CAPACIDAD TECNICA PAC 53

1. Presentar el Currículum Vitae y certificados de al menos dos técnicos que en conjunto cuenten con:
    - Certificación Profesional o semejante en Diseño de redes de la marca ofertada.
    - Certificación Profesional o semejante en Configuración y Resolución de Problemas de equipos de redes de la marca ofertada.
    - Certificación del fabricante.
2. Presentar la Planilla del Instituto de Previsión Social del mes anterior vencido al del acto de presentación de ofertas en donde figuren los técnicos propuestos.
3. Demostrar que los técnicos propuestos forman parte del plantel estable de la compañía y que residan localmente.
4. El oferente debe ser servicio técnico autorizado o estar debidamente autorizado por el fabricante o el representante para brindar asistencia para equipos de la marca ofertada.
5. Manifestar que cuente con personal debidamente calificado para ejecutar y coordinar los servicios solicitados.
6. Dos certificados o constancias de satisfacción de clientes, en la prestación de servicios relacionados a los del presente llamado. Dichos documentos deberán corresponder a los años (2019, 2020, 2021).
7. El oferente deberá presentar catálogo de su producto donde indique claramente el cumplimiento de las especificaciones solicitadas. Y todas las documentaciones técnicas adicionales que garanticen el cumplimiento de lo solicitado.
8. Contar con certificado de calidad ISO 9001:2015 o similar del fabricante de los equipos ofertados **(PARA TODOS LOS ÍTEMS)**

DOCUMENTOS - CAPACIDAD TECNICA PAC 53

1. Currículum Vitae y certificados de al menos dos técnicos que en conjunto cuenten con:
    - Certificación Profesional o semejante en Diseño de redes de la marca ofertada.
    - Certificación Profesional o semejante en Configuración y Resolución de Problemas de equipos de redes de la marca ofertada.
    - Certificación del fabricante.
2. Planilla del Instituto de Previsión Social del mes anterior vencido al del acto de presentación de ofertas en donde figuren los técnicos propuestos.
3. Constancia o Declaración Jurada que los técnicos propuestos forman parte del plantel estable de la compañía y que residan localmente.
4. La empresa oferente deberá contar con autorización del fabricante para proveer, instalar y soportar los equipos adquiridos.

   Para Representantes debe reunir los siguientes requisitos: Documentación expedida por el Fabricante que los acredite como representante de la marca ofertada y, dichos documentos deben estar debidamente legalizados por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay. Los mismos deben ser originales o copias autenticadas por Escribano Público.

   Para Distribuidor Autorizado debe reunir los siguientes requisitos: Documentación expedida por el Fabricante que los acredite como distribuidor autorizado de la marca ofertada, para tal efecto debe presentar el documento original o copia autenticada por

Escribano Público, y el mismo debe estar debidamente legalizado por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay.

Para Sub-Distribuidor debe reunir los siguientes requisitos: Documento original o copia autenticada por Escribano Público de la autorización del Fabricante extendida al Representante, Distribuidor y/o Resellers para el PARAGUAY Y/O LATINOAMERICA que lo nombra como representante, o distribuidor autorizado de la marca ofertada y en la cual lo autoriza a nombrar sub-distribuidores. Para tal efecto debe presentar el documento original o copia autenticada por Escribano Público, y el mismo debe estar debidamente legalizada por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay.

Serán considerados válidos los documentos apostillados como los documentos legalizados por el Consulado y el Ministerio de Relaciones Exteriores en conformidad a la Ley N° 4987/13 QUE APRUEBA EL CONVENIO SUPRIMIENDO LA EXIGENCIA DE LA LEGALIZACIÓN DE LOS DOCUMENTOS PÚBLICOS EXTRANJEROS.

5. Declaración Jurada en que se manifieste que cuente con personal debidamente calificado para ejecutar y coordinar los servicios solicitados.
6. Adjuntar al menos dos certificados o constancias de satisfacción de clientes, en la prestación de servicios relacionados a los del presente llamado. Dichos documentos deberán corresponder a los años (2019, 2020, 2021).
7. Catálogo de los Bienes Ofertados.
8. Certificado de calidad ISO 9001:2015 o similar del fabricante de los equipos ofertados **(PARA TODOS LOS ÍTEMS)**

ESPECIFICACIONES TÉCNICAS.

