ANEXO CONVOCATORIA

1/2018

RENGLONES

Renglón	Especificación Técnica	Imagen
1	• Unidad de procesamiento: • Intel Core I5 7200U o superior(NO Atom, NO Celeron). • Memoria: • Memoria: Tipo DDR4 2133 o superior. • Capacidad: 8Gb. Instalados. • Almacenamiento: • Disco Duro tipo Serial ATA 500Gb o superior. • Video: • Controlador de video con acceso a memoria RAM (ya sea independiente o tomada de la memoria principal) no inferior de 512MB, arquitectura PCI, PCI-E o AGP. • Audio: • Placa de sonido (o chipset integrado) de 16bit, frec. de muestreo no inferior de 48K • Conectores para linea de entrada, micrófono y salida para auricular/bocinas externas. • Bocinas internas 1 como mínimo. • Networking y comunicaciones: • Interface de red ethernet integrada(interna), con las siguientes características: • Bit rate 10/100/1000Mbps (autosensing). • Estandard: IEEE 802.3i 10BaseT, IEEE802.3u 100BaseTX. • Conexión UTP-RJ45. • Capacidad de operación full duplex • Driver para manejar Windows: 2000, XP, Vista, 7 y Linux. • Interface de Red WiFi (WLAN) interna con antena integrada con las siguientes características: • Conexión inalambrica por Aire.	

Renglón	Especificación Técnica	Imagen
1	• Bit rate de 54Mbps, con interfaz de aire OFDM (IEEE 802.11b/g/n). • Soporte de canal de encriptación WEP de 64/128 bit, WPA, WAP2. • Driver para manejar Windows: 2000, XP, Vista, 7 y Linux. • Dispositivos de interfaz humana: • Teclado tipo qwerty de por lo menos 79 teclas. Teclas de cursor separadas en forma de “T” invertida. Teclado numérico incorporado seleccionable por tecla de función o combinación similar. • Dispositivo de señalamiento de tipo mouse o similar (trackball, trackpoint, touchpad, mini-joistick, etc.) con una sensibilidad no menor a 200 unidades por pulgada. • Mouse óptico externo 2.4Ghz, con conexión inalambrica a través de receptor USB reducido. • Pantalla incorporada: • Tipo color LCD de matriz activa , TFT o LED. • Resolución: no inferior a 1920 x 1080 pixels. • Tamaño diagonal de pantalla no inferior a 14”. • Debe poseer conector D-Sub15 o DVI, con salida de video SVGA, activa en forma simultanea con la visualización de pantalla incorporada. • Puertos incorporados y periféricos: • 1 puerto USB 2.0. • 1 puerto USB 3.0. • 1 puerto para conexión de monitor externo (opcional). • 1 puerto HDMI. • Interfaz para dispositivo de señalamiento externo (podrá utilizarse uno de los puertos USB) • Interfaz para conexión de teclado externo (podrá utilizarse uno de los puertos USB). • Cámara Web incorporada al equipo con las siguientes características: • Debe permitir la toma de videos, así como la de instantáneas. • Sensor de imagen con una resolución no inferior a los 1280x720pixels (1.3M pixels) • Formato de video: 320x240 a 30 fps (cuadros/seg) y 640x480 a 15fps o superior. • Driver para manejar Windows XP, Vista, 7, 8, 10 y Linux. • Lector de tarjetas de memoria SD	

Renglón	Especificación Técnica	Imagen
1	incorporado. • Sistema Operativo y Software pre-instalado(alguno de los siguientes): • Windows 10 Home o superior. • Alimentación Portabilidad y ahorro de energía: • Alimentación por baterías recargables de níquel-cadmio (NiCd), níquel-hidruro metálico (NiMH), Li-Ion o similar, 4 celdas o superior, y directamente del suministro de red pública (a través del alimentador/cargador), 110V/220V. • Peso: no superior a 1,4 Kg (no incluyendo la batería y el transformador). • Duración de la batería: superior a 6 horas (en condiciones de uso permanente). • Deberá contar con configuración para programar el apagado automático de pantalla, disco duro y otros dispositivos, transcurrido un tiempo sin actividad determinable por el operador. • Deberá contar con características de modo de suspensión y/o backup automático de los archivos abiertos transcurrido un cierto tiempo sin actividad determinable por el operador, y/o cuando el nivel de batería haya descendido a niveles peligrosos. • Se deberá indicar toda otra característica adicional de ahorro de energía. • Un (1) alimentador para recarga de baterías y conexión directa a la red de suministro, con capacidad de detectar automáticamente las características de la corriente alterna (voltaje y frecuencia). • Plazo de garantía no inferior a los 12 meses certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). El proveedor debe ser el representante o distribuidor autorizado de todas las partes que componen el equipo y la garantía debe comprender al equipo con todas sus partes como un todo.	
2	• Resolución de pantalla hasta 1080p/30 (1920 x 1080 píxeles a una progresión de 30 fps) desde 720p/30. • Cámara de alta definición PTZ (panorámica – inclinación – zoom) con exposición automática que soporte formato de hasta 1080p30 y un campo mínimo horizontal de visión de 70°, un zoom óptico de al menos 10 y un rango mínimo de panorámica	

Renglón	Especificación Técnica	Imagen
2	de +/90° y de inclinación +/20°. Los parámetros de la cámara deberán poder configurarse en la interfaz de usuario del sistema de VC. • Deberá soportar dos pantallas y soportar funciones de video dual tanto en H.323 (H.239) y SIP(basado en BFCP). Se deberá poder configurar la posición del contenido y del video en vivo en las pantallas disponibles. • Deberá soportar las normas ITU-T H.264, H.264 High Profile para video y las normas ITU-T G.711, G.722, G.722.1. • Deberá contar con audio de banda completa (20 kHz) y soportar normas ITU (G.719). • Deberá incluir 2 altavoz y 2 micrófonos digitales adicionales, con cobertura 360° provistos a través de un arreglo multimicrofono de por lo menos 3 micrófonos. Cada micrófono deberá contar con cancelación de eco independiente. • Deberá poder capturar contenido de alta definición de una computadora portátil / PD / fuente DVI hasta 1920 x 1080 a 60 fps. • Deberá proveer capacidad de enviar / recibir de manera simultánea video de 1080p/30 en el canal principal y video de 1080p/30 en el canal de video dual y ser capaz de el contenido a una resolución completa en el segundo monitor, cuando esté disponible. • El usuario deberá poder definir la relación entre el ancho de banda utilizado para video y presentaciones en vivo. • Deberá soportar AES128 para el canal de video de la sala y el canal de video del contenido de manera simultánea. • Deberá proveer herramientas de seguridad para la autenticación e integridad (para SIP requiera HTTP Digest MD5, para H.323 requiere H.235 MD5 y H.235). • Deberá brindar soporta a IPv4 e IPv6 de forma simultánea y herramientas de QOS. • Deberá contar con al menos 1 puerta de red LAN 10/100/1000. • Deberá contar con soporte al os servicios de directorio LDAP / H.350 con un servidor LDAP integrado y cliente LDAP(para acceso a servidores remotos). • Deberá disponer de interfaz web de administración completa del equipo y con capacidad de proveer capturas de al menos la visualización de la cámara local.	

