adexsus

DRA. ALEJANDRINA MORENO YEPES
Abogada Notaria Público
De los del Distrito Nacion
Colegiatura Nº 2774

CARACTERISTICAS DE LOS PRODUCTOS OFERTADOS

- □ Rendimiento HTTP/ Appmix 14.5 Gbps / 11 Gbps, con las funciones habilitadas. Rendimiento de 5.1/5.6 Gbps para las funcionalidades IPS, prevención de amenazas, antivirus, antispyware, DNS Security, bloqueo de archivos
- El equipo soportar como mínimo 1,400,000 sesiones/conexiones concurrentes y 145,000 nuevas sesiones/conexiones por segundo, medidos en capa 7 (con paquetes HTTP).
- Cuenta con fuente de poder redundante.
- Disco interno de estado sólido de 480GB o superior, en espejo.
- Cuenta con una interfaz de cobre RJ45 dedicada para la gestión del equipo

- **Cuenta con la siguiente cantidad de interfaces para el tráfico de datos:**
- - (12) interfaces de cobre (RJ45) a 1G/2.5G/5G/10G.
- - (10) interfaces SFP+ a 1G/10G.
- - (4) interfaces SFP28 a 25G

- **Cuenta con las siguientes interfaces para la sincronización de HA:**
- (2) interfaces de cobre (RJ45) a 100/1000.
- - (1) interfaces SFP+ a 1G/10G.

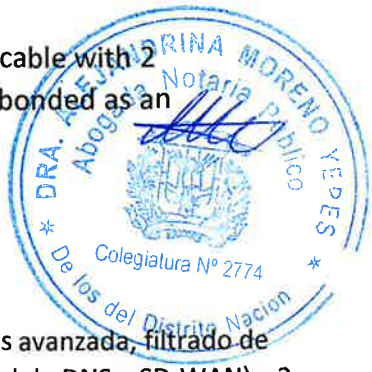
- Soportar configuraciones en alta disponibilidad Activo-Activo / Activo-Pasivo

ACCESORIOS

- (2) x Kit de montaje en rack
- (2) x Fuentes de poder redundantes adicionales.
- (8) x Transceptores Ópticos óptico (LR) FP+ form factor, LR 10Gb long reach 10Km, SMF, duplex LC, IEEE 802.3ae 10GBASE-LR.
- (20) x Transceptores Ópticos (SR) SFP+ form factor, SR 10Gb short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR.

adexsus
GRUPO TECNOLOGICO ADEXSUS SRL

- (1) x Cable DAS para interconnexion directa 10G twin-ax passive cable with 2 transceiver SFP+ form factor, ends and 5m of cable permanently bonded as an assembly.



LICENCIAS

- Paquete de suscripción de seguridad principal (prevención de amenazas avanzada, filtrado de URL avanzado, plataforma de nube avanzada contra Malware, seguridad de DNS y SD-WAN) x 2 Licenciamientos por tres (3) años.

GARANTIA

- Tres (3) años de garantía para los equipos y accesorios para dos (2) equipos en alta disponibilidad.
- Tres (3) años en actualizaciones en el software (Firmware) para dos (2) equipos en alta disponibilidad.

CAPACITACIONES

- incluido capacitaciones para cuatro (4) personas, las cuales abarquen las siguientes áreas:

- - Instalación.
- - Configuración.
- - Administración
- - Mejores Prácticas

SERVICIOS DE IMPLEMENTACIÓN

- Servicios de implementación contratados directamente con el fabricante.
- Migración de la plataforma actual (4) Firewall e IPS a la nueva solución ofertada.

08 de Abril del 2024
Santo Domingo, D. N.

Señores
Junta Central Electoral.
Ciudad.

REF: JCE-CCC-LPN-2024-0002.

Nosotros los suscritos, declaramos que:

Concedemos **Plazo de Mantenimiento de Oferta por Sesenta (60) días**, contados a partir de la fecha de apertura de ofertas.

Si nuestra oferta es aceptada, nos comprometemos a recibir el pago como corresponde: a un **Pago de anticipo no mayor de un 20%, al recibir la orden de compras, y el 80% a los Treinta (30)** días, después de realizada la entrega total de los equipos y servicios adquirido y recepción satisfactoria y la emisión de la factura con comprobante gubernamental firmada y sellada.

Así mismo nuestro tiempo de Entrega: **Sesenta (60) días, luego de recibir la Orden de Compras.**

Tiempo de Garantía:

- Tres (3) años de garantía para los equipos y accesorios
- Tres (3) años en actualizaciones en el software (Firmware)

ALEJANDRO MONTAS en calidad de representante legal debidamente autorizado para actuar en nombre y representación de GRUPO TECNOLOGICO ADEXSUS

Firma _____

Av. Pedro Henríquez Ureña No.18, Suite 101, Gazcue, Santo Domingo, República Dominicana
Tel. 809-685-3527 Fax. 809-238-5231 / amontas@adexsus.com , http://www.adexsus.com

R.N.C. 1-01-87625-5

08 de Abril del 2024
Santo Domingo, D. N.

Señores
Junta Central Electoral.
Ciudad.

REF: JCE-CCC-LPN-2024-0002.

Nosotros los suscritos, declaramos que:

Concedemos **Plazo de Mantenimiento de Oferta por Sesenta (60) días**, contados a partir de la fecha de apertura de ofertas.

Si nuestra oferta es aceptada, nos comprometemos a recibir el pago como corresponde: a un **Pago de anticipo no mayor de un 20%, al recibir la orden de compras, y el 80% a los Treinta (30)** días, después de realizada la entrega total de los equipos y servicios adquirido y recepción satisfactoria y la emisión de la factura con comprobante gubernamental firmada y sellada.

Así mismo nuestro tiempo de Entrega: **Sesenta (60) días, luego de recibir la Orden de Compras**.

Tiempo de Garantía:

- Tres (3) años de garantía para los equipos y accesorios
- Tres (3) años en actualizaciones en el software (Firmware)

ALEJANDRO MONTAS en calidad de representante legal debidamente autorizado para actuar en nombre y representación de GRUPO TECNOLOGICO ADEXSUS

Firma _____

Av. Pedro Henríquez Ureña No.18, Suite 101, Gazcue, Santo Domingo, República Dominicana
Tel. 809-685-3527 Fax. 809-238-5231 / amontas@adexsus.com , http://www.adexsus.com

R.N.C. 1-01-87625-5

ESPECIFICACIONES TÉCNICAS

Adquisición de una solución de Next Generation Firewall (NGFW) para la seguridad de la red Perimetral		
Requerimiento	**Cumple /No Cumple**	**Comentarios**
Debe ser ofrecida en alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones técnicas.	Cumple	La propuesta incluye dos (2) appliances físicos para ser configurados en alta disponibilidad.
El fabricante debe pertenecer al cuadrante de Líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 10 reportes.	Cumple	Palo Alto Networks ha sido galardonado como líder en el cuadrante de Gartner de Network Firewalls por 11avo año consecutivo, siendo la última evaluación en el año 2022. **Documentación:** Palo Alto Networks Positioned as a Leader in 2022 Gartner Magic Quadrant for Network Firewalls for the 11th Consecutive Year - Palo Alto Networks - https://bit.ly/4aGlObR
El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls.	Cumple	Palo Alto Networks está posicionado como líder en el reporte de Forrester Wave: Enterprise Firewalls. **Documentación:** 2022 Forrester Wave: Enterprise Firewalls – We're a Leader - https://bit.ly/4air2un
El fabricante de estar como líder en el último análisis de Forrester para Zero Trust eXtended (ZTX)	Cumple	Palo Alto Networks está posicionado como líder en el reporte de Forrester Wave: Zero Trust Enterprise, Q3 2023. **Documentación:** Zero Trust Edge - Forrester Names Palo Alto Networks a Leader https://bit.ly/4aW62d5
El fabricante debe estar como líder en el último informe de Forrester Wave Automated Malware Analysis.	Cumple	Palo Alto Networks está posicionado como líder en el reporte de Forrester Wave: Automated Malware Analysis. **Documentación:** Forrester Research Rates Palo Alto Networks a Leader for Automated Malware Analysis - https://bit.ly/4ai6YtJ

El fabricante de poseer las certificaciones siguientes para los productos ofertados: • ISO/IEC 27001:2013 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019 • ISO/IEC 27701	Cumple	**Documentación:** Product Certifications - Palo Alto Networks https://bit.ly/3J2OQqd
CARACTERÍSTICAS DE LOS EQUIPOS		
Rendimiento 14.1Gbps con las funciones de App-ID, habilitadas y 5.1/5.6 Gbps para las funcionalidades IPS, prevención de amenazas, antivirus, antispyware, DNS Security, bloqueo de archivos.	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** Datasheet - PA-3400 Series https://bit.ly/3U0kuuL
El equipo debe soportar como mínimo 1,400,000 sesiones/conexiones concurrentes y 145,000 nuevas sesiones/conexiones por segundo, medidos en capa 7 (con paquetes HTTP)	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** Datasheet - PA-3400 Series https://bit.ly/3U0kuuL
Debe contar con fuente de poder redundante.	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** Datasheet - PA-3400 Series https://bit.ly/3U0kuuL
Disco interno de estado sólido de 480GB o superior.	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** Datasheet - PA-3400 Series https://bit.ly/3U0kuuL
Debe contar con una interfaz de cobre RJ45 dedicada para la gestión del equipo.	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** Datasheet - PA-3400 Series https://bit.ly/3U0kuuL
Debe contar con la siguiente cantidad de interfaces para el tráfico de datos: • 12 interfaces de cobre (RJ45) a 1G/2.5G/5G/10G.	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** Datasheet - PA-3400 Series

• 10 interfaces SFP+ a 1G/10G • 4 interfaces SFP28 a 25G		https://bit.ly/3U0kuuL
Debe contar con las siguientes interfaces para la sincronización de HA: • 2 interfaces de cobre (RJ45) a 100/1000 • 1 interfaces SFP+ a 1G/10G	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** Datasheet - PA-3400 Series https://bit.ly/3U0kuuL
Debe soportar configuraciones en alta disponibilidad Activo Activo / Activo Pasivo.	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** Datasheet - PA-3400 Series https://bit.ly/3U0kuuL
ACCESORIOS		
• 2 x Kit de montaje en rack. • 2 x Fuentes de poder redundantes adicionales. • 8 x Transceptores Ópticos óptico (LR) FP+ form factor, LR 10Gb long reach 10Km, SMF, duplex LC, IEEE 802.3ae 10GBASE-LR. • 20 x Transceptores Ópticos (SR) SFP+ form factor, SR 10Gb short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR. • 1 x Cable DAS para interconexión directa 10G twin-ax passive cable with 2 transceiver SFP+ form factor, ends and 5m of cable permanently bonded as an assembly.	Cumple	
LICENCIAS		
Paquete de suscripción de seguridad principal (prevención de amenazas avanzada, filtrado de URL avanzado,	Cumple	El licenciamiento para las funciones de seguridad requeridas estará dentro de nuestra propuesta. **Documentación:**

avanzado, seguridad de DNS y SD-WAN) x 2 Licenciamiento por 3 años.		Subscriptions You Can Use with the Firewall https://bit.ly/4cCKfZp
Suscripción de protección global, para un (2) dispositivo en alta disponibilidad 2 Licenciamiento por 3 años.	Cumple	El licenciamiento para la función de global protection requeridas estará dentro de nuestra propuesta.
GARANTIA		
3 años de garantía para los equipos y accesorios para 2 equipos en alta disponibilidad.	Cumple	
3 años en actualizaciones en el software (Firmware) para para 2 equipos en alta disponibilidad.	Cumple	
CAPACITACIONES		
Debe incluir capacitaciones para 3 personas	Cumple	
SERVICIOS DE IMPLEMENTACION		
Alcance Servicios contratados directamente con el fabricante. • Migración de la plataforma actual (4) Firewall e IPS a la nueva solución ofertada. • 500 Reglas • 800 Objetos • 500 políticas • 700 Vpn Site to Site Por razones de confidencialidad no podemos compartir los equipos que actualmente están en uso.	Cumple	
REQUERIMIENTO SOPORTE		
Ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life, end-of-sale o end-of-support. Se deberá adjuntar	Cumple	Los equipos (PA-3410) propuestos aún no estan enlistado para: end-of-life, end-of-sale o end-of-support por parte del fabricante. **Documentación:** Hardware End-of-Life-Dates - Palo Alto Networks https://bit.ly/3xcqCaf

La solución propuesta deberá tener soporte vigente de fábrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware.	Cumple	**Documentación:** Palo Alto - Premium Support https://bit.ly/3vDB5LG
El soporte deberá estar disponible 24x7x365, la apertura de casos deberá poder realizarse vía online o vía telefónica.	Cumple	**Documentación:** Palo Alto - Premium Support https://bit.ly/3vDB5LG
Se deberá proporcionar accesos al portal de soporte del fabricante, donde se tenga la potestad de dar seguimiento a los mismos.	Cumple	**Documentación:** Palo Alto - Premium Support https://bit.ly/3vDB5LG
RENDIMIENTO DE LOS EQUIPOS		
Deberá tener un rendimiento de Prevención de Amenazas de 5.6 Gbps medido con tráfico productivo real (transacciones usando una mezcla de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Seguridad del tráfico DNS, Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido al habilitar los módulos de seguridad indicados en el modo más alto de inspección. No se	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** Datasheet - PA-3400 Series https://bit.ly/3U0kuuL

aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242.		
No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de rendimiento con documentación pública del fabricante adjuntando el link que lo respalde.	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** Datasheet - PA-3400 Series https://bit.ly/3U0kuuL
Deberá tener núcleos dedicados para tareas de gestión del equipo, de manera independiente a los recursos de CPU para el procesamiento del tráfico. Esta arquitectura deberá estar integrada dentro del NGFW.	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** PA-Series Next-Generation Firewalls - Hardware Architectures - Palo Alto Networks https://bit.ly/43KlO8m
CAPACIDADES DE RED		
El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.	Cumple	Todas las funciones requeridas son soportadas. **Documentación:** • Configure an Aggregate Interface Group https://bit.ly/49r0k1j • Network – VLANs https://bit.ly/3J0yvSK • Policy-Based Forwarding https://bit.ly/43ltPus • Configure NAT https://bit.ly/3xoFwuo • How to Enable/Use/Disable/Check Jumbo Frame Support on a Palo Alto Networks Firewall https://bit.ly/3VJouB8 • Layer 3 Interface (sub-interfaces) https://bit.ly/3xhxW4G
Capacidad de etiquetas VLAN 802.1Q por equipo/interfaz: 4,094/4,094	Cumple	**Documentación:** Network – VLANs https://bit.ly/4aFvoLQ

Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).	Cumple	El equipo ofertado soporta la configuración de protocolos dinámicos de enrutamientos, los cuales son: OSPF, IBGP, EBGP y RIP. **Documentación:** Configure Virtual Routers https://bit.ly/3J31eq8
Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.	Cumple	**Documentación:** Tunnel Content Inspection Overview https://bit.ly/3IZ0vGC
Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.	Cumple	**Documentación:** Firewall Interfaces Overview **https://bit.ly/3xsgBG0**
Soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based forwarding, ECMP, dual-stack, QoS, DSCP, NPTv6, NAT64, LLDP, BFD, DHCPv6 Relay, SLAAC, SNMP.	Cumple	**Documentación:** Palo Alto Networks Compatibility Matrix, IPv6 Support by Feature **https://bit.ly/4ah8Wcp**
La plataforma propuesta por el fabricante debe contar con certificación USGv6-r1 para las pruebas de Firewall, IDS e IPS.	Cumple	**Documentación:** Palo Alto - The U.S. Government IPv6 (USGv6) **https://bit.ly/4aE95WZ**
ALTA DISPONIBILIDAD		
Debe soportar configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).	Cumple	**Documentación:** Palo Alto - High Availability https://bit.ly/3TKW07k
La configuración en alta disponibilidad debe sincronizar: sesiones, certificados de descifrado, configuraciones, incluyendo, más no limitado a políticas de seguridad, NAT, QoS y objetos de red.	Cumple	**Documentación:** Palo Alto - High Availability Synchronization https://bit.ly/3VJmwRs

Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.	Cumple	**Documentación:** Palo Alto - High Availability and Path Monitoring https://bit.ly/4cEvkxU
Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.	Cumple	**Documentación:** Palo Alto - High Availability Links and Backup Links **https://bit.ly/3PKwDS5**
La funcionalidad de clustering debe permitir incorporar al mismo tiempo dispositivos independientes, así como dispositivos configurados en HA	Cumple	**Documentación:** Palo Alto - High Availability Clustering Overview **https://bit.ly/3xj4Th9**
FUNCIONALIDADES DE FIREWALL		
Debe tener control de políticas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos).	Cumple	**Documentación:** Palo Alto - Components of a Security Policy Rule https://bit.ly/3PKBB1b
Debe permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.	Cumple	**Documentación:** Palo Alto - Network Security – Policy Object: Tags https://bit.ly/3xcMnXt
Debe realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).	Cumple	**Documentación:** Palo Alto - Commit, Validate, and Preview Firewall Configuration Changes https://bit.ly/3vMJL26
Debe mostrar la primera y última vez que se utilizó una regla de seguridad.	Cumple	**Documentación:** Palo Alto - Rule Usage Hit Count Query https://bit.ly/3xlDWJE
Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.	Cumple	**Documentación:** Palo Alto - Creating and Managing Policies https://bit.ly/3U0LAlj
Debe mostrar a través de un filtro, las reglas de seguridad que no han	Cumple	**Documentación:**

tenido uso en la red desde el último encendido del dispositivo firewall.		Palo Alto - Sorting and Filtering Security Policy Rules https://bit.ly/49ls1Zm
Debe permitir tener un registro de auditoría en cada política que permita conocer que cambios se realizó con anterioridad.	Cumple	**Documentación:** Palo Alto - Audit Comment Archive https://bit.ly/3xlu3vo
Debe permitir la definición de grupos dinámicos de direcciones IP, que permita colocar de manera automática direcciones IP en grupos de cuarentena si éstos realizan acciones maliciosas o restringidas. Estas acciones, deberán poder ser personalizadas en la consola del equipo.	Cumple	**Documentación:** Palo Alto - Use Dynamic Address Groups in Policy https://bit.ly/3J3Zo8A
Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoria.	Cumple	**Documentación:** Palo Alto - Audit Comment Archive https://bit.ly/3xlu3vo
DESCIFRADO DE TRÁFICO SSL/TLS		
Deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, RC4, AES128, AES256, CHACHA20-POLY1305; MD5, SHA1, SHA256, SHA384.	Cumple	**Documentación:** Palo Alto - SSL Protocol Settings Decryption Profile https://bit.ly/4cla2Q0
Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos y/o no fiables, a pesar de no descifrar el tráfico.	Cumple	La solución soporta la configuración de perfiles de SSL, en los cuales se puede seleccionar la visión de TLS, Key Exchange Algorithms, Encryption Algorithms y Authentication Algorithms a utilizar. **Documentación:** Palo Alto - SSL Protocol Settings Decryption Profile https://bit.ly/4cla2Q0
Debe soportar certificados que utilicen Subject Alternative Name (SAN) y Server Name Indication (SNI).	Cumple	**Documentación:** Palo Alto - SSL Decryption and Subject Alternative Names (SANs) https://bit.ly/3J4GXRi

Debe permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar excluir del descifrado a páginas con contenido sensible y descifrar el resto de las páginas.	Cumple	**Documentación:** Palo Alto - Create a Decryption Policy Rule https://bit.ly/3VKWmxG
Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado en base al Common Name del certificado.	Cumple	**Documentación:** Palo Alto - Decryption Exclusions https://bit.ly/43N9FiT
Debe contar con un dashboard que muestre gráficamente la proporción del tráfico descifrado, aplicaciones y dominios con descifrado correcto, errores de descifrado.	Cumple	**Documentación:** Palo Alto - Decryption Application Command Center Widgets https://bit.ly/3J9wB2d
Debe contar con un panel de logs dedicados a monitorear el tráfico de descifrado SSL/TLS, estos logs deberán permitir una identificación rápida de problemas del descifrado.	Cumple	**Documentación:** Palo Alto - Decryption Log https://bit.ly/3J5YEzP
Debe de permitir que desde su consola gráfica mostrar todo el detalle de la sesión SSL/TLS identificada, tales como IP origen y destino, subject common name, issuer common name, server name indication, datos del certificado digital (fecha de expiración, serial number), versión de TLS, algoritmo asimétrico, algoritmo simétrico, hash, estado del descifrado (correcto o con error), motivo del error del descifrado Este detalle de logs no deberá afectar el performance del equipo.	Cumple	**Documentación:** Palo Alto - Decryption Log https://bit.ly/3J5YEzP
PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS)		
Deberá poder definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood.	Cumple	**Documentación:** Palo Alto - DoS Protection Profiles https://bit.ly/3TGHsFN
Debe ser posible utilizar SYN Cookies como medida de defensa.	Cumple	**Documentación:** Palo Alto - DoS Protection Profiles https://bit.ly/3TGHsFN

Deberá tener la protección contra ataques Flood que deben ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor)	Cumple	**Documentación:** Palo Alto - DoS Protection Profiles https://bit.ly/3TGHsFN
Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo.	Cumple	**Documentación:** • Palo Alto - DoS Protection Profiles https://bit.ly/3TGHsFN • Host Sweep Triggering Method in Zone Protection Profile https://bit.ly/4aiVR2c
Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route.	Cumple	**Documentación:** Palo Alto - DoS Protection Profiles https://bit.ly/3TGHsFN
Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia dicho equipo.	Cumple	**Documentación:** Palo Alto - DoS Protection Profiles https://bit.ly/3TGHsFN
Debe proteger contra ataques basados en protocolos No-IP en interfaces Layer 2 (como Appletalks, Banyan, VINES, Novell, SCADA y otros), la solución deberá soportar la definición de protocolos a ser aceptados en base al formato Ethertype (Hex).	Cumple	**Documentación:** Palo Alto - Protocol Protection https://bit.ly/4aj5PAv
Se debe poder definir un horario para que automáticamente se aplique la regla de prevención contra ataques DoS	Cumple	**Documentación:** Palo Alto - How to Set Up DoS Protection https://bit.ly/3PM9BKs
La protección contra ataques Flood deberá permitir definir al menos 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS	Cumple	**Documentación:** Palo Alto - DoS Protection Profiles https://bit.ly/3TGHsFN
VISIBILIDAD EN CAPA 7 Y CONTROL DE APLICACIONES		

La solución propuesta deberá reconocer por lo menos 4000 aplicaciones, incluyendo, más no limitando a aplicaciones de tipo peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.	Cumple	**Documentación:** Palo Alto – Application Research Center (Applipedia). https://bit.ly/2JoYEhm
Las aplicaciones deberán estar clasificadas en al menos 30 tipos, de tal manera que se puedan configurar políticas en base al tipo de aplicación.	Cumple	**Documentación:** Palo Alto – Application Research Center (Applipedia). https://bit.ly/2JoYEhm
Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.	Cumple	**Documentación:** Palo Alto - Create a Decryption Policy Rule https://bit.ly/3VKWmxG
Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. Debe ser capaz de determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.	Cumple	**Documentación:** Palo Alto - App-ID Overview https://bit.ly/3THr48a
Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.	Cumple	**Documentación:** Palo Alto - Components of a Security Policy Rule https://bit.ly/3PKBB1b
Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación. Es decir, si 2 aplicaciones utilizan el mismo puerto y protocolo, se debe poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación. Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión.	Cumple	**Documentación:** Palo Alto - Components of a Security Policy Rule https://bit.ly/3PKBB1b

Deberá contar con un módulo de aprendizaje que permita migrar las políticas basadas en puertos específicos y políticas con puertos ALL/ANY, a políticas basadas en aplicaciones.	Cumple	**Documentación:** Palo Alto - Security Policy Rule Optimization https://bit.ly/3VPQvXA
El módulo de aprendizaje deberá ser específico por cada política de seguridad.	Cumple	**Documentación:** Palo Alto - Security Policy Rule Optimization https://bit.ly/3VPQvXA
El módulo de aprendizaje deberá mostrar el nombre de la(s) aplicación(es) que han pasado por una política de seguridad, fecha de primera y última ocurrencia y volumen de datos transferido por cada aplicación.	Cumple	**Documentación:** Palo Alto - Security Policy Rule Optimization https://bit.ly/3VPQvXA
Deberá contar con un wizard que permita convertir una política basada en puertos (capa 4) a una política basada en aplicaciones (capa 7) en base al aprendizaje realizado.	Cumple	**Documentación:** Palo Alto - Security Policy Rule Optimization https://bit.ly/3VPQvXA
El proveedor debe incluir en su propuesta los servicios de migración de todas las políticas de seguridad, reglas y objetos de nuestro firewall actual.	Cumple	
PREVENCION DE AMENAZAS		
La solución propuesta deberá contar con capacidades de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.	Cumple	**Documentación:** Palo Alto – Security Profile https://bit.ly/4agxr9x
La solución propuesta debe tener las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar de forma permanente, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.	Cumple	**Documentación:** Palo Alto - What Happens When Licenses Expire? https://bit.ly/3J3e2gf
La solución propuesta deberá soportar el throughput solicitado operando en el máximo nivel o modo	Cumple	**Documentación:** • Palo Alto - Single Pass Architecture https://bit.ly/3TGqaJa

de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.		• The Benefits of Palo Alto Networks Firewall Single Pass Parallel Processing (SP3) And Hardware Architecture https://bit.ly/3xjkxZV
La solución deberá identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que se pueda bloquear dichas consultas DNS.	Cumple	**Documentación:** Palo Alto – DNS Security https://bit.ly/3vssX0t
Deberá contar con un mecanismo que permita identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, inclusive si el tráfico entre la potencial víctima y su servidor DNS utilizado no pasa por el NGFW.	Cumple	**Documentación:** Palo Alto - Use the Compromised Hosts Widget in the ACC https://bit.ly/3J8dvti
Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), y también DNS sobre TLS.	Cumple	**Documentación:** Palo Alto - DNS Security Support for DNS Over HTTPS (DoH) https://bit.ly/3J1tglW
La solución propuesta debe proveer el módulo de IPS debe ser capaz de bloquear ataques en base a firmas, heurística y anomalías en el protocolo.	Cumple	**Documentación:** Palo Alto - Threat Signature Categories https://bit.ly/3THzGM6
El módulo de IPS deberá permitir personalizar firmas directamente desde la consola gráfica y ser capaz de identificar y bloquear amenazas avanzadas indetectables por firmas o heurística, incluyendo ataques de inyección y command and control realizados con herramientas de Cobalt Strike, Brute Ratel C4.	Cumple	**Documentación:** Palo Alto - Custom Application IDs and Signatures https://bit.ly/49nKxk6
La protección contra amenazas avanzadas indetectables por firmas, heurística o reputación del dominio o contenido deberá estar basado en mecanismos de inteligencia artificial, tales como deep learning y/o machine learning.	Cumple	**Documentación:** Palo Alto - Advanced WildFire https://bit.ly/3W1oHQv

Respecto a ataques de malware, las firmas deberán estar basadas en patrones y no únicamente en hashes, con el objetivo de identificar y bloquear el malware polimórfico que pertenezca a una misma familia.	Cumple	**Documentación:** Palo Alto - What is a Payload-Based Signature? https://bit.ly/49lcsB2
Con la finalidad de contar con una protección robusta contra amenazas emergentes a nivel mundial, la solución deberá ser capaz de actualizar su base de firmas de malware en tiempo real sin afectar el performance del equipo.	Cumple	**Documentación:** Palo Alto - WildFire Real-Time Signature Updates https://bit.ly/4cDoAQP
Deberá contar con un mecanismo basado en aprendizaje de máquina que sea capaz de analizar en tiempo real los archivos desconocidos no identificables por firmas ni heurística; el análisis deberá identificar si los archivos son maliciosos, en cuyo caso el equipo deberá bloquear su ingreso para evitar la infección por amenazas de día cero.	Cumple	**Documentación:** Palo Alto - Advanced WildFire https://bit.ly/3W1oHQv
Debe incorporar una plataforma de sandbox basada en nube para el análisis de ejecutables desconocidos.	Cumple	**Documentación:** Palo Alto – WildFire https://bit.ly/3vtKuFA
Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SFTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.	Cumple	**Documentación:** Palo Alto – Security Profile – Antivirus https://bit.ly/3J0IQ18
PREVENCIÓN DE AMENAZAS AVANZADAS EN DNS		
La plataforma deberá ser alimentada por un servicio de inteligencia global de amenazas capaz de identificar millones de dominios maliciosos con análisis en tiempo real.	Cumple	**Documentación:** Palo Alto – DNS Security - Cloud-Delivered DNS Signatures and Protections https://bit.ly/3PMcLOk
La protección del tráfico DNS deberá contar con mecanismos avanzados de protección, para identificar	Cumple	**Documentación:** Palo Alto – About DNS Security https://bit.ly/49u2aPm

ataques imposibles de mitigar con firmas y/o reputación del dominio. Para lo cual se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial.		
Deberá ser capaz de prevenir ataques como DGA (Domain Generation Algorithm) Random y de Diccionario, DNS Tunneling, Fast Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS.	Cumple	**Documentación:** • Palo Alto - Domain Generation Algorithm (DGA) Detection https://bit.ly/4cURWdN • Palo Alto - DNS Tunneling Detection https://bit.ly/3VFQFRl
Deberá soportar el manejo de excepciones para poder mitigar los falsos positivos.	Cumple	**Documentación:** Palo Alto - DNS Security - Create Domain Exceptions and Allow | Block Lists https://bit.ly/4akwxJ3
Deberá contar con dashboards y estadísticas sobre la cantidad, tipo de peticiones DNS, clasificación de la amenaza, generadas por los dispositivos internos de la Empresa/Institución.	Cumple	**Documentación:** Palo Alto - DNS Security - View DNS Security Logs https://bit.ly/3xnEC1a
El análisis del tráfico DNS podrá ser realizado de manera local en el mismo equipo, una solución externa (en nube u onpremise) del mismo u otro fabricante.	Cumple	
En caso de ser una plataforma en nube deberá estar certificado en SOC2 Tipo II de AICPA.	Cumple	**Documentación:** Product Certifications - Palo Alto Networks https://bit.ly/3J2OQqd
SANDBOXING		
La plataforma de Sandbox podrá ser ofrecido en Nube (Cloud), On-premise o ambos.	Cumple	**Documentación:** Palo Alto – WildFire https://bit.ly/3vtKuFA
Deberá ser capaz de emular el potencial malware en entornos Windows, Linux y MacOS.	Cumple	**Documentación:** Palo Alto – WildFire https://bit.ly/3vtKuFA
La solución propuesta deberá ser capaz de enviar 6,000 archivos por hora al sandbox.	Cumple	

El sandbox deberá ser capaz de analizar 6,000 archivos por hora realizando análisis dinámico del archivo (entiéndase por análisis dinámico aquel que no está basado en firmas, ni prefiltros, sino en emulación completa del potencial malware).	Cumple	**Documentación:** Palo Alto – Advanced WildFire - Firewall File Forwarding Capacity by Model https://bit.ly/3U0SK9c
Deberá realizar el análisis dinámico de forma paralela para todos los archivos enviados y no deberá tomar más de 10 minutos en dar un veredicto.	Cumple	**Documentación:** Palo Alto - Real Time WildFire Verdicts and Signatures for Documents https://bit.ly/4aldetb
En caso de tratarse de una plataforma de Sandbox Cloud, deberá cumplir con los siguientes requerimientos: • Deberá tener una disponibilidad de al menos 99.9% contabilizados mensualmente. • Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II Plus de AICPA, ISO 27001, ISO 27017 e ISO 27018.	Cumple	**Documentación:** Palo Alto – WildFire https://bit.ly/3vtKuFA
Debe proveer información forense sobre las acciones realizadas por el malware, tales como resumen del comportamiento visto, actividad sobre los archivos, peticiones DNS, conexiones de red, actividad de los archivos, procesos y registros. Esta información deberá poder ser extraída en un reporte PDF.	Cumple	**Documentación:** Palo Alto - Advanced WildFire - Advanced WildFire Analysis Reports—Close Up https://bit.ly/49rb2Fc
Deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.	Cumple	**Documentación:** Palo Alto – WildFire – Global URL Analysis https://bit.ly/3VMVwQP

Debe permitir al administrador la descarga del archivo original analizado por el sandbox.	Cumple	**Documentación:** Palo Alto - Advanced WildFire - Advanced WildFire Analysis Reports—Close Up https://bit.ly/49rb2Fc
Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.	Cumple	**Documentación:** Palo Alto - Advanced WildFire - Advanced WildFire Analysis Reports—Close Up https://bit.ly/49rb2Fc
Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico.	Cumple	**Documentación:** Palo Alto - Advanced WildFire - Manually Upload Files to the WildFire Portal https://bit.ly/3J4Jc70
Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.	Cumple	**Documentación:** Palo Alto – WildFire https://bit.ly/3vtKuFA
La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.	Cumple	**Documentación:** Palo Alto – WildFire https://bit.ly/3vtKuFA
FILTRO DE CONTENIDO WEB		
Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.	Cumple	**Documentación:** Palo Alto - Where Can I Find a Complete List of PAN-DB URL Filtering Categories? https://bit.ly/3VIAkvt
Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.	Cumple	**Documentación:** Palo Alto – URL Categories https://bit.ly/43II1EN
Debe soportar un cache local de URLs en el dispositivo, evitando el delay de comunicación/validación de las URLs	Cumple	**Documentación:** Palo Alto – Advanced URL Filtering https://bit.ly/3THyZSW
Debido a que diariamente se crean decenas de miles de nuevas páginas web, la solución deberá ser capaz de analizar en tiempo real si la página	Cumple	**Documentación:** Palo Alto – Advanced URL Filtering - Local Inline Categorization https://bit.ly/3vBY75q

web tiene contenido malicioso cuando un usuario intenta acceder.		
El análisis en tiempo real deberá determinar si la página web desconocida (no categorizada en la base de datos del fabricante), tiene contenido javascript malicioso, phishing, actividad de command and control y otros tipos de contenido malicioso.	Cumple	**Documentación:** Palo Alto – Advanced URL Filtering - Local Inline Categorization https://bit.ly/3vBY75q
Debe contar con medidas de antievasión como Cloaking, Captcha falsos, codificación de caracteres HTML, entre otros.	Cumple	**Documentación:** Palo Alto – Advanced URL Filtering https://bit.ly/3THyZSW
Debe permitir la creación de categorías personalizadas.	Cumple	**Documentación:** Palo Alto – Advanced URL Filtering - Create a Custom URL Category https://bit.ly/3J67ttr
Debe permitir la personalización de la página de bloqueo.	Cumple	**Documentación:** Palo Alto – Advanced URL Filtering - Customize the URL Filtering Response Pages https://bit.ly/3vAFa3c
Debe permitir notificar al usuario, mostrándole sólo una página de alerta personalizable, pero permitiéndole continuar la navegación al site.	Cumple	**Documentación:** Palo Alto - Advanced URL Filtering - URL Filtering Profiles https://bit.ly/3VJPu3E
Debe ser capaz de registrar el User-agent, Referer, XFF de cada sesión hacia internet	Cumple	**Documentación:** Palo Alto - Advanced URL Filtering - HTTP Header Logging **https://bit.ly/49g1KMc**
Debe ser capaz de forzar la navegación de los usuarios en el modo Safe Search Enforcement.	Cumple	**Documentación:** Palo Alto - Advanced URL Filtering - Safe Search Enforcement https://bit.ly/3vqMw9u
Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de robo de credenciales.	Cumple	**Documentación:** Palo Alto - Prevent Credential Phishing https://bit.ly/43JaQQs
IDENTIFICACION DE USUARIOS		

Debe permitir la creación de políticas de seguridad basadas en la identidad del usuario y grupo al cual pertenece, a través de la integración de servicios de autenticación como Active Directory, Novell eDirectory, Open LDAP y base de datos local.	Cumple	**Documentación:** Palo Alto - Authentication Profile https://bit.ly/4az8vd0
Debe contar con varios mecanismos para la identificación del usuario y la dirección IP del equipo en donde se encuentra autenticado. Como mínimo deberá poder integrarse a las siguientes plataformas para cubrir este requerimiento: • Eventos de login gestionados en Domain Controller y/o Microsoft Exchange. • Capacidad de leer eventos de login y logout usando el protocolo WinRM. • Terminal Server de Microsoft o Citrix • Consultando directamente a cada estación de trabajo a través del protocolo WMI • Lectura de la cabecera XFF al integrarse con soluciones terceras de Proxy • Capacidad de extraer la información de IP y usuarios a través de la lectura y extracción de datos del tráfico syslog. • Integración con soluciones de Wireless LAN Controller basadas en 802.1x y Soluciones NAC, con el objetivo de que el NGFW no dependa del Domain Controller para identificar al usuario. • A través de agentes instalados en las estaciones de trabajo, que reporten directamente al	Cumple	**Documentación:** • Palo Alto - Configure the Windows User-ID Agent for User Mapping https://bit.ly/4cDv16r • Palo Alto Networks Compatibility Matrix - Terminal Server (TS) Agent https://bit.ly/3TLqA0C • Forescout and Palo Alto Networks https://bit.ly/4ahN2W9 • Map IP Addresses to Users https://bit.ly/4cGm7VE

NGFW el usuario y dirección IP de cada equipo.		
Deberá contar con un componente que permita integrarse a diversas plataformas de identidades tales como Azure AD, Google Directory, Okta, Cisco Duo, PingID.	Cumple	**Documentación:** Palo Alto - Cloud Identity Engine https://bit.ly/3vFHgyH
Debe contar con la funcionalidad de Portal Captivo (Captive Portal), de tal manera que el NGFW muestre un portal al usuario para que se autentique manualmente. Las cuentas podrán ser definidas localmente en el NGFW o integradas con plataformas terceras.	Cumple	**Documentación:** Palo Alto - How to Configure Captive Portal https://bit.ly/3U15rB1
Debe tener integración con plataformas de MFA (Multi Factor Authentication), de tal forma que cuando un dispositivo requiera acceder a recurso, se le solicite el OTP.	Cumple	**Documentación:** Palo Alto - Configure Multi-Factor Authentication https://bit.ly/3vsBEb7
Debe permitir la definición de grupos dinámicos de usuarios, que permita colocar de manera automática a los	Cumple	**Documentación:** Palo Alto - Dynamic User Groups https://bit.ly/4aI8Pq5

usuarios en grupos de cuarentena si éstos realizan acciones maliciosas o restringidas. Estas acciones, deberán poder ser personalizadas en la consola del equipo.		
VERIFICACIÓN DE LA POSTURA DE SEGURIDAD DEL ENDPOINT		
A través de políticas de seguridad, el NGFW deberá ser capaz de validar si el equipo que intenta acceder a algún recurso de red (IP o IPs destino) cuenta con una postura de seguridad adecuada.	Cumple	**Documentación:** Palo Alto - GlobalProtect - HIP Objects https://bit.ly/3U31aMr
La restricción al recurso de red debe ser personalizable, es decir, el NGFW deberá permitir acceder de manera total o parcial al recurso de red destino en base al nivel de cumplimiento de la postura de seguridad del equipo. Por ejemplo, si cumple parcialmente con la postura de seguridad únicamente se le dará acceso para hacer PING a un servidor, sí cumple completamente podrá acceder vía RDP.	Cumple	**Documentación:** Palo Alto – GlobalProtect - Configure HIP-Based Policy Enforcement https://bit.ly/49gxXmE
La validación de la postura de seguridad del endpoint deberá ser continua; el NGFW automáticamente deberá restringir el acceso si es que luego de la conexión establecida el equipo modifica su postura de seguridad.	Cumple	**Documentación:** Palo Alto – GlobalProtect - Configure HIP-Based Policy Enforcement https://bit.ly/49gxXmE
Como mínimo la postura de seguridad del endpoint deberá validar lo siguiente: • Sistema operativo del equipo. • Serial number del equipo. • Pertenencia al dominio corporativo • Software antivirus instalado y habilitado en tiempo real. • Software antivirus con la base de datos de firmas actualizada en un número de días personalizable	Cumple	**Documentación:** Palo Alto - GlobalProtect - HIP Objects https://bit.ly/3U31aMr

• Haber realizado un escaneo del malware en un equipo dentro de un número de días personalizable • Marca del software antivirus. • Parche de seguridad instalado, según su nivel de criticidad. • Firewall de host habilitado. • Software de cifrado de disco instalado. • Software de DLP instalado. • Permitir validaciones personalizadas en base a registros de REGEDIT.		
Las políticas de validación de postura del endpoint deben poder ser aplicadas a un grupo de usuarios o direcciones IP.	Cumple	**Documentación:** Palo Alto – GlobalProtect - Configure HIP-Based Policy Enforcement https://bit.ly/49gxXmE
Deberá permitir configurar un mensaje personalizado, el cual permita notificar al usuario que controles no está cumpliendo.	Cumple	**Documentación:** Palo Alto - HIP Notification Tab https://bit.ly/3TLYSB5
Esta verificación se podrá realizar a través de un agente instalado en los endpoints. Debe tener soporte como mínimo para Windows y MacOS.	Cumple	**Documentación:** Palo Alto - Where Can I Install the GlobalProtect App? https://bit.ly/3vN8AuO
La solución podrá integrarse a una plataforma de Network Access Control (NAC) para cumplir los requerimientos listados. Se deja libertad al postor de elegir la plataforma NAC que se pueda integrar. Tales como • Forescout • Aruba • Cisco ISE	Cumple	**Documentación:** • ForeScout Extended Module for Palo Alto Networks Next-Generation Firewall https://bit.ly/3VLPEr0 • Aruba - ClearPass and Palo-Alto Networks Integration TechNote https://bit.ly/3J69TZ3 • Palo Alto - Configure Cisco ISE with RADIUS for Palo Alto Networks https://bit.ly/4ae5lf0
Esta capacidad deberá tener cobertura dentro de la red interna, sin necesidad de hacer túneles VPN.	Cumple	**Documentación:** Palo Alto – GlobalProtect - GlobalProtect Gateways https://bit.ly/4aFDgwU
QOS		

Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix), se requiere que la solución tenga la capacidad de controlarlas a través de políticas personalizables.	Cumple	**Documentación:** Palo Alto - QoS Policy https://bit.ly/43JE5T8
Soportar la creación de políticas de QoS por: dirección de origen y destino, por grupo de usuario de LDAP, por aplicaciones, por puerto.	Cumple	**Documentación:** Palo Alto - QoS Overview https://bit.ly/3xiZsyK
El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.	Cumple	**Documentación:** Palo Alto – QoS Classes https://bit.ly/3U1SHtV
Soportar marcación de paquetes DSCP, inclusive por aplicaciones.	Cumple	**Documentación:** Palo Alto - Enforce QoS Based on DSCP Classification https://bit.ly/4cHOz9B
Permitir el monitoreo en tiempo real del tráfico gestionado por el QoS.	Cumple	**Documentación:** Palo Alto – QoS Statistics https://bit.ly/4aBy6Cb
FILTRO DE DATOS		
Los archivos deben ser identificados por extensión y firmas.	Cumple	**Documentación:** Palo Alto – Set Up File Blocking https://bit.ly/3U287hG
Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro).	Cumple	**Documentación:** Palo Alto – Set Up File Blocking https://bit.ly/3U287hG
Permitir, identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.	Cumple	**Documentación:** Palo Alto - Data Pattern Settings https://bit.ly/3U3S3Lt
VPN		
Rendimiento de VPN 6.8 Gbps.	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:**

		Datasheet - PA-3400 Series https://bit.ly/3U0kuuL
Soportar VPN Site-to-Site en protocolo IPSec.	Cumple	El equipo propuesto, es el PA-3410, el cumple con los requerimientos realizados. **Documentación:** Datasheet - PA-3400 Series https://bit.ly/3U0kuuL
La VPN site to site debe soportar como mínimo: • DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard) • Autenticación MD5, SHA-1, SHA-2; • Diffie-Hellman Group 1, Group 2, Group 5 y Group 14. • Algoritmo Internet Key Exchange (IKEv1 & IKEv2);	Cumple	**Documentación:** • Palo Alto - Define IKE Crypto Profiles https://bit.ly/3VKVau2 • Palo Alto - Define IPSec Crypto Profiles https://bit.ly/3xe4cFB
Debe permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.	Cumple	**Documentación:** Palo Alto - Security Policies Based on Zone Assignment for VPN Tunnel Interface https://bit.ly/4aA1RmI
Debe permitir aplicar QoS dentro de los túneles VPN.	Cumple	**Documentación:** Palo Alto - Applying QoS on Tunnel Interfaces **https://bit.ly/49pbUKD**
Debe soportar VPN client-to-site pudiendo operar usando el protocolo IPSec o SSL.	Cumple	**Documentación:** Palo Alto - How to Confirm if GlobalProtect Tunnel is Using IPSec or SSL? **https://bit.ly/3PMmjsK**
Debe soportar la conexión por medio de agente instalado en el sistema operativo.	Cumple	**Documentación:** Palo Alto - GlobalProtect App https://bit.ly/3U4dtJA
Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS.	Cumple	**Documentación:** Palo Alto – Supported GlobalProtect Authentication Methods https://bit.ly/3U1YQGn

Capacidad de integrarse con plataformas de Doble Factor de Autenticación (2FA).	Cumple	**Documentación:** Palo Alto – Supported GlobalProtect Authentication Methods https://bit.ly/3U1YQGn
Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.	Cumple	**Documentación:** Palo Alto - Configure a Split Tunnel Based on the Access Route **https://bit.ly/3PPfnei**
Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN, incluyendo el soporte de Split DNS.	Cumple	**Documentación:** Palo Alto - Configure a Split Tunnel Based on the Access Route **https://bit.ly/3PPfnei**
El Split Tunnel debe permitir elegir el tipo de tráfico que se enrutará por el túnel VPN, basado en el nombre de la Aplicación y el Dominio.	Cumple	**Documentación:** Palo Alto - Configure a Split Tunnel Based on the Access Route **https://bit.ly/3PPfnei**
Debe permitir los siguientes tipos de conexión del cliente al túnel VPN: • Antes de que el usuario se autentique en la estación. • Después de la autenticación del usuario en la estación usando Single Sign On (SSO). • A demanda, de forma manual por parte del usuario.	Cumple	**Documentación:** • Palo Alto – GlobalProtect - GlobalProtect Always on VPN Configuration https://bit.ly/3PPK0Ap • Palo Alto – GlobalProtect – GlobalProtect - Remote Access VPN with Pre-Logon **https://bit.ly/3TGPGhj**
El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y IOS	Cumple	**Documentación:** Palo Alto - Where Can I Install the GlobalProtect App? https://bit.ly/3vN8AuO
La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada, de manera manual y automática. Los equipos en cuarentena no deberán tener conexión con ningún recurso de red protegido por la solución.	Cumple	**Documentación:** Palo Alto – GlobalProtect - Quarantine Devices Using Host Information **https://bit.ly/3xjZExA**
Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado, que permita validar determinadas características del equipo y en base al nivel de cumplimiento del host permitir,	Cumple	**Documentación:** Palo Alto - GlobalProtect - HIP Objects https://bit.ly/3U31aMr

denegar o limitar el acceso a los recursos de la red interna. Por lo menos se deberá poder configurar los siguientes casos de uso y una combinación de ellas: • Sistema operativo del equipo • Serial number del equipo • Pertenencia al dominio corporativo • Software antivirus instalado y habilitado en tiempo real • Software antivirus con la base de datos de firmas actualizada en un número de días personalizable • Haber realizado un escaneo del malware en un equipo dentro de un número de días personalizable • Marca del software antivirus • Parche de seguridad instalado, según su nivel de criticidad • Firewall de host habilitado • Software de cifrado de disco instalado • Software de DLP instalado • Permitir añadir validaciones de aplicaciones personalizadas añadiendo la Clave de Registro (en caso de Windows) o Plist (en caso de MacOS) • Este control deberá estar disponible al menos para equipos Windows y MacOS. • Todos los parámetros indicados deberán poder ser realizados desde la consola		

gráfica de la plataforma. No se aceptarán configuraciones a través de CLI.		
CAPACIDADES DE OPTIMIZACIÓN		
Como parte de la propuesta, se deberá proporcionar hasta 10 cuentas de acceso al portal oficial de educación del fabricante, para acceder, de manera gratuita, a cursos en línea sobre sus diversas tecnologías.	Cumple	
Se deberá incluir una herramienta integrada y/o externa que genere alertas si existen problemas de salud del equipo en materia de hardware y software, como mínimo: consumo de memoria, problemas de la alta disponibilidad (HA), problemas de disco duro, firmware vulnerable, firmware cerca a la obsolescencia, expiración de licencias.	Cumple	**Documentación:** Palo Alto - Next-Generation Firewall Free and Premium Features https://bit.ly/3xj8A6d
Con el objetivo de que la Empresa/Institución cuente con **autonomía para evaluar si el NGFW se encuentra configurado acorde a las buenas prácticas. El oferente debe proveedor debe incluir una herramienta que permita evaluar automáticamente si el NGFW se encuentra** configurado acorde a las buenas prácticas del fabricante en materia de los diferentes módulos de seguridad que se le haya activado.	Cumple	**Documentación:** Palo Alto - Next-Generation Firewall - On-Demand BPA Report https://bit.ly/3vGJH47
Esta herramienta deberá ser única y consolidar la información de todos los NGFW por adquirir en el presente proyecto.	Cumple	**Documentación:** Palo Alto - Next-Generation Firewall - AIOps for NGFW https://bit.ly/4cLgN3l
Debe contar con gráficos ejecutivos que permitan mostrar el nivel de adopción de los módulos de seguridad del NGFW en las políticas de seguridad.	Cumple	**Documentación:** Palo Alto - Next-Generation Firewall - AIOps for NGFW https://bit.ly/4cLgN3l

Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red.	Cumple	**Documentación:** Palo Alto - Security Policy Rule Optimization https://bit.ly/3VPQvXA
Debe identificar automáticamente las políticas abiertas que no tengan restricciones de puertos y/o aplicaciones (ANY o ALL), con el objetivo de corregirlas y hacer cumplir el principio de mínimo privilegio.	Cumple	**Documentación:** Palo Alto - Security Policy Rule Optimization https://bit.ly/3VPQvXA
Debe identificar las reglas superpuestas (shadowed rules), los cuales representen un riesgo de seguridad al permitir mayores accesos que los autorizados.	Cumple	**Documentación:** Palo Alto - Security Policy Rule Optimization https://bit.ly/3VPQvXA
La herramienta podrá estar integrada al NGFW o externa, ya sea de la misma marca u otra que se puede integrar.	Cumple	**Documentación:** Palo Alto - Security Policy Rule Optimization https://bit.ly/3VPQvXA
PROTECCIÓN PARA AMBIENTES EN LA NUBE		
Se deberá incluir un firewall para desplegar en ambientes de nube pública, como Azure, AWS o GCP del mismo fabricante.	Cumple	**Documentación:** Palo Alto - VM-Series Virtual Next-Generation Firewalls **https://bit.ly/3J5Wj88**
La solución de protección de ambiente en la nube debe de cumplir con los mismos requerimientos que los NGFW físicos	Cumple	Las funcionalidades de los NGFWs son las mismas, independientemente de su forma (físico, virtual, contenerizado).
El firewall virtual debe contar con las siguientes capacidades: • 1.4 Gbps de NGFW (capa 7) • 4 vCPUs • 16GB de memoria	Cumple	Estos requerimientos son cubiertos con el VM-100, el cual esta dentro de nuestra propuesta. **Documentación:** Palo Alto - VM-Series on Microsoft Azure Performance and Capacity https://bit.ly/49hA3Ti
El firewall virtual debe ser escalable a medida que los requerimientos de inspección de tráfico aumenten o se requieran agregar capacidades adicionales. No se aceptarán modelos virtuales fijos que exijan un reemplazo de estos en caso de no permitir crecimiento alguno.	Cumple	El esquema de licenciamiento basado en créditos permite la escalabilidad de los FWs, de tal manera de que no se requiera reemplazar en caso de que se necesite mayor capacidad de procesamiento. **Documentación:** Palo Alto - VM-Series Deployment Guide - Software NGFW Credits

		https://bit.ly/3VLugSW
LICENCIAMIENTO		
Licenciamiento por suscripción para 64 créditos	Cumple	**Documentación:** Palo Alto - VM-Series Deployment Guide - Software NGFW Credits https://bit.ly/3VLugSW
ADMINISTRACIÓN Y MONITOREO		
Se deberá incluir una consola para la centralización de gestión de múltiples NGFWs del mismo fabricante.	Cumple	**Documentación:** Palo Alto – Panorama https://bit.ly/4anqCDg
La consola de gestión debe soportar los siguientes ambientes virtuales: • VMware • Hyper-V • Hipervisores basados en KVM	Cumple	**Documentación:** Palo Alto – Panorama https://bit.ly/4anqCDg
La consola de gestión centralizada debe cumplir, como mínimo, con los siguientes requerimientos técnicos: • 32GB de memoria • 16 CPUs virtuales • 2TB para almacenamiento de bitácoras	Cumple	**Documentación:** Palo Alto - Panorama Administrator's Guide - Setup Prerequisites for the Panorama Virtual Appliance https://bit.ly/3TI7Ten
Debe permitir cambiar de contextos, para manejar los NGFWs en distintos grupos o de manera individual. Esto con el objetivo de aplicar objetos y políticas de manera jerárquica o individualmente en cada firewall gestionado.	Cumple	**Documentación:** Palo Alto - Panorama - Device Groups https://bit.ly/3TYHLgB
Debe permitir el uso de variables para permitir la reutilización de objetos y políticas alrededor de los firewalls gestionados.	Cumple	**Documentación:** Palo Alto – Panorama – Templetes Variables https://bit.ly/4cJ0pjV
Debe reportar estadísticas de los firewalls gestionados, incluyendo, pero no limitándose a: • Rendimiento. • Cantidad de sesiones. • Uso de interfaces.	Cumple	**Documentación:** Palo Alto – Monitor Device Health https://bit.ly/4cA9R9c

• Consumo de CPUs del plano de gestión. • Consumo de CPUs del plano de datos.		
Debe identificar los dispositivos comprometidos a partir de actividad de botnets o C&C, y tener la capacidad de aislar estos dispositivos de manera automática a través de políticas de seguridad transversales a todos los firewalls gestionados.	Cumple	**Documentación:** Palo Alto – Use the Compromised Hosts Widget in the ACC https://bit.ly/3J8dvti
La consola de gestión centralizada debe contar con conectores para integración de múltiples tecnologías y proveedores de servicios de nube privada y pública, como herramientas de NAC, VMware, Azure, AWS, Nutanix, Openstack, entre otras. Estos conectores no deben representar un costo adicional en las licencias	Cumple	**Documentación:** Palo Alto - Palo Alto Networks Compatibility Matrix - Panorama Plugins https://bit.ly/43Jk1jO
Debe permitir aplicar políticas individuales por cada administrador, en vez de aplicar todas las políticas que estén guardadas en la configuración general de la misma. Esto para evitar cambios no deseados o no autorizados por otros administradores de la plataforma.	Cumple	**Documentación:** Palo Alto - Panorama Administrator's Guide - Manage Locks for Restricting Configuration Changes https://bit.ly/3xunhDv
La consola de gestión centralizada debe permitir la calendarización de la aplicación de políticas, esto para permitir mayor flexibilidad en ventanas de mantenimiento o controles de cambio.	Cumple	**Documentación:** Palo Alto - Panorama Administrator's Guide - Schedule a Configuration Push to Managed Firewalls https://bit.ly/3U2YPlE
LICENCIAMIENTO		
software de gestión central, 25 dispositivos (3 años de suscripción)	Cumple	Incluido en la propuesta.
REQUERIMIENTOS PARA EL OFERENTE		
• Características detalladas de los equipos y soluciones ofertada.	Cumple	

• Certificación de la casa matriz que indique que los equipos ofertados son nuevos (no remanufacturados). • Certificación de la casa matriz (de la marca propuesta), indicando que el proveedor está autorizado a comercializar sus productos. • Tiempo de entrega 60 días. • El oferente debe mostrar evidencias de instalaciones similares de los equipos propuestos en instituciones de gobierno.		