ALCANCE DE LOS TRABAJOS Y SERVICIOS

Los oferentes deben entregar todos los subsistemas del presente llamado en la modalidad de llave en mano, por lo cual deben tener en cuenta todos los equipamientos, accesorios, materiales de instalación, horas de servicio técnico especializado para la correcta implementación de la solución ofertada, de acuerdo con los requerimientos técnicos del presente documento. A continuación, se listan de manera enunciativa y no limitativa algunas de las consideraciones dentro del alcance del presente llamado.

1. El sistema de seguridad perimetral para el Datacenter de la DGRP correspondiente a este documento comprende la provisión, instalación y configuración del Firewall, Sistema de Reporte y Switches de Acceso para proveer seguridad, alta disponibilidad y gestión a la red de la DGRP.
2. Se deben proveer la cantidad de equipos necesarios que cumplan con los requerimientos mínimos de este documento para soportar los servicios actuales y futuros de voz, datos, video en todas las dependencias del edificio.
3. Se debe considerar que, para la correcta implementación de la solución e integración a los equipos existentes, serán necesarios realizar cambios en la infraestructura actual, para lo cual, la convocante prestará la asistencia necesaria.
4. Queda a cargo de los oferentes, la correcta configuración, implementación e integración de la solución ofertada con la infraestructura actual, de acuerdo a los más altos estándares y mejores prácticas de la industria, contemplando configuración, por mencionar apenas algunas de ellas, hardening, acceso a proveedores, ruteo dinámico y estático externo, ruteo interno local y entre vlans, integración con Active Directory mediante LDAP, políticas de acceso a Internet por usuario y grupos, filtrado web, VPNs, antivirus, IPS, anti malware, anti phishing, ACLs, NAT, port forwarding,

publicación de servicios web. El tiempo máximo para el despliegue no deberá superar los 30 días hábiles.

La convocante se reserva el derecho de verificación in situ de las instalaciones de los oferentes de manera a corroborar que los oferentes cuentan con los recursos y capacidad necesaria para proveer este servicio.

Soporte
El soporte requerido deberá ser in-situ e incluir la configuración de los equipos en el formato que la convocante lo exija.
En caso de alguna falla en un equipo, que impida su correcto uso o funcionamiento, se deberá prever un tiempo máximo de respuesta de 4 horas a partir de la comunicación por correo electrónico de la convocante al proveedor. En caso de que el equipo no pueda ser reparado se deberá reemplazar por uno igual o de mayores prestaciones hasta la devolución del equipo reparado; se deberá dejar en funcionamiento todos los servicios con todas las configuraciones. Este soporte es solicitado por el tiempo que dure la Garantía.

La empresa oferente deberá contar con un Centro de Atención al Cliente propio de la empresa y que sea con funcionalidad operativa 7x24 (24 horas del día, los 365 días del año). Este centro de atención debe tener a disposición técnicos de guardia permanente para los casos de asistencia remota o en situ. Además, deberá anexar una documentación donde mencione niveles de escalamiento con números de teléfonos y direcciones de correo, y deberá garantizar que las solicitudes e incidencias sean gestionadas mediante un sistema de Tickets que permita el seguimiento y la gestión de los incidentes hasta su cierre (solución de los mismos). Igualmente, deberá anexar una Declaración Jurada indicando el cumplimiento, así como también la convocante se reserva el derecho de una verificación en sitio del oferente, en caso de que así se requiera.

Capacitación
El Oferente deberá prever, por cada ítem ofertado, la capacitación local corriendo con todos los gastos por cuenta propia, para 5 (cinco) funcionarios de la convocante con una duración mínima de 30 horas (reloj), en modalidad presencial en las oficinas de la Convocante en horario de oficina con entrega de certificados.

ÍTEM N°	BIEN	ESPECIFICACIONES TÉCNICAS	UNIDAD DE MEDIDA	PRESENTACIÓN	CANTIDAD
1	PROVISIÓN, INSTALACIÓN Y CONFIGURACIÓN DE EQUIPOS DE SEGURIDAD DE REDES (UTM)	SEGÚN EETT	UNIDAD	EVENTO	2
2	PROVISIÓN, INSTALACIÓN Y CONFIGURACIÓN DE SOFTWARE DE REGISTROS, ANÁLISIS Y REPORTES	SEGÚN EETT	UNIDAD	EVENTO	1
3	PROVISIÓN, INSTALACIÓN Y CONFIGURACIÓN DE EQUIPOS DE CONMUTACIÓN (SWITCH)	SEGÚN EETT	UNIDAD	EVENTO	2
4	SERVICIO DE CAPACITACIÓN	SEGÚN EETT	UNIDAD	EVENTO	1

ESPECIFICACIONES TÉCNICAS

ITEM 1. PROVISIÓN, INSTALACIÓN Y CONFIGURACIÓN DE EQUIPOS DE SEGURIDAD DE REDES (UTM)	
Descripción	**Requerimiento mínimo**
Marca	indicar
Modelo	indicar
Procedencia	indicar
Cantidad	2 (dos)

Requisitos Mínimos	
NGFW en factor de forma appliance, rackeable de 1U	REQUERIDO
Throughput de por lo menos 25 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6	REQUERIDO
Soporte a por lo menos 3M conexiones simultaneas	REQUERIDO
Soporte a por lo menos 250K nuevas conexiones por segundo	REQUERIDO
Throughput de al menos 12 Gbps de VPN IPSec	REQUERIDO
Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos	REQUERIDO
Estar licenciado para, o soportar sin necesidad de licencia, 15K túneles de clientes VPN IPSec simultáneos	REQUERIDO
Throughput de al menos 2 Gbps de VPN SSL	REQUERIDO
Soportar al menos 500 clientes de VPN SSL simultáneos	REQUERIDO
Soportar al menos 5 Gbps de throughput de IPS	REQUERIDO
Soportar al menos 4 Gbps de throughput de Inspección SSL	REQUERIDO
Soportar al menos 10 Gbps de throughput de Application Control	REQUERIDO
Soportar al menos 3 Gbps de throughput de NGFW	REQUERIDO
Soportar al menos 3 Gbps de throughput de Threat Protection	REQUERIDO
Permitir gestionar al menos 25 Access Points	REQUERIDO
Tener al menos 24 interfaces, 16 RJ45 y 8 SFP de 1 Gbps cada uno	REQUERIDO
Tener al menos 4 interfaces SFP+ de 10 Gbps cada uno	REQUERIDO
Estar licenciado y/o tener incluido sin costo adicional, al menos 9 sistemas virtuales lógicos (Contextos) por appliance	REQUERIDO
Soporte de por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance	REQUERIDO
Fuente redundante	REQUERIDO
Al menos deberá contar con las siguientes certificaciones: FCC, CE, VCCI	REQUERIDO
Al menos deberá contar con las siguientes certificaciones: ISO 9001 y ICSA Labs	REQUERIDO
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;	REQUERIDO
Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	REQUERIDO
Las funcionalidades de protección de red que conforman la plataforma de seguridad, pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;	REQUERIDO
La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;	REQUERIDO
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;	REQUERIDO
La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;	REQUERIDO
Los dispositivos de protección de red deben soportar mínimamente 4094 VLANs Tags 802.1q;	REQUERIDO
Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;	REQUERIDO
Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;	REQUERIDO
Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);	REQUERIDO
Los dispositivos de protección de red deben soportar DHCP Relay;	REQUERIDO

Los dispositivos de protección de red deben soportar DHCP Server;	REQUERIDO
Los dispositivos de protección de red deben soportar sFlow;	REQUERIDO
Los dispositivos de protección de red deben soportar Jumbo Frames;	REQUERIDO
Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;	REQUERIDO
Debe ser compatible con NAT dinámica (varios-a-1);	REQUERIDO
Debe ser compatible con NAT dinámica (muchos-a-muchos);	REQUERIDO
Debe soportar NAT estática (1-a-1);	REQUERIDO
Debe admitir NAT estática (muchos-a-muchos);	REQUERIDO
Debe ser compatible con NAT estático bidireccional 1-a-1;	REQUERIDO
Debe ser compatible con la traducción de puertos (PAT);	REQUERIDO
Debe ser compatible con NAT Origen;	REQUERIDO
Debe ser compatible con NAT de destino;	REQUERIDO
Debe soportar NAT de origen y NAT de destino de forma simultánea;	REQUERIDO
Debe soportar NAT de origen y NAT de destino en la misma política	REQUERIDO
Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;	REQUERIDO
Debe ser compatible con NAT64 y NAT46;	REQUERIDO
Debe implementar el protocolo ECMP;	REQUERIDO
Debe soportar SD-WAN de forma nativa	REQUERIDO
Debe soportar el balanceo de enlace hash por IP de origen;	REQUERIDO
Debe soportar el balanceo de enlace por hash de IP de origen y destino;	REQUERIDO
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;	REQUERIDO
Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;	REQUERIDO
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;	REQUERIDO
Enviar logs a sistemas de gestión externos simultáneamente;	REQUERIDO
Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;	REQUERIDO
Debe soporta protección contra la suplantación de identidad (anti-spoofing);	REQUERIDO
Implementar la optimización del tráfico entre dos dispositivos;	REQUERIDO
Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);	REQUERIDO
Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);	REQUERIDO
Soportar OSPF graceful restart;	REQUERIDO
Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;	REQUERIDO
Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;	REQUERIDO
Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;	REQUERIDO
Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;	REQUERIDO
Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;	REQUERIDO
Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;	REQUERIDO
Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la	REQUERIDO

capa 3 y con al menos 3 dispositivos en el cluster;	
La configuración de alta disponibilidad debe sincronizar: Sesiones;	REQUERIDO
La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;	REQUERIDO
La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;	REQUERIDO
La configuración de alta disponibilidad debe sincronizar: Tablas FIB;	REQUERIDO
En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;	REQUERIDO
Debe soportar la creación de sistemas virtuales en el mismo equipo;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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);	REQUERIDO
Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
La consola de administración debe soportar como mínimo, inglés y español.	REQUERIDO
La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad	REQUERIDO
La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.	REQUERIDO
Control por Política de Firewall	
Debe soportar controles de zona de seguridad;	REQUERIDO
Debe contar con políticas de control por puerto y protocolo;	REQUERIDO
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;	REQUERIDO
Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;	REQUERIDO
Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;	REQUERIDO
Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;	REQUERIDO
Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.	REQUERIDO
Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);	REQUERIDO

Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes	REQUERIDO
Debe soportar el protocolo estándar de la industria VXLAN;	REQUERIDO
La solución debe permitir la implementación sin asistencia de SD-WAN	REQUERIDO
En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;	REQUERIDO
la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall.	REQUERIDO
Control de Aplicación	
Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;	REQUERIDO
Detección de miles de aplicaciones en 18 categorías, 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;	REQUERIDO
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;	REQUERIDO
Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;	REQUERIDO
Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;	REQUERIDO
Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;	REQUERIDO
Actualización de la base de firmas de la aplicación de forma automática;	REQUERIDO
Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por politica de usuarios y grupos;	REQUERIDO
Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;	REQUERIDO
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;	REQUERIDO
El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;	REQUERIDO
Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;	REQUERIDO
Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;	REQUERIDO
Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video;	REQUERIDO
Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;	REQUERIDO
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);	REQUERIDO
Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;	REQUERIDO
Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;	REQUERIDO
Debe ser posible configurar Application Override seleccionando las aplicaciones	REQUERIDO

individualmente	
Prevención de Amenazas	
Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;	REQUERIDO
Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);	REQUERIDO
Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;	REQUERIDO
Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;	REQUERIDO
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;	REQUERIDO
Debe permitir el bloqueo de vulnerabilidades y exploits conocidos	REQUERIDO
Debe incluir la protección contra ataques de denegación de servicio;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);	REQUERIDO
Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;	REQUERIDO
Detectar y bloquear los escaneos de puertos de origen;	REQUERIDO
Bloquear ataques realizados por gusanos (worms) conocidos;	REQUERIDO
Contar con firmas específicas para la mitigación de ataques DoS y DDoS;	REQUERIDO
Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);	REQUERIDO
Debe poder crear firmas personalizadas en la interfaz gráfica del producto;	REQUERIDO
Identificar y bloquear la comunicación con redes de bots;	REQUERIDO
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;	REQUERIDO
Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;	REQUERIDO
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;	REQUERIDO
Los eventos deben identificar el país que origino la amenaza;	REQUERIDO
Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);	REQUERIDO
Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;	REQUERIDO
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;	REQUERIDO
En caso de que el firewall pueda coordinarse con software de seguridad en equipo	REQUERIDO

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;	
Proporcionar 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);	REQUERIDO
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);	REQUERIDO
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;	REQUERIDO
Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;	REQUERIDO
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;	REQUERIDO
Tener por lo menos 75 categorías de URL;	REQUERIDO
Debe tener la funcionalidad de exclusión de URLs por categoría;	REQUERIDO
Permitir página de bloqueo personalizada;	REQUERIDO
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);	REQUERIDO
Además del Explicit Web Proxy, soportar proxy web transparente;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/control basados en usuarios y grupos de usuarios;	REQUERIDO
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);	REQUERIDO
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;	REQUERIDO
Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;	REQUERIDO
Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;	REQUERIDO

Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;	REQUERIDO
QoS Traffic Shaping	
Capacidad de controlar el ancho de banda máximo utilizado, por usuario o aplicación, tanto audio como vídeo sobre demanda	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;	REQUERIDO
Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;	REQUERIDO
En QoS debe permitir la definición de tráfico con ancho de banda garantizado;	REQUERIDO
En QoS debe permitir la definición de tráfico con máximo ancho de banda;	REQUERIDO
En QoS debe permitir la definición de colas de prioridad;	REQUERIDO
Soportar marcación de paquetes DiffServ, incluso por aplicación;	REQUERIDO
Soportar la modificación de los valores de DSCP para Diffserv;	REQUERIDO
Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);	REQUERIDO
Debe soportar QoS (traffic-shaping) en las interfaces agregadas o redundantes;	REQUERIDO
Filtro de Datos	
Permite la creación de filtros para archivos y datos predefinidos;	REQUERIDO
Los archivos deben ser identificados por tamaño y tipo;	REQUERIDO
Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;	REQUERIDO
Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;	REQUERIDO
Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;	REQUERIDO
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;	REQUERIDO
Geo Localización	
Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;	REQUERIDO
Debe permitir la visualización de los países de origen y destino en los registros de acceso;	REQUERIDO
Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;	REQUERIDO
VPN	
Soporte VPN de sitio-a-sitio y cliente-a-sitio;	REQUERIDO
Soportar VPN IPSec;	REQUERIDO
Soportar VPN SSL;	REQUERIDO
La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512	REQUERIDO
La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;	REQUERIDO
La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);	REQUERIDO
La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);	REQUERIDO
Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;	REQUERIDO
Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6	REQUERIDO

IPSec;	
Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución.	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;	REQUERIDO
Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;	REQUERIDO
Deberá mantener una conexión segura con el portal durante la sesión;	REQUERIDO
El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.	REQUERIDO
Wireless Controller	
Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);	REQUERIDO
Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;	REQUERIDO
Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac y que transmitan tráfico IPv4 e IPv6 a través del controlador;	REQUERIDO
La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;	REQUERIDO
El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;	REQUERIDO
La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario;	REQUERIDO
Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points;	REQUERIDO
El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tunelados hasta el controlador inalámbrico;	REQUERIDO
Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;	REQUERIDO
Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico;	REQUERIDO
Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPA/WPA2-Personal (PSK), en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;	REQUERIDO
La solución debe permitir definir qué redes serán tuneladas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso;	REQUERIDO
La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tunelados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso;	REQUERIDO

La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz;	REQUERIDO
La solución debe detectar Receiver Start of Packet (RX-SOP) en paquetes inalámbricos y ser capaz de omitir aquellos que están por debajo de determinado umbral especificado en dBm;	REQUERIDO
La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso;	REQUERIDO
La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y batida en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados;	REQUERIDO
La solución debe identificar automáticamente puntos de acceso intrusos que estén conectados a la red de cable (LAN). La solución debe ser capaz de identificar el punto de acceso intruso incluso cuando el MAC Address de la interfaz LAN es ligeramente diferente (adyacente) del MAC Address de la interfaz WLAN;	REQUERIDO
La solución debe detectar los puntos de acceso no autorizados y / o intrusos a través de radios dedicados a la función de análisis o a través de Off-channel / Background scanning. Cuando se realiza a través de Off-channel / Background scanning, la solución debe ser capaz de identificar el uso del punto de acceso para, en caso necesario, retrasar el análisis y de esta forma no perjudicar a los clientes conectados;	REQUERIDO
La solución debe permitir la configuración individual de las radios del punto de acceso para que operen en el modo monitor, o sea, con función dedicada para detectar amenazas en la red inalámbrica y con ello permitir mayor flexibilidad en el diseño de la red;	REQUERIDO
La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y sincronizar la configuración del principal, además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener función de primario de forma temporal;	REQUERIDO
La solución debe permitir el agrupamiento de VLANs para que se distribuyan múltiples subredes en un determinado SSID, reduciendo así el broadcast y aumentando la disponibilidad de direcciones IP;	REQUERIDO
La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado;	REQUERIDO
La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios;	REQUERIDO
Debe permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;	REQUERIDO
La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;	REQUERIDO
La solución debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia;	REQUERIDO
La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming de la cliente conectada mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;	REQUERIDO
La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la	REQUERIDO

infraestructura inalámbrica;	
La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado;	REQUERIDO
La solución debe implementar técnicas de Call Admission Control para limitar el número de llamadas simultáneas;	REQUERIDO
La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica y presentar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado, Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación;	REQUERIDO
Para garantizar una mejor distribución de dispositivos entre las frecuencias disponibles y mejorar la utilización de la radiofrecuencia, la solución debe ser capaz de distribuir automáticamente los dispositivos de banda dual para que se conecten primariamente a 5GHz a través del recurso conocido como Band Steering;	REQUERIDO
La solución debe permitir la configuración de los data rates que se activarán en la herramienta y las que se deshabilitan para las frecuencias de 2.4 y 5GHz y los estándares 802.11a / b / g / n / ac;	REQUERIDO
La solución debe tener capacidad capaz de convertir paquetes Multicast en paquetes Unicast cuando se reenvían a los dispositivos que están conectados a la infraestructura inalámbrica, mejorando así el consumo de Airtime;	REQUERIDO
La solución debe soportar la característica que ignore Probe Requests de clientes que tienen una señal débil o distante. Debe permitir definir el umbral para que los Probe Requests sean ignorados;	REQUERIDO
La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz;	REQUERIDO
La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;	REQUERIDO
La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio direcciones de origen y destino (IPv4 e IPv6), puertos y protocolos;	REQUERIDO
La solución debe implementar la función de web filtering para controlar los sitios que se accede a la red. Debe poseer una base de conocimiento para categorizar los sitios y permitir configurar qué categorías de sitios serán permitidos y bloqueados para cada perfil de usuario y SSID;	REQUERIDO
La solución debe tener capacidad de reconocimiento de aplicaciones a través de la técnica de DPI (Deep Packet Inspection) que permita al administrador de la red monitorear el perfil de acceso de los usuarios e implementar políticas de control. Debe permitir el funcionamiento de esta característica y la actualización periódica de la base de aplicaciones durante todo el período de garantía de la solución;	REQUERIDO
La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil quinientas) aplicaciones;	REQUERIDO
La solución debe permitir la creación de reglas para el bloqueo y el límite de banda (en Mbps, Kbps ou Bps) para las aplicaciones reconocidas a través de la técnica de DPI;	REQUERIDO
La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;	REQUERIDO
La solución debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica. Al menos los siguientes ataques deben ser identificados:	REQUERIDO
- Ataques de flood contra el protocolo EAPOL (EAPOL Flooding);	
- Los siguientes ataques de denegación de servicio: Association Flood, Authentication Flood, Broadcast Deauthentication y Spoofed Deauthentication;	

- ASLEAP;	
- Null Probe Response / Null SSID Probe Response;	
- Long Duration;	
- Ataques contra Wireless Bridges;	
- Weak WEP;	
- Invalid MAC OUI.	
La solución debe implementar mecanismos de protección para mitigar ataques a la infraestructura inalámbrica. Al menos ataques de denegación de servicio deben ser mitigados por la infraestructura a través del envío de paquetes de deauthentication	REQUERIDO
La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;	REQUERIDO
La solución debe monitorear y clasificar el riesgo de las aplicaciones accedidas por los clientes inalámbricos;	REQUERIDO
Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;	REQUERIDO
Debe implementar la autenticación administrativa a través del protocolo RADIUS;	REQUERIDO
En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);	REQUERIDO
En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;	REQUERIDO
La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;	REQUERIDO
Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada;	REQUERIDO
La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS;	REQUERIDO
La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X;	REQUERIDO
La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;	REQUERIDO
La solución debe implementar la característica de autenticación de los usuarios a través de la página web HTTPS, también conocido como Captive Portal. La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red;	REQUERIDO
La solución debe permitir el hospedaje del portal cautivo (captive portal) en la memoria interna del controlador inalámbrico;	REQUERIDO
La solución debe permitir la personalización de la página de autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes;	REQUERIDO
La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;	REQUERIDO
La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;	REQUERIDO
La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada;	REQUERIDO
La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6;	REQUERIDO
La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución;	REQUERIDO

Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;	REQUERIDO
La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;	REQUERIDO
La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;	REQUERIDO
La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible;	REQUERIDO
La solución debe permitir la configuración de redes Mesh entre los puntos de acceso administrados por ella;	REQUERIDO
La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;	REQUERIDO
La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;	REQUERIDO
La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;	REQUERIDO
La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps;	REQUERIDO
La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;	REQUERIDO
La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);	REQUERIDO
La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato. pcap;	REQUERIDO
La solución debe permitir la adición de planta baja del pavimento para ilustrar gráficamente la posición geográfica y el estado de operación de los puntos de acceso administrados por ella. Debe permitir la adición de plantas bajas en los siguientes formatos: JPEG, PNG, GIF o CAD;	REQUERIDO
La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos;	REQUERIDO
La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;	REQUERIDO
La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;	REQUERIDO
La solución debe permitir la identificación del firmware utilizado por cada punto de acceso administrado y permitir la actualización individualizada a través de interfaz gráfica;	REQUERIDO
La solución debe tener herramientas de diagnóstico y depuración;	REQUERIDO
La solución debe soportar la comunicación con elementos externos a través de las API;	REQUERIDO
La solución deberá ser compatible y administrar los puntos de acceso de este proceso;	REQUERIDO
Instalación, configuración y garantía	
Se requiere que el oferente cuente con el más alto nivel de asociado, con la empresa fabricante del producto, garantizando a la institución un vínculo con un canal experto del fabricante. Entiéndase por ello categorías como Elite, Premium, Experto, o similares que hagan referencia al nivel más alto.	REQUERIDO
El plazo de garantía será de 36 meses, se entiende por garantía el mantenimiento preventivo y correctivo del software en la modalidad de al menos 24x7 incluyendo el reemplazo del software en caso de necesidad, solución de errores debido a algún incidente o corrupción en el software, así como la instalación de las actualizaciones que pudieran surgir durante el referido periodo.	REQUERIDO

El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La validez de las licencias debe ser por un periodo de mínimo 36 meses.	REQUERIDO

ITEM 2. PROVISIÓN, INSTALACIÓN Y CONFIGURACIÓN DE SOFTWARE DE REGISTROS, ANÁLISIS Y REPORTES	
Descripción	**Requerimiento mínimo**
Software de Reporte	REQUERIDO
Denominación	indicar
Versión	indicar
Procedencia	indicar
Cantidad	1 (uno)
Requisitos Mínimos	
Sistema de Reportería en formato Virtualizado (VM) para instalación en ambientes virtualizados	REQUERIDO
Funcionalidades Generales	
Compatible con el ambiente VMware ESXi 5.0/5.1/5.5/6.0/6.5/6.7;	REQUERIDO
Compatible con el ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2/2016	REQUERIDO
Compatible con el ambiente Citrix XenServer 6.0+	REQUERIDO
Compatible con el ambiente Open Source Xen 4.1+	REQUERIDO
Compatible con el ambiente KVM on Redhat 6.5+ and Ubuntu 17.04	REQUERIDO
Compatible con el ambiente Nutanix AHV (AOS 5.10.5)	REQUERIDO
Compatible con el ambiente Amazon Web Services (AWS)	REQUERIDO
Compatible con el ambiente Microsoft Azure.	REQUERIDO
Compatible con el ambiente Google Cloud (GCP)	REQUERIDO
Compatible con el ambiente Oracle Cloud Infrastructure (OCI)	REQUERIDO
Compatible con el ambiente Alibaba Coud (AliCloud)	REQUERIDO
No debe haber límites a la cantidad de múltiples vCPU	REQUERIDO
No debe haber límites a la expansión de memoria RAM	REQUERIDO
Debe soportar acceso vía SSH, WEB (HTTPS) para la gestion de la solución	REQUERIDO
Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.	REQUERIDO
Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.	REQUERIDO
Soporte SNMP versión 2 y 3	REQUERIDO
Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.	REQUERIDO
Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.	REQUERIDO
Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH	REQUERIDO
Autenticación de usuarios de acceso a la plataforma vía LDAP	REQUERIDO
Autenticación de usuarios de acceso a la plataforma vía Radius	REQUERIDO
Autenticación de usuarios de acceso a la plataforma vía TACACS+	REQUERIDO
Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos	REQUERIDO
Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.	REQUERIDO
Generación de informes en tiempo real de tráfico, en formato de gráfica tabla	REQUERIDO

Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.	REQUERIDO
Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.	REQUERIDO
Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado	REQUERIDO
Contar con mecanismos de borrado automático de logs antiguos.	REQUERIDO
Permitir la importación y exportación de reportes	REQUERIDO
Debe contar con la capacidad de crear informes en formato HTML	REQUERIDO
Debe contar con la capacidad de crear informes en formato PDF	REQUERIDO
Debe contar con la capacidad de crear informes en formato XML	REQUERIDO
Debe contar con la capacidad de crear informes en formato CSV	REQUERIDO
Debe permitir exportar los logs en formato CSV	REQUERIDO
Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.	REQUERIDO
Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.	REQUERIDO
La solución debe contar con reportes predefinidos	REQUERIDO
Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución	REQUERIDO
Debe ser posible la duplicación de reportes existentes para su posterior edición.	REQUERIDO
Debe tener la capacidad de personalizar la portada de los reportes obtenidos.	REQUERIDO
Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.	REQUERIDO
Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.	REQUERIDO
Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas	REQUERIDO
Debe poseer mecanismo de “Drill-Down” para navegar en los reportes de tiempo real.	REQUERIDO
Debe permitir descargar de la plataforma los archivos de logs para uso externo.	REQUERIDO
Tener la capacidad de generar y enviar reportes periódicos automáticamente.	REQUERIDO
Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.	REQUERIDO
Permitir el envío por email de manera automática de reportes.	REQUERIDO
Debe permitir que el reporte a enviar por email sea al destinatario específico.	REQUERIDO
Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.	REQUERIDO
Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.	REQUERIDO
Debe permitir el uso de filtros en los reportes.	REQUERIDO
Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.	REQUERIDO
Permitir especificar el idioma de los reportes creados	REQUERIDO
Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.	REQUERIDO
Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.	REQUERIDO
Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.	REQUERIDO

Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.	REQUERIDO
Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.	REQUERIDO
Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.	REQUERIDO
Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.	REQUERIDO
Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.	REQUERIDO
Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.	REQUERIDO
Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos	REQUERIDO
Debe permitir visualizar en tiempo real los logs recibidos.	REQUERIDO
Debe permitir el reenvío de logs en formato syslog.	REQUERIDO
Debe permitir el reenvío de logs en formato CEF (Common Event Format).	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea actividad VPN ren su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)	REQUERIDO
Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC	REQUERIDO
Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3	REQUERIDO
Debe permitir generar alertas de eventos a partir de logs recibidos	REQUERIDO
Debe permitir crear incidentes a partir de alertas de eventos para endpoint	REQUERIDO
Debe permitir la integración al sistema de tickets ServiceNow	REQUERIDO
Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.	REQUERIDO
Debe permitir respaldar logs en nube publica de Amazon S3	REQUERIDO
Debe permitir respaldar logs en nube publica de Microsoft Azure	REQUERIDO
Debe permitir respaldar logs en nube publica de Google Cloud	REQUERIDO
Debe soportar el estándar SAML para autenticación de usuarios administradores	REQUERIDO
Reportes de Firewall	
Debe contar con reporte de cumplimiento de PCI DSS	REQUERIDO

Debe contar con reporte de utilización de aplicaciones SaaS	REQUERIDO
Debe contar con reporte de prevención de perdida de datos (DLP)	REQUERIDO
Debe contar con reporte de VPN	REQUERIDO
Debe contar con reporte de Sistema de prevención de intrusos (IPS)	REQUERIDO
Debe contar con reporte de reputación de cliente	REQUERIDO
Debe contar con reporte de análisis de seguridad de usuario	REQUERIDO
Debe contar con reporte de análisis de amenaza cibernética	REQUERIDO
Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad	REQUERIDO
Debe contar con reporte de tráfico DNS	REQUERIDO
Debe contar con reporte tráfico de correo electrónico	REQUERIDO
Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red	REQUERIDO
Debe contar con reporte de Top 10 de Websites utilizadas en la red	REQUERIDO
Debe contar con reporte de uso de redes sociales	REQUERIDO
Compatibilidad con ITEM 1 Firewall	
Para garantizar la compatibilidad de las funciones requeridas, el sistema deberá ser del mismo fabricante del Ítem 1, o en su defecto contar con un respaldo documentacional de interoperabilidad de las funciones solicitadas del sistema de reporte, tanto del Fabricante del ITEM 1, como del Fabricante del ITEM 2. Es decir, ambos fabricantes deberán garantizar mediante nota dirigida a la Convocante la interoperabilidad.	REQUERIDO
Instalación, configuración y garantía.	
Se requiere que el oferente cuente con el más alto nivel de asociado, con la empresa fabricante del producto, garantizando a la institución un vínculo con un canal experto del fabricante. Entiéndase por ello categorías como Elite, Premium, Experto, o similares que hagan referencia al nivel más alto.	REQUERIDO
El plazo de garantía será de 36 meses, se entiende por garantía el mantenimiento preventivo y correctivo del software en la modalidad de al menos 24x7 incluyendo el reemplazo del software en caso de necesidad, solución de errores debido a algún incidente o corrupción en el software, así como la instalación de las actualizaciones que pudieran surgir durante el referido periodo.	REQUERIDO
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La validez de las licencias debe ser por un periodo de mínimo 36 meses.	REQUERIDO

ITEM 3. "PROVISIÓN, INSTