;<br>• Debe permitir el monitoreo por SNMP de fallas de |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;<br>• Enviar logs a sistemas de gestión externos simultáneamente;<br>• Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;<br>• Debe soporta protección contra la suplantación de identidad (anti-spoofing);<br>• Implementar la optimización del tráfico entre dos dispositivos;<br>• Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);<br>• Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);<br>• Soportar OSPF graceful restart;<br>• Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;<br>• Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;<br>• Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;<br>• Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;<br>• Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;<br>• Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;<br>• Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;<br>• La configuración de alta disponibilidad debe sincronizar: Sesiones; |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | • La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;<br>• La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;<br>• La configuración de alta disponibilidad debe sincronizar: Tablas FIB;<br>• En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;<br>• Debe soportar la creación de sistemas virtuales en el mismo equipo;<br>• Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;<br>• Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;<br>• La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;<br>• Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);<br>• Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;<br>• El tejido de seguridad debe identificar potenciales |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;<br>• Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;<br>• La consola de administración debe soportar como mínimo, inglés, español y portugués.<br>• La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad<br>• La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.<br>• La solución debe ser compatible con los dispositivos WIFI de la Entidad (FortiAP 421E de referencia FAP421E).<br>• El contratista debe asegurar la conectividad de los dispositivos wifi-actuales de Agencia, su acceso de administración y configuraciones, cumpliendo además con la siguiente arquitectura: |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | <br>• La solución debe dar respuesta a la siguiente arquitectura.<br><br>Los switches donde se deberán conectar los firewalls |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | (LAN) son:<br>• Dell PowerConnect 7024<br><br>• Dell EMC Networking N3048ET-O<br><br>Para lo anterior el proveedor deberá suministrar los transceiver que sean necesarios para la conectividad.<br><br>• Los switches tor que tienen actualmente la Agencia son:<br>• TOR 1 – IronRack / Dell EMC S5224F-ON Switch (Tráfico de virtualización, máquinas virtuales, v-Motion y vSan)<br>• TOR 2 - Avengers/ Dell EMC S5224F-ON Switch (Tráfico de virtualización, máquinas virtuales, v-Motion y vSan) |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | • El proponente debe presentar certificados como partners mínimo en Nivel Profesional, es decir se acepta que este certificado como:<br>  • Profesional: Acredita competencias técnicas para configurar, administrar, operar y solucionar incidentes de la tecnología de manera autónoma, siguiendo buenas prácticas y lineamientos establecidos. Requiere experiencia práctica y dominio funcional del entorno.<br>  • Especialista: Certifica conocimientos profundos y experiencia especializada en un área particular de la solución, permitiendo optimizar configuraciones, resolver escenarios complejos y asesorar técnicamente en su ámbito de especialidad. Usualmente complementa un nivel profesional.<br>  • Experto: Acredita dominio integral de la tecnología, capacidad de diseño de arquitecturas complejas, integración con otras soluciones, definición de estrategias técnicas y liderazgo en proyectos de alta criticidad. Orientado a arquitectos, consultores senior y responsables técnicos principales.<br>• El proveedor deber realizar la migración o replicación de las políticas de seguridad actuales de la Agencia. |
| **DOCUMENTACIÓN** | • EL contratista deberá entregar a la entidad<br>• Manuales del fabricante del producto propuesto.<br>• Documentación que registre el estado de configuración e implementación al momento de la recepción formal de la solución (Informe definitivo de la Implementación)<br>• Diagramas y planos.<br>• Documentos de garantía<br>• Manuales de administración.<br>• Manuales de operación.<br>• Manuales de usuario. |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | • Catálogos de la herramienta ofrecida.<br>•<br>• Es obligatorio, para el cumplimiento del requisito habilitante, incluir en su propuesta el catálogo o documentación técnica del fabricante, en el cual se permita la comprobación de lo ofrecido y resaltar el párrafo en los catálogos donde se cumple con las características ofrecidas. |
| **CONFIDENCIALIDAD** | El contratista debe garantizar la preservación de la integridad y la confidencialidad de la información a la cual llegara a tener acceso directamente o por intermedio de terceros, y suscribirá con la entidad el documento que determine el alcance del compromiso de confidencialidad e integridad de la información, dentro de los cinco (5) días hábiles<br>• siguientes a la suscripción del Acta de Inicio de la ejecución del contrato. |
| **TRANSFERENCIA DE CONOCIMIENTO** | El oferente debe contemplar una capacitación en la modalidad de transferencia de conocimiento de mínimo de 24 horas la cual debe incluir como mínimo temas de administración, monitoreo y resolución de problemas correspondiente al dispositivo de seguridad, objeto del presente contrato |
| **ACCESORIOS INCLUIDOS** | Todos los accesorios necesarios para dar cumplimiento a la solución. |
| **FIREWALL** | • Debe soportar controles de zona de seguridad;<br>• Debe contar con políticas de control por puerto y protocolo.<br>• Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;<br>• Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad. |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | • Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad.<br>• Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;<br>• Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.<br>• Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);<br>• Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes<br>• Debe soportar el protocolo estándar de la industria VXLAN;<br>• La solución debe permitir la implementación sin asistencia de SD-WAN<br>• En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN; la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall. |
| **CONTROL DE APLICACIONES** | • Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;<br>• Detección de miles de aplicaciones en 18 categorias, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico; |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | • Reconocer al 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;<br>• Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;<br>• Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;<br>• Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;<br>• Actualización de la base de firmas de la aplicación de forma automática;<br>• Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por politica de usuarios y grupos;<br>• Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;<br>• Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante<br>• El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos<br>• Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | • Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo<br>• La solución debe permitir bloquear youtube y permitir apertura de canales de youtube elegidos por la Agencia.<br>• Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video<br>• Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo<br>• Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc)<br>• Debe ser posible crear grupos dinámicos de aplicaciones basados en características de estas, tales como: Nivel de riesgo de la aplicación<br>• Debe ser posible crear grupos estáticos de aplicaciones basadas en características de estas, tales como: Categoría de Aplicación<br>• Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente. |
| **PREVENCIÓN DE AMENAZAS** | • Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo<br>• Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware)<br>• Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante<br>• Debe sincronizar las firmas de IPS, antivirus, anti- |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | spyware cuando se implementa en alta disponibilidad<br>• 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 estos elementos<br>• Deber permitir el bloqueo de vulnerabilidades y exploits conocidos<br>• Debe incluir la protección contra ataques de denegación de servicio<br>• Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocol<br>• Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo<br>• Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP<br>• Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP<br>• Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets)<br>• Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc<br>• Detectar y bloquear los escaneos de puertos de origen<br>• Bloquear ataques realizados por gusanos (worms) conocidos<br>• Contar con firmas específicas para la mitigación de ataques DoS y DDoS<br>• Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow)<br>• Debe poder crear firmas personalizadas en la interfaz gráfica del producto;<br>• Identificar y bloquear la comunicación con redes de |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | bots<br>• Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;<br>• Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación<br>• Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos<br>• Los eventos deben identificar el país que origino la amenaza<br>• Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms)<br>• Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP<br>• Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad<br>• En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles<br>• Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | NGFW y Sandbox (en las instalaciones y en la nube). |
| **FILTRADO URL** | • Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora)<br>• Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito<br>• Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL<br>• Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL<br>• Tener por lo menos 75 categorías de URL<br>• Debe tener la funcionalidad de exclusión de URLs por categoría<br>• Permitir página de bloqueo personalizada<br>• Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio)<br>• Además del Explicit Web Proxy, soportar proxy web transparente. |
| **IDENTIDAD DE USUARIO** | • Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local<br>• Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | granularidad a las políticas / controles basados en usuarios y grupos de usuarios<br>• Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc<br>• Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios<br>• Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios<br>• Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);<br>• Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios<br>• Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD<br>• Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma<br>• Debe incluir al menos dos tokens de forma nativa, lo |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | que permite la autenticación de dos factores. |
| **CALIDAD DE SERVICIO (QOS & SHAPING)** | • Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming<br>• Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen<br>• Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino<br>• Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo<br>• Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube<br>• Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto<br>• En QoS debe permitir la definición de tráfico con ancho de banda garantizado<br>• En QoS debe permitir la definición de tráfico con máximo ancho de banda<br>• En QoS debe permitir la definición de colas de prioridad<br>• Soportar marcación de paquetes DiffServ, incluso por aplicación<br>• Soportar la modificación de los valores de DSCP para Diffserv<br>• Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service)<br>• Debe soportar QoS (traffic-shapping) en las |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | interfaces agregadas o redundantes. |
| **DLP** | • Permite la creación de filtros para archivos y datos predefinidos<br>• Los archivos deben ser identificados por tamaño y tipo<br>• Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones<br>• Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos<br>• Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos<br>• Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares. |
| **GEO IP** | • Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países<br>• Debe permitir la visualización de los países de origen y destino en los registros de acceso<br>• Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas. |
| **VPN** | • Soporte VPN de sitio-a-sitio y cliente-a-sitio<br>• Soportar VPN IPSec<br>• Soportar VPN SSL<br>• La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512<br>• La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14<br>• La VPN IPSec debe ser compatible con Internet Key |

| COMPONENTES DE SEGURIDAD PERIMETRAL PERÍMETRO | CARACTERISTICAS |
|---|---|
| | Exchange (IKEv1 y v2)<br>• La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard)<br>• Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall<br>• Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec<br>• Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting<br>• Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy<br>• Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL<br>• Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local<br>• Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL<br>• Deberá mantener una conexión segura con el portal durante la sesión;<br>• El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS. |
| **SOPORTE** | • Los dispositivos deben contar con el licenciamiento correspondiente para las funcionalidades.<br>• EL soporte debe ser de un (1) año. |
| **LICENCIAMIENTO** | • El proveedor deberá entregar el licenciamiento requerido por un término de doce (12) meses. |

## 2. REQUERIMIENTOS TÉCNICOS SEGURIDAD ZERO TRUST.

| CANTIDAD | ESPECIFICACIONES TECNICAS |
|---|---|
| **SEGURIDAD ZERO TRUST** | • La solución debe estar dimensionada inicialmente para soportar 150 usuarios y tener capacidad de escalabilidad mediante el uso de licenciamiento, sin la necesidad de tener que reemplazar hardware.<br>• Para poder garantizar control de acceso a la red de confianza cero para usuarios de la entidad, sitios locales y remotos, el OFERENTE debe incluir en su propuesta como mínimo los siguientes componentes:<br>• Agente de software para las estaciones de trabajo y su respectiva consola web para la administración centralizada<br>• Proxy ZTNA |

| COMPONENTES SEGURIDAD ZERO TRUST | CARACTERISTICAS |
|---|---|
| **GENERAL** | • Agente de software para las estaciones de trabajo y su respectiva consola web para la administración centralizada<br>• Características de Unified Endpoint que incluyan cumplimiento, protección y acceso seguro en un único cliente modular liviano<br>• El agente debe tener diferentes funciones (Agente unificado que permita visibilidad de los endpoints y cumplimiento de estos, Acceso Seguro ZTNA, Cliente VPN, Filtrado de Contenido, Protección de Endpoint) |

| COMPONENTES SEGURIDAD ZERO TRUST | CARACTERISTICAS |
|---|---|
| | • La solución debe estar en capacidad de acceso a las aplicaciones en cada sesión de usuario.<br>• La solución debe estar licenciada para la protección de 200 usuarios.<br>• La solución debe establecer comunicaciones seguras para validación de usuario y dispositivo, antes de permitir la conexión del usuario a la aplicación.<br>• La solución debe poder integrar autenticación multifactor usando certificados o tokens.<br>• La solución debe poder operar en una arquitectura híbrida, con componentes en las premisas de la entidad, y en la nube.<br>• La solución debe poder integrarse con los Firewall de Nueva Generación con los que cuenta la entidad en sud Datacenters, para la aplicación de políticas y visibilidad de Telemetría.<br>• La solución debe estar en capacidad de hacer escaneo de vulnerabilidades en los equipos finales protegidos y aplicar parches virtuales para su remediación.<br>• Debe proveer una interfaz API para integración con productos de terceros<br>• La característica de gestión de vulnerabilidades debe:<br>  • Permitir configurar la programación de escaneos<br>  • Permitir configurar opciones de instalación automática de vulnerabilidades dependiendo de la criticidad de esta. Por ejemplo, instalar solo actualizaciones críticas, o instalar todas las actualizaciones.<br>  • Debe permitir hacer exclusiones de aplicaciones o vulnerabilidades para actualizar<br>• La capacidad de protección de endpoint debe soportar al menos las siguientes capacidades:<br>  • Antivirus de nueva generación con Machine Learning |

| COMPONENTES SEGURIDAD ZERO TRUST | CARACTERISTICAS |
|---|---|
| | • Protección contra botnets<br>• Malware y Anti-Exploits<br>• Firewall de aplicaciones<br>• Control de dispositivos<br>• Filtrado web por categorías<br>• Control dinámico de acceso basado en la postura de seguridad del dispositivo<br>• Inventario de software<br>• Gestión de vulnerabilidades y aplicación automática de actualizaciones<br>• El agente debe proveer capacidades de cliente Single Sign On (SSO) para Windows<br>• El módulo anti-exploit debe proteger aplicaciones como Chrome, Firefox, Adobe, Microsoft Office.<br>• El módulo anti-exploit debe proteger contra ataques basados en memoria<br>• El módulo anti-exploit no debe estar basado en firmas<br>• Debe permitir agrupar los dispositivos basado en etiquetas automáticas que se apliquen basado en SO, dominio, procesos ejecutados, entre otras<br>• La consola de administración debe recibir reglas de alerta de brotes de amenazas para ayudar a proteger la red de vulnerabilidades y ver rápidamente que máquinas están expuestas a la nueva amenaza<br>• Debe permitir gestión de usuarios localmente, vía LDAP y SAML<br>• La funcionalidad de filtrado web debe:<br>• Debe permitir bloquear búsquedas por palabras clave<br>• Tener la funcionalidad de Safe Search para buscadores como Google y Bing<br>• Tomar acción sobre la página accedida (Bloquear, Advertir, Permitir, Monitorear)<br>• Debe permitir configurar una acción en caso de que el cliente presente un error. La acción debe |

| COMPONENTES SEGURIDAD ZERO TRUST | CARACTERISTICAS |
|---|---|
| | ser permitir todos los sitios y/o bloquear todos los sitios<br>• Debe permitir la creación de reglas de navegación basado en expresiones regulares<br>• La protección anti-ransomware debe poder definir carpetas o archivos protegidos<br>• La protección anti-ransomware debe realizar backup de los archivos protegidos cada vez que sean modificados con el fin de poder restaurarlos en caso de actividad sospechosa.<br>• La solución debe estar en capacidad de brindar control de aplicaciones, incluyendo aplicaciones SaaS.<br>• La solución debe estar en capacidad de enviar archivos maliciosos a una inspección tipo SandBox en la nube del fabricante o en premisas, para proteger contra nuevas amenazas, y poder actualizar la inteligencia de amenazas de acuerdo con el resultado de la inspección en el ambiente SandBox.<br>• La solución debe proveer servicios de parte del fabricante para el despliegue, configuración, integración monitoreo.<br>• La funcionalidad de cliente VPN debe permitir:<br>• Split-tunneling basado en aplicación<br>• SSL VPN<br>• IPSec VPN<br>• VPN Tunnel basado en verificación de cumplimiento<br>• La solución debe permitir observar en la consola de administración, el inventario de aplicaciones en los equipos protegidos.<br>• El módulo de inventario de aplicaciones debe tener como mínimo los siguientes campos:<br>• Número Total de aplicaciones detectadas<br>• Número Total de fabricantes detectados<br>• Nuevas aplicaciones detectadas en los endpoints |

| COMPONENTES SEGURIDAD ZERO TRUST | CARACTERISTICAS |
|---|---|
| | • Versión de la aplicación<br>• Fabricante<br>• Primera vez que se detectó la aplicación<br>• Última vez que se instaló la aplicación<br>• Cantidad de dispositivos con la aplicación instalada<br>• La solución debe poderse integrar con la plataforma de logs y reportes con la que cuenta la entidad, para el envío de logs a la misma.<br>• La solución debe poder utilizar los equipos NGFW en premisas con los que cuenta la entidad, para la implementación de políticas de cero confianzas.<br>• La solución debe estar en capacidad de generar acciones automáticas de cuarentena, ante la detección de eventos maliciosos en uno de los dispositivos protegidos.<br>• La solución debe poderse integrar con el directorio activo de la entidad para la identificación de usuarios y grupos<br>• Debe ser posible el despliegue y control de actualizaciones de la versión de agente en los dispositivos desde la consola de administración.<br>• Debe ser posible asignar una imagen (fotografía) al usuario asociado al endpoint, de manera que se facilite la identificación de este.<br>• La solución debe permitir generar grupos dinámicos basados en la postura de seguridad de los dispositivos protegidos, y permitir usar esta información para construcción de políticas para control de acceso dinámico en los firewalls de nueva generación de la entidad.<br>• Para el caso de VPNs, debe ser posible excluir del túnel VPN el tráfico de una aplicación.<br>• El agente de la solución debe poder enviar información de telemetría para que la información de los dispositivos finales sea visible en la vista de topología del Firewall de Nueva Generación de la entidad, con el fin de poder tener una visibilidad |

| COMPONENTES SEGURIDAD ZERO TRUST | CARACTERISTICAS |
|---|---|
| | unificada de la red y sus equipos.<br>• La solución debe estar en capacidad de proteger dispositivos Windows, Mac y Linux<br>• La solución debe soportar los siguientes sistemas operativos:<br>  • Windows 7 o superior<br>  • Windows Server 2012 o superior<br>  • MacOS 11 o superior<br>  • Ubuntu 18.04 o superior<br>  • Debian 11 superior<br>  • Red Hat 7.4 o superior<br>  • CentOS Stream 8, 7.4 or superior<br>  • Fedora 36 o superior<br>  • iOS 9 o superior<br>  • Android 5 o superior<br>• La Solución debe integrarse con la Arquitectura de Seguridad de la entidad (NGFW, Administración de identidad y Privilegios de Acceso) con el propósito de garantizar una postura proactiva y nativamente integrada de Seguridad. |
| **SOPORTE** | • EL soporte debe ser de un (1) año. |

## 3. DECLARACIÓN DE ACEPTACIÓN DEL ALCANCE Y CONDICIONES TÉCNICAS DEL SERVICIO

Nota: El alcance y las anteriores condiciones de este y demás anexos deben ser aceptadas expresamente por el proponente, suscribiendo el correspondiente Anexo.

Por medio de la presente, yo _____ en representación legal de _____ identificada con NIT: _____, entendemos, aceptamos y cumplimos todos y cada uno de los ítems relacionados en el presente anexo y demás que lo conformen, así como las obligaciones generales, específicas y adendas para el proceso.

_____

En constancia firma,

| | |
|---|---|
| Razón Social: | |
| Nombre del Representante Legal: | |
| C.C. o NIT: | |
| Dirección y ciudad: | |
| Teléfonos: | |
| Email: | |

_____

Firma del Representante Legal