Renglón	Especificación Técnica	Imagen
2	• Deberá proveer herramientas de administración del administrador de red para controlar y administrar videoconferencias • Deberá soportar firewall transversal H.460.18/.19. • La interfaz de entrada y salida de audio deberá soportar tanto formato digital como análogo. • Deberá disponer de puertos USB y permitir la grabación de conferencias mediante dichos puertos USB. • Deberá contar con soporte a MCU interno de hasta 9 participantes en 1080p (no se requieren las licencias para habilitar dicho soporte). • Deberá contar con su correspondiente fuente de alimentació 100 - 240 VAC, 50/60 Hz. • Garantía: 1 año sobre todo el hardware con reemplazo de partes.	
3	• Inteligente/SMART • Pantalla: LED 55'' Full HD o superior • Resolución: 1920 x 1080 • Sonido: 10w x 2 parlantes integrados, Dolby digital plus, Dolby pulse, DTS Studio Sound, DTS Premium Audio 5.1 • Salida: Ethernet LAN x 1 y LAN inalámbrica integrada • Interfaz: HDMI x 3, RF in x 2 (antena y cable), USB x 2, Componente entrada (Y/Pb/Pr) x 1, Compuesto entrada (AV) x Entrada Audio (Mini Jack) x 1, Entrada Auriculares x 1. • Se debe proveer soporte para pared. • Debe incluir control remoto, manuales de usuario. • Garantía: 1 año.	
4	• Tecnología: Ultrium 15000 • Capacidad nativa / comprimida 2:1 : 6 Tb/ 15Tb • Máxima transferencia de datos (Compresión 2:1) 300Mb/s • Interface: 8Gb/sec FC • Cable de conexión incluir de acuerdo a especificaciones • Capacidad interna de alojamiento de cintas: 8 unidades (con recambio automatizado y programable) • Capacidad interna de alojamiento de drives: 1 unidad	

Renglón	Especificación Técnica	Imagen
4	• Gabinete: Formato rack, 1(una) U. Debe incluir los accesorios para su correcta disposición en rack • Debera incluir la interface, cable/s y accesorio/s que garanticen la conectividad con servidores HP DL 380G9, HP 3Par. • Lector de código de barras integrado • Manejo remoto a través de consola Web • Encriptación: AES 256bits por hardware con compresión • Se deberán incluir 30(treinta) Media(cintas LTO7) 6TB RW y 1(uno) Media para limpieza • 1 Sobre de 30 etiquetas(minimo) con codigos de barras para identificacion de carretes LTO-7. • Compatible con Veam Backup Versión 9.5 o superior. • Plazo de garantía no inferior a los 36 meses certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). El proveedor debe ser el representante o distribuidor autorizado de todas las partes que componen el equipo y la garantía debe comprender al equipo con todas sus partes como un todo. • Plazo de entrega 60 días.	
5	• Tape Backup Externa Tecnologia SAS LTO-7 Ultrium 15000, con sus correspondientes cables de energia y datos. • Capacidad interna de alojamiento de cintas: 1 unidad. • Se deberá incluir Placa controladora SAS para conexión a servidores HP DL380 G9 con sus correspondientes cables. • Se deberán incluir 20(diez) Media(cintas LTO7) 6TB RW y 1(uno) Media para limpieza • 1 Sobre de etiquetas con codigos de barras para identificacion de carretes LTO-7.Compatible con Veam Backup Versión 9.5 o superior. • Plazo de garantía no inferior a los 36 meses certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). El proveedor debe ser el representante o distribuidor autorizado de todas las partes que componen el equipo y la garantía debe comprender al equipo con todas sus partes como un todo. • Plazo de entrega 60 días.	
6	• Capacidad Util: 12TB (mínimo) • Velocidad de transferencia mínima de datos:	

Renglón	Especificación Técnica	Imagen
6	6.4TB/hr. • Compatibilidad certificada con Veeam Backup &Replication para deduplicación en origen , Veeam vPower NFS. • Conectividad: 4 x 1Gb Ethernet por controladora. • Tipo de discos: LFF SAS 7200 RPM o superior 6 Gb transfer rate. • Factor de forma: 1U (mínimo). • Tipo de target soportados para backup: NAS (CIFS/NFS), e iSCSI/FC VTL. • Capacidad de optimizar el almacenamiento de datos redundantes mediante deduplicación y compresión por hardware. • Emulación de librerías : HPE LTO-2/LTO-3/LTO-4/LTO-5/LTO-6 Ultrium Tape Drives in MSL2024 Tape Library, MSL4048 Tape Library • Fuente de alimentación redundante de 500W Flex Slot Platinum Hot Plug Power Supply . • Deberá contar con cables de alimentación C13. • Debe incluir los accesorios necesarios para montaje en rack standard 19" • Plazo de garantía no inferior a los 36 meses certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). El proveedor debe ser el representante o distribuidor autorizado de todas las partes que componen el equipo y la garantía debe comprender al equipo con todas sus partes como un todo. • Plazo de entrega 60 días.	
7	Solución UTM/NGFW con las siguientes características: • Throughput de por lo menos 24 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete. • Soporte a por lo menos 5M conexiones simultaneas. • Soporte a por lo menos 270K nuevas conexiones por segundo. • Throughput de al menos 20 Gbps de VPN IPSec. • Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos. • Estar licenciado para, o soportar sin necesidad de licencia, 50K túneles de clientes VPN IPSec simultáneos.	

Renglón	Especificación Técnica	Imagen
7	• Throughput de al menos 2,2 Gbps de VPN SSL. • Soportar al menos 5000 clientes de VPN SSL simultáneos. • Soportar al menos 7 Gbps de throughput de IPS. • Soportar al menos3,5 Gbps de throughput de Inspección SSL. • Throughput de al menos 3 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la solución de seguridad tenga debidamente activadas y operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado múltiples números de desempeño para cualquiera de las funcionalidades, solamente el de valor más pequeño será aceptado. • Tener al menos 8 interfaces 1Gbps sobre Fibra. • Tener al menos 8 interfaces 1Gbps sobre Cobre • Disco de 100GB para almacenamiento de información local. • Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance • Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance. • Tener al menos 2 interfaces 10 Gbps sobre SFP+ • Requisitos Mínimos de Funcionalidad. • Características Generales • 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. • Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos. • Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación. • La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7. • Todo el equipo proporcionado debe ser	

Renglón	Especificación Técnica	Imagen
7	adecuado para montaje en rack de 19", incluyendo un rail kit (si sea necesario) y los cables de alimentación. • La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red. • El dispositivo debe soportar 4094 VLANs Tags 802.1q. • El dispositivo debe soportar agregación de enlaces 802.3ad y LACP. • El dispositivo debe soportar Policy based routing y policy based forwarding. • El dispositivo debe soportar encaminamiento de multicast (PIM-SM y PIM-DM). • El dispositivo debe soportar DHCP Relay. • El dispositivo debe soportar DHCP Server. • El dispositivo debe soportar sFlow. • El dispositivo debe soportar Jumbo Frames. • El dispositivo debe soportar sub-interfaces Ethernet lógicas. • El dispositivo Debe ser compatible con NAT dinámica (varios-a-1). • El dispositivo Debe ser compatible con NAT dinámica (muchos-a-muchos). • El dispositivo Debe soportar NAT estática (1-a-1). • El dispositivo Debe admitir NAT estática (muchos-a-muchos). • El dispositivo Debe ser compatible con NAT estático bidireccional 1-a-1. • El dispositivo Debe ser compatible con la traducción de puertos (PAT). • El dispositivo Debe ser compatible con NAT Origen. • El dispositivo Debe ser compatible con NAT de destino. • El dispositivo Debe soportar NAT de origen y NAT de destino de forma simultánea. • Debe soportar NAT de origen y NAT de destino en la misma política. • Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico. • Debe ser compatible con NAT64 y NAT46. • Debe implementar el protocolo ECMP.	

Renglón	Especificación Técnica	Imagen
7	• Debe soportar el balanceo de enlace hash por IP de origen. • Debe soportar el balanceo de enlace por hash de IP de origen y destino. • 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. • Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales. • Debe permitir el monitoreo por SNMP de fallas de 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. • Enviar logs a sistemas de gestión externos simultáneamente. • Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL. • Debe soporta protección contra la suplantación de identidad (anti-spoofing). • Implementar la optimización del tráfico entre dos dispositivos. • Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP). • Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3). • Soportar OSPF graceful restart. • Los dispositivos de protección deben tener la capacidad de operar simultáneamente en una única instancia de servidor de seguridad, mediante el uso de sus interfaces físicas en los siguientes modos: modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3). • Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red. • Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico. • Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico. • Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.	

Renglón	Especificación Técnica	Imagen
7	• Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente. • Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3. • Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster. • La configuración de alta disponibilidad debe sincronizar: Sesiones. • La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red. • La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN. • La configuración de alta disponibilidad debe sincronizar: Tablas FIB. • En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace. • Debe soportar la creación de sistemas virtuales en el mismo equipo. • 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. • 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. • 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. • 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). • Debe soportar un tejido de seguridad	

Renglón	Especificación Técnica	Imagen
7	para proporcionar una solución de seguridad integral que abarque toda la red. • El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red. • 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. • Control por Politica de Firewall: • Debe soportar controles de zona de seguridad. • Debe contar con políticas de control por puerto y protocolo. • 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. • Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad. • Firewall debe poder aplicar la inspección UTM (control de aplicaciones y filtrado web como mínimo) directamente a las políticas de seguridad en vez de usar perfil obligatoriamente. • Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall. • Debe soportar el almacenamiento de bitácoras (logs) en tiempo real tanto para entorno de la nube como entorno local (on-premise). • Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF). • Debe existir una manera de evitar que el almacenamiento de logs en tiempo real no superen la velocidad de subida de los mismos (upload). • Debe soportar el protocolo estándar de la industria VXLAN. • Control de Aplicación: • Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo. • Debe ser posible liberar y bloquear	

Renglón	Especificación Técnica	Imagen
7	aplicaciones sin necesidad de abrir o cerrar puertos y protocolos. • Reconocer al menos 1.700 aplicaciones diferentes, 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. • 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. • Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo. • Debe detectar aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent. • 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 Torrent. • Para trafico 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. • Debe hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el tráfico corresponde a la especificación del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTTP. La decodificación de protocolo también debe identificar las características específicas dentro de una aplicación, incluyendo, pero no limitado al intercambio de ficheros dentro de Webex. 4.81)Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas. • Actualización de la base de firmas de la	

Renglón	Especificación Técnica	Imagen
7	aplicación de forma automática. • Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos. • Los dispositivos de protección de red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario. • Debe ser posible añadir múltiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas. • Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación. • Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas. • 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. • La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP. • El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos. • Debe alertar al usuario cuando sea bloqueada una aplicación. • Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo. • Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo. • Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video.	

Renglón	Especificación Técnica	Imagen
7	• Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo. • Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc). • Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación. • Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación. • 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 • Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware). • Las características de IPS, antivirus y anti-spyware 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. • Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad. • Debe implementar los siguientes tipos de acciones a las amenazas detectadas por IPS: Permitir, permitir y generar registro, bloquear, bloquear IP del atacante durante un tiempo y enviar tcp-reset. • Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo. • Debe ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad. • Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas.	

Renglón	Especificación Técnica	Imagen
7	• 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. • Deber permitir el bloqueo de vulnerabilidades. • Debe permitir el bloqueo de exploits conocidos. • Debe incluir la protección contra ataques de denegación de servicio. • Debe tener los siguientes mecanismos de inspección IPS: • Análisis de patrones de estado de las conexiones. • Análisis de decodificación de protocolo. • Análisis para detectar anomalías de protocolo. • Análisis heurístico. • Desfragmentación IP. • Re ensamblado de paquetes TCP. • Bloqueo de paquetes con formato incorrecto (malformed packets). • Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP UDP, etc. • Detectar y bloquear los escaneos de puertos de origen. • Bloquear ataques realizados por gusanos (worms) conocidos. • Contar con firmas específicas para la mitigación de ataques DoS y DdoS. • Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow). • Debe poder crear firmas personalizadas en la interfaz gráfica del producto. • Debe permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración. • Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3. • Soportar el bloqueo de archivos por tipo. • Identificar y bloquear la comunicación con redes de bots.	

Renglón	Especificación Técnica	Imagen
7	• 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. • Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación. • Debe permitir la captura de paquetes por tipo de firma IPS y definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la alerta, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos. • 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. • Los eventos deben identificar el país que origino la amenaza. • Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms). • Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP. • 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. • El Firewall debería permitirle analizar la implementación del tejido de seguridad para identificar posibles vulnerabilidades y resaltar las mejores prácticas que podrían utilizarse para mejorar la seguridad y el rendimiento general de su red. • 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.	

Renglón	Especificación Técnica	Imagen
7	• Los recursos de postura de seguridad deben existir para permitir que el software de seguridad de endpoint aplique protección en tiempo real, antivirus, filtrado de Web y control de aplicaciones en el punto final. • Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube). • Filtrado de 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) • Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad. • Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory y la base de datos local. • 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. • Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL. • 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 • Tener por lo menos 60 categorías de URL. • Debe tener la funcionalidad de exclusión de URLs por categoría • Permitir página de bloqueo personalizada. • 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). • Además del Explicit Web Proxy, soportar proxy web transparente.	

Renglón	Especificación Técnica	Imagen
7	• Identificación de Usuarios: • 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. • Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados ??en usuarios y grupos de usuarios. • Debe tener integración y soporte para Microsoft Active Directory para los siguientes sistemas operativos: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2. • Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control 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. • Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados ??en usuarios y grupos de usuarios. • Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados ??en usuarios y grupos de usuarios. • 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). • 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. • Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.	

Renglón	Especificación Técnica	Imagen
7	• Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma. • Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores. • QoS Traffic 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. • Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen. • Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino. • Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo. • Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube. • Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto. • En QoS debe permitir la definición de tráfico con ancho de banda garantizado. • En QoS debe permitir la definición de tráfico con máximo ancho de banda. • En QoS debe permitir la definición de colas de prioridad. • Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype. • Soportar marcación de paquetes DiffServ, incluso por aplicación. • Soportar la modificación de los valores de DSCP para Diffserv. • Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service). • Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping • Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes. • Filtro de Datos	

Renglón	Especificación Técnica	Imagen
7	• Permite la creación de filtros para archivos y datos predefinidos. • Los archivos deben ser identificados por tamaño y tipo. • Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.). • Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos. • Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos. • 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 Localización: • Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países. • Debe permitir la visualización de los países de origen y destino en los registros de acceso. • 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. • Soportar VPN IPSec. • Soportar VPN SSL. • La VPN IPSec debe ser compatible con 3DES. • La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1. • La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14. • La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2). • La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard). • La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI.	

Renglón	Especificación Técnica	Imagen
7	• Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall. • Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec. • Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting. • La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web. • Las características de VPN SSL se deben cumplir con o sin el uso de agentes. • 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 • Asignación de DNS en la VPN de cliente remoto. • 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. • Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local. • Suportar lectura y revisión de CRL (lista de revocación de certificados). • Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL. • Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Antes de que el usuario se autentique en su estación. • Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Después de la autenticación de usuario en la estación. • Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Bajo demanda de los usuarios. • Deberá mantener una conexión segura con el portal durante la sesión. • El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (v10.10 o superior). • Wireless Controller: • Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la	

Renglón	Especificación Técnica	Imagen
7	solución ofertada. • Soportar servicio de servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos. • Soporte IPv4 e IPv6 por SSID. • Permitir elegir si el tráfico de cada SSID se enviará a la controladora o directamente por la interfaz de punto de acceso en una determinada VLAN. • Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point. • Soportar monitoreo y supresión de puntos de acceso indebidos. • Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS. • Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows. • Permitir la visualización de los dispositivos inalámbricos conectados por usuario. • Permitir la visualización de los dispositivos inalámbricos conectados por IP. • Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación. • Permitir la visualización de los dispositivos inalámbricos conectados por canal. • Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado. • Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal. • Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación. • Debe soportar Fast Roaming en autenticación con portal cautivo. • Debe soportar configuración de portal cautivo por SSID. • Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico. • Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP. • Debe ser compatible con el protocolo	

Renglón	Especificación Técnica	Imagen
7	802.1x RADIUS. • La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DNS. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Broadcast. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Multicast. • La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue). • La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico. • La controladora deberá contar con mecanismos de protección de tramas de administración de acuerdo a las especificaciones de la alianza Wi-Fi y estándar 802.11ac. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding.	

Renglón	Especificación Técnica	Imagen
7	• La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge. • Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas. • Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso. • La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible. • La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario. • Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID. • Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso. • Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio. • La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh. • Ofrecer un mecanismo de creación automática y/o manual de usuarios visitantes y	

Renglón	Especificación Técnica	Imagen
7	contraseñas, que puedan ser enviados por correo electrónico o SMS a los usuarios, con ajuste de tiempo de expiración de la contraseña. • La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS. • Debe tener un mecanismo de ajuste automático de potencia de la señal con el fin de reducir la interferencia entre canales entre dos puntos de acceso administrados. • Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso. • Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso. • Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica • Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión • Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados • La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz. • Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados. • Debe permitir asociación dinámicas de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS. • Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling. • Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico. • La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones. • La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino. • La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza. • La controladora inalámbrica debe	

Renglón	Especificación Técnica	Imagen
7	permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones. • La controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico. • El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo. • El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales. • La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico. • La controladora inalámbrica deberá soportar aceleración de túnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico. • La controladora inalámbrica debe soportar protocolo LLDP. • Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta. • Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC adyacente. • Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos. • La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado. • La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas. • La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada. • Deberá soportar la conversión de Multicast a Unicast para mejorar el rendimiento del tiempo de aire. • En el entorno de alta disponibilidad, debe existir el concepto de controladores primarios y secundarios en la unidad AP, permitiendo que la unidad decida el orden en el que el AP selecciona una unidad controlador y cómo la unidad AP se	

Renglón	Especificación Técnica	Imagen
7	conecta a un controlador de backup en el caso de que el controlador primario falle. • Debe proporcionar la capacidad de crear varias claves pre-compartidas de acceso protegido WiFi (WPA-PSK) para que no sea necesario compartir PSK entre dispositivos. • Actualizaciones: • Las actualizaciones deberán ser por el termino de 1 año(se solicita cotizar alternativas por 24 y 36 meses). • Actualización y soporte de firmas, AV. • Actualización de firmas automáticas de IPS. • Laboratorios y centro de investigación propios. • WebContent Rating updates. • Categorización de WebFilters. • Actualización de grupos de categorías de filtrado web. • Actualización de firmas de Aplicaciones. • Actualización de Base de Datos de Antivirus • Actualización y mantenimiento de IP & Domain Reputation. • Actualización y mantenimiento de una lista de Botnets. • Garantía: • No inferior a los 12 meses, con posibilidad de renovación en forma anual(se solicita cotizar alternativas por 24 y 36 meses). • La garantía deberá ser certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). El proveedor debe ser el representante o distribuidor autorizado de todas las partes que componen el equipo y la garantía debe comprender al equipo con todas sus partes como un todo. • Acceso al soporte técnico por medio de un web portal, chat on line o telefonico • Retorno y reemplazo por falla de hardware. • Capacitación: • Se solicita capacitación para una persona por cada equipo. • La capacitación deberá ser brindada por un agente oficial y certificado del producto. • La Capacitación deberá abarcar el uso de herramientas de networking en lo que refiere a gestión y administración del dispositivo, Estructura interna del equipo, IPSec, Diagnostico, Web Filters, Control de Aplicaciones, Diseño e implementación de IPS, Creación de firmas IPS, así como el	

Renglón	Especificación Técnica	Imagen
7	workaround necesario para el uso del dispositivo. • Plazo de entrega 60 días.	
8	Solución UTM/NGFW con las siguientes características: • Throughput de por lo menos 9 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete. • Soporte a por lo menos 2M conexiones simultaneas. • Soporte a por lo menos 135K nuevas conexiones por segundo. • Throughput de al menos 9 Gbps de VPN IPSec. • Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos. • Estar licenciado para, o soportar sin necesidad de licencia, 10K túneles de clientes VPN IPSec simultáneos. • Throughput de al menos 900 Mbps de VPN SSL. • Soportar al menos 300 clientes de VPN SSL simultáneos. • Soportar al menos 6 Gbps de throughput de IPS. • Soportar al menos 1 Gbps de throughput de Inspección SSL. • Throughput de al menos 1,2 Gbps Mbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la solución de seguridad tenga debidamente activadasy operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado múltiples números de desempeño para cualquiera de las funcionalidades, solamente el de valor más pequeño será aceptado.. • Permitir gestionar al menos 32 Access Points. • Tener al menos 18 interfaces 1Gbps. • Tener al menos 2 interfaces 1Gbps por SFP. • Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance. • Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance. • Requisitos Mínimos de Funcionalidad. • Características Generales • La solución debe consistir en una plataforma de protección de Red, basada en un	

Renglón	Especificación Técnica	Imagen
8	dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo. • Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos. • Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación. • La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7. • 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. • La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red. • El dispositivo debe soportar 4094 VLANs Tags 802.1q. • El dispositivo debe soportar agregación de enlaces 802.3ad y LACP. • El dispositivo debe soportar Policy based routing y policy based forwarding. • El dispositivo debe soportar encaminamiento de multicast (PIM-SM y PIM-DM). • El dispositivo debe soportar DHCP Relay. • El dispositivo debe soportar DHCP Server. • El dispositivo debe soportar sFlow. • El dispositivo debe soportar Jumbo Frames. • El dispositivo debe soportar sub-interfaces Ethernet lógicas. • El dispositivo Debe ser compatible con NAT dinámica (varios-a-1). • El dispositivo Debe ser compatible con NAT dinámica (muchos-a-muchos). • El dispositivo Debe soportar NAT estática (1-a-1). • El dispositivo Debe admitir NAT estática (muchos-a-muchos). • El dispositivo Debe ser compatible con NAT estático bidireccional 1-a-1. • El dispositivo Debe ser compatible con la	

Renglón	Especificación Técnica	Imagen
8	traducción de puertos (PAT). • El dispositivo Debe ser compatible con NAT Origen. • El dispositivo Debe ser compatible con NAT de destino. • El dispositivo Debe soportar NAT de origen y NAT de destino de forma simultánea. • Debe soportar NAT de origen y NAT de destino en la misma política. • Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico. • Debe ser compatible con NAT64 y NAT46. • Debe implementar el protocolo ECMP. • Debe soportar el balanceo de enlace hash por IP de origen. • Debe soportar el balanceo de enlace por hash de IP de origen y destino. • 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. • Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales. • Debe permitir el monitoreo por SNMP de fallas de 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. • Enviar logs a sistemas de gestión externos simultáneamente. • Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL. • Debe soporta protección contra la suplantación de identidad (anti-spoofing). • Implementar la optimización del tráfico entre dos dispositivos. • Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP). • Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3). • Soportar OSPF graceful restart. • Los dispositivos de protección deben tener la capacidad de operar simultáneamente en una única instancia de servidor de seguridad,	

Renglón	Especificación Técnica	Imagen
8	mediante el uso de sus interfaces físicas en los siguientes modos: modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3). • Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red. • Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico. • Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico. • Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas. • Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente. • Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3. • Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster. • La configuración de alta disponibilidad debe sincronizar: Sesiones. • La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red. • La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN. • La configuración de alta disponibilidad debe sincronizar: Tablas FIB. • En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace. • Debe soportar la creación de sistemas virtuales en el mismo equipo. • 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. • 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	

Renglón	Especificación Técnica	Imagen
8	pueden administrar por diferentes áreas funcionales. • 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. • 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). • Debe soportar un tejido de seguridad para proporcionar una solución de seguridad integral que abarque toda la red. • El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red. • 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. • Control por Politica de Firewall: • Debe soportar controles de zona de seguridad. • Debe contar con políticas de control por puerto y protocolo. • 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. • Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad. • Firewall debe poder aplicar la inspección UTM (control de aplicaciones y filtrado web como mínimo) directamente a las políticas de seguridad en vez de usar perfil obligatoriamente. • Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall. • Debe soportar el almacenamiento de bitácoras (logs) en tiempo real tanto para entorno	

Renglón	Especificación Técnica	Imagen
8	de la nube como entorno local (on-premise). • Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF). • Debe existir una manera de evitar que el almacenamiento de logs en tiempo real no superen la velocidad de subida de los mismos (upload). • Debe soportar el protocolo estándar de la industria VXLAN. • Control de Aplicación: • Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo. • Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos. • Reconocer al menos 1.700 aplicaciones diferentes, 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. • 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. • Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo. • Debe detectar aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent. • 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 Torrent. • Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload	

Renglón	Especificación Técnica	Imagen
8	para permitir la identificación de firmas de la aplicación conocidas por el fabricante. • Debe hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el tráfico corresponde a la especificación del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTTP. La decodificación de protocolo también debe identificar las características específicas dentro de una aplicación, incluyendo, pero no limitado al intercambio de ficheros dentro de Webex. 4.81)Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas. • Actualización de la base de firmas de la aplicación de forma automática. • Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos. • Los dispositivos de protección de red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario. • Debe ser posible añadir múltiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas. • Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación. • Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas. • 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. • La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y	

Renglón	Especificación Técnica	Imagen
8	RTSP. • El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos. • Debe alertar al usuario cuando sea bloqueada una aplicación. • Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo. • Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo. • Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video. • Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo. • Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc). • Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación. • Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación. • 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 • Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware). • Las características de IPS, antivirus y anti-spyware 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. • Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en	

Renglón	Especificación Técnica	Imagen
8	alta disponibilidad. • Debe implementar los siguientes tipos de acciones a las amenazas detectadas por IPS: Permitir, permitir y generar registro, bloquear, bloquear IP del atacante durante un tiempo y enviar tcp-reset. • Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo. • Debe ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad. • Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas. • 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. • Deber permitir el bloqueo de vulnerabilidades. • Debe permitir el bloqueo de exploits conocidos. • Debe incluir la protección contra ataques de denegación de servicio. • Debe tener los siguientes mecanismos de inspección IPS: • Análisis de patrones de estado de las conexiones. • Análisis de decodificación de protocolo. • Análisis para detectar anomalías de protocolo. • Análisis heurístico. • Desfragmentación IP. • Re ensamblado de paquetes TCP. • Bloqueo de paquetes con formato incorrecto (malformed packets). • Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP UDP, etc. • Detectar y bloquear los escaneos de puertos de origen. • Bloquear ataques realizados por gusanos (worms) conocidos. • Contar con firmas específicas para la mitigación de ataques DoS y DdoS.	

Renglón	Especificación Técnica	Imagen
8	• Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow). • Debe poder crear firmas personalizadas en la interfaz gráfica del producto. • Debe permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración. • Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3. • Soportar el bloqueo de archivos por tipo. • Identificar y bloquear la comunicación con redes de bots. • 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. • Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación. • Debe permitir la captura de paquetes por tipo de firma IPS y definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la alerta, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos. • 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. • Los eventos deben identificar el país que origino la amenaza. • Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms). • Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP. • 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	

Renglón	Especificación Técnica	Imagen
8	diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad. • El Firewall debería permitirle analizar la implementación del tejido de seguridad para identificar posibles vulnerabilidades y resaltar las mejores prácticas que podrían utilizarse para mejorar la seguridad y el rendimiento general de su red. • 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. • Los recursos de postura de seguridad deben existir para permitir que el software de seguridad de endpoint aplique protección en tiempo real, antivirus, filtrado de Web y control de aplicaciones en el punto final. • Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube). • Filtrado de 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) • Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad. • Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory y la base de datos local. • 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. • Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL. • 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	

Renglón	Especificación Técnica	Imagen
8	direcciones URL • Tener por lo menos 60 categorías de URL. • Debe tener la funcionalidad de exclusión de URLs por categoría • Permitir página de bloqueo personalizada. • 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). • Además del Explicit Web Proxy, soportar proxy web transparente. • Identificación de Usuarios: • 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. • Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados ??en usuarios y grupos de usuarios. • Debe tener integración y soporte para Microsoft Active Directory para los siguientes sistemas operativos: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2. • Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control 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. • Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados ??en usuarios y grupos de usuarios. • Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados ??en usuarios y grupos de usuarios.	

Renglón	Especificación Técnica	Imagen
8	• 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). • 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. • Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD. • Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma. • Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores. • QoS Traffic 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. • Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen. • Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino. • Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo. • Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube. • Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto. • En QoS debe permitir la definición de tráfico con ancho de banda garantizado. • En QoS debe permitir la definición de tráfico con máximo ancho de banda. • En QoS debe permitir la definición de	

Renglón	Especificación Técnica	Imagen
8	colas de prioridad. • Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype. • Soportar marcación de paquetes DiffServ, incluso por aplicación. • Soportar la modificación de los valores de DSCP para Diffserv. • Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service). • Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping • Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes. • Filtro de Datos • Permite la creación de filtros para archivos y datos predefinidos. • Los archivos deben ser identificados por tamaño y tipo. • Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.). • Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos. • Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos. • 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 Localización: • Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países. • Debe permitir la visualización de los países de origen y destino en los registros de acceso. • 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. • Soportar VPN IPSec.	

Renglón	Especificación Técnica	Imagen
8	• Soportar VPN SSL. • La VPN IPSec debe ser compatible con 3DES. • La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1. • La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14. • La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2). • La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard). • La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI. • Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall. • Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec. • Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting. • La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web. • Las características de VPN SSL se deben cumplir con o sin el uso de agentes. • 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 • Asignación de DNS en la VPN de cliente remoto. • 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. • Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local. • Suportar lectura y revisión de CRL (lista de revocación de certificados). • Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL. • Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Antes de que el usuario se autentique en su estación.	

Renglón	Especificación Técnica	Imagen
8	• Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Después de la autenticación de usuario en la estación. • Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Bajo demanda de los usuarios. • Deberá mantener una conexión segura con el portal durante la sesión. • El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (v10.10 o superior). • Wireless Controller: • Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada. • Soportar servicio de servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos. • Soporte IPv4 e IPv6 por SSID. • Permitir elegir si el tráfico de cada SSID se enviará a la controladora o directamente por la interfaz de punto de acceso en una determinada VLAN. • Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point. • Soportar monitoreo y supresión de puntos de acceso indebidos. • Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS. • Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows. • Permitir la visualización de los dispositivos inalámbricos conectados por usuario. • Permitir la visualización de los dispositivos inalámbricos conectados por IP. • Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación. • Permitir la visualización de los dispositivos inalámbricos conectados por canal. • Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado. • Permitir la visualización de los	

Renglón	Especificación Técnica	Imagen
8	dispositivos inalámbricos conectados por potencia de la señal. • Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación. • Debe soportar Fast Roaming en autenticación con portal cautivo. • Debe soportar configuración de portal cautivo por SSID. • Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico. • Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP. • Debe ser compatible con el protocolo 802.1x RADIUS. • La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DNS. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Broadcast. • La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Multicast. • La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue). • La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico. • La controladora deberá contar con mecanismos de protección de tramas de administración de acuerdo a las especificaciones de la alianza Wi-Fi y estándar 802.11ac. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP. • La controladora inalámbrica deberá	

Renglón	Especificación Técnica	Imagen
8	tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection. • La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge. • Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas. • Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso. • La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible.	

Renglón	Especificación Técnica	Imagen
8	• La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario. • Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID. • Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso. • Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio. • La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh. • Ofrecer un mecanismo de creación automática y/o manual de usuarios visitantes y contraseñas, que puedan ser enviados por correo electrónico o SMS a los usuarios, con ajuste de tiempo de expiración de la contraseña. • La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS. • Debe tener un mecanismo de ajuste automático de potencia de la señal con el fin de reducir la interferencia entre canales entre dos puntos de acceso administrados. • Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso. • Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso. • Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica • Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión • Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados • La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz. • Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados. • Debe permitir asociación dinámicas de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS.	

Renglón	Especificación Técnica	Imagen
8	• Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling. • Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico. • La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones. • La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino. • La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza. • La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones. • La controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico. • El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo. • El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales. • La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico. • La controladora inalámbrica deberá soportar aceleración de túnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico. • La controladora inalámbrica debe soportar protocolo LLDP. • Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta. • Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC adyacente. • Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos. • La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con	

Renglón	Especificación Técnica	Imagen
8	un software switch integrado. • La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas. • La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada. • Deberá soportar la conversión de Multicast a Unicast para mejorar el rendimiento del tiempo de aire. • En el entorno de alta disponibilidad, debe existir el concepto de controladores primarios y secundarios en la unidad AP, permitiendo que la unidad decida el orden en el que el AP selecciona una unidad controlador y cómo la unidad AP se conecta a un controlador de backup en el caso de que el controlador primario falle. • Debe proporcionar la capacidad de crear varias claves pre-compartidas de acceso protegido WiFi (WPA-PSK) para que no sea necesario compartir PSK entre dispositivos. • Actualizaciones: • Las actualizaciones deberán ser por el termino de 1 año(se solicita cotizar alternativas por 24 y 36 meses). • Actualización y soporte de firmas, AV. • Actualización de firmas automáticas de IPS. • Laboratorios y centro de investigación propios. • WebContent Rating updates. • Categorización de WebFilters. • Actualización de grupos de categorías de filtrado web. • Actualización de firmas de Aplicaciones. • Actualización de Base de Datos de Antivirus • Actualización y mantenimiento de IP & Domain Reputation. • Actualización y mantenimiento de una lista de Botnets. • Garantía: • No inferior a los 12 meses, con posibilidad de renovación en forma anual(se solicita cotizar alternativas por 24 y 36 meses). • La garantía deberá ser certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). El proveedor debe ser el representante o distribuidor autorizado de todas las partes que componen el equipo y la garantía debe comprender al equipo con todas sus partes como	

Renglón	Especificación Técnica	Imagen
8	un todo. • Acceso al soporte técnico por medio de un web portal, chat on line o telefonico • Retorno y reemplazo por falla de hardware. • Capacitación: • Se solicita capacitación para una persona por cada equipo. • La capacitación deberá ser brindada por un agente oficial y certificado del producto. • La Capacitación deberá abarcar el uso de herramientas de networking en lo que refiere a gestión y administración del dispositivo, Estructura interna del equipo, IPSec, Diagnostico, Web Filters, Control de Aplicaciones, Diseño e implementación de IPS, Creación de firmas IPS, así como el workaround necesario para el uso del dispositivo. • Plazo de entrega 60 días.	
9	• 2(dos) Procesador Intel® Xeon® E5-2697v4 18 core o superior. • Memoria: 128 GB Ram DDR4 Dual Rank o superior a una frecuencia de 2400MHz instalada, deberá quedar al menos el 50% de los slots de memoria disponibles por procesador, para poder ampliar al doble su capacidad. • Controladora de disco para soportar 8 o mas discos SSD SATA 6G / SAS de 12GB de transferencia con 2GB de cache o superior, con batería incorporada o tecnología superior; deberá soportar niveles de Raid, 0, 1 y 5 por hardware. • **6(seis) Disco SAS 900GB o superior, 12G de transferencia, 15000rpm, 2,5”, hot plug/swap, configurados en raid 1 por hardware**. • 2 (dos) Discos SSD SAS 400GB o superior, 12GB de transferencia. • Deberá poder alojar 8 discos del tipo SAS 2.5”, sin tener que realizar ninguna ampliación y/o modificación. • 4(cuatro) Puertos ethernet 10/100/1000. • 2(dos) PCIe DualPort, 8Gb, Fiber Channel Adapter. Las mismas deberán ser compatible con HP 3Par 8400. Se deberá presentar certificación de compatibilidad escrita del fabricante de la placa FC, respecto al storage FC HP 3PAR 8400 y al servidor en el cual será instalada. • Deberá poseer 3 (tres) Slots PCIe o superior. Mínimo 2 Slots PCIe x16 y 1 Slot PCIe x8, deberá quedar disponible 1(uno) Slot PCIe libre sin realizar	

Renglón	Especificación Técnica	Imagen
9	modificación alguna, una vez configurada la totalidad del equipo. • 1 (una) Lectora y grabadora de DVD SATA. • 2(dos) Fuentes de alimentación para soportar todo lo anteriormente mencionado y trabajar en forma redundante, las mismas serán del tipo hot plug/swap. Con una potencia de al menos 500W cada una o superior. • El equipo deberá contar con ventiladores redundantes. • Kit de rackeo debe estar incluido. • Deberá contener un puerto de administración remota por red(RJ45) exclusivo no compartido con otros puertos Ethernet(ILO/IMM/IDRAC) • Plazo de garantía no inferior a los 36 meses certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). El proveedor debe ser el representante o distribuidor autorizado de todas las partes que componen el equipo y la garantía debe comprender al equipo con todas sus partes como un todo. • Plazo de entrega 60 días. Software: • 1(uno) Windows Server 2012 Server OLP Academico.	
10	• Dispositivo intercambiador de Teclado, Video y Mouse de 8 puertos con conexiones VGA y USB. • Debe Admitir conexiones USB y PS/2 a puerto de consola. • Control de dispositivo con Auto-Scan (exploración automática) ajustable y avisos audibles. • Formato Rackeable, con sus correspondiente accesorios para montar en rack de servidores. • 4 Cables USB de por lo menos 1.80Mts a 2Mts. • 4 Cables USB de por lo menos 3 Mts a 3.20Mts. • Compatible con Sistemas Operativos Windows 2003, Windows 2008, Windows 2012, Windows 2016, Linux Centos 7, Red Hat 7, Debian. • Plazo de garantía no inferior a los 12 meses certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). El proveedor debe ser el representante o distribuidor autorizado de todas las partes que componen el equipo y la	

Renglón	Especificación Técnica	Imagen
10	garantía debe comprender al equipo con todas sus partes como un todo.	
11	Impresora multifunción que combine tareas de impresión y copiado en blanco y negro con digitalización de imágenes en color a) Función Impresora Impresora de tecnología laser con las siguientes características: • Medios y tamaños soportados: • A4 • Carta • Capacidad de impresión no inferior a 2400x600 dpi en B&N para textos y gráficos. • Velocidad de impresión: no inferior a 30 para tamaño A4. • Volumen de impresión mensual recomendado: 2000 hojas o superior. • Bandeja de entrada: no menos de 250 hojas cortadas. • Accesorio dúplex para impresión doble-faz automática sin intervención del usuario. *b) Función Escáner* Digitalizador de imágenes con las siguientes características: • Tamaño máximo de documento escaneable: • A4 • Carta • Resolución Óptica: 600x600 dpi, como mínimo. • Alimentador automático de documentos de 35 mínimo o superior. • Escala de grises: 8 bits (256 niveles) como mínimo. • Soporte de escaneo en colores. • Velocidad de escaneo: no inferior a 25 ppm en B&N y 12 ppm en color para tamaño A4. c) Función Copiadora Copiadora con las siguientes características: • Tamaño de documento: • A4 • Carta • Velocidad promedio de copiado no inferior a	

Renglón	Especificación Técnica	Imagen
11	25 ppm para tamaño A4. • Resolución mínima: 1200x1200 dpi. d) Conectividad • Interfaz USB 2.0 o superior. • Interfaz para Red Ethernet 10/100 (Cable UTP / Conector RJ 45) e) Sistemas Operativos • Deberán proveerse los drivers para Windows 7, 8.1, 10, 2008Server, 2012 Server. f) Insumos • Deberán proveerse (para cada impresora) todos los insumos necesarios (cartuchos de tóner y, de corresponder, el tambor de revelado –drum–) g) Otras Características • Deberá poder conectarse directamente a la red de suministro de energía eléctrica de 220V - 50 Hz. Deberá tener conexión a tierra, o poseer circuito de doble aislación y/o doble protección. • Deberán incluirse los manuales, cables de conexión del equipo con la CPU, cables de alimentación eléctrica, cables de conexión telefónica en caso de optar por incluir la funcionalidad de FAX, y todo otro elemento necesario para el normal funcionamiento del equipo. Garantía: un año certificada por escrito.	
12	Se solicita SW HP 2530-48G(Part. Number J9775A) por compatibilidad con equipamiento existente. • Plazo de garantía no inferior a los 36 meses certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). El proveedor debe ser el representante o distribuidor autorizado de todas las partes que componen el equipo y la garantía debe comprender al equipo con todas sus partes como un todo. • Plazo de entrega 60 días.	
13	Se solicita SW HP 2530-24G (Part. Number J9776A) por compatibilidad con equipamiento existente. • Plazo de garantía no inferior a los 36 meses	

Renglón	Especificación Técnica	Imagen
13	certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). El proveedor debe ser el representante o distribuidor autorizado de todas las partes que componen el equipo y la garantía debe comprender al equipo con todas sus partes como un todo. • Plazo de entrega 60 días.	
14	Se solicita modelo HP 5500 48Ports con su Kit de apilamiento. • Apilamiento: • Deberá incluir todos los elementos necesarios de apilamiento entre switchs como ser placa adicionales, módulos de expansión(kit de apilamiento), 1(uno) cable de 2Mts y 1(uno) cable de 3Mts, para su correspondiente instalación. • La velocidad de apilamiento no podrá ser inferior a 10Gbps • Deberán poder apilarse no menos 8 switchs en total. • No se permitirá el apilamiento por medio de puertos puertos uplink. • Plazo de garantía no inferior a los 36 meses certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). El proveedor debe ser el representante o distribuidor autorizado de todas las partes que componen el equipo y la garantía debe comprender al equipo con todas sus partes como un todo. • Plazo de entrega 60 días.	
15	• Disco Rígido: SATA o superior con un mínimo de 4TB de capacidad y 7200RPMs como mínimo, 128mb. Buffer o superior. • Factor de forma: 3.5” • Plazo de garantía no inferior a los 12 meses certificada por escrito y mano de obra con servicio en Sede de Gobierno (on-site). • Plazo de entrega 15 días. • Obs: se recomienda WD 4 TB SATA3 BLACK (WD4004FZWX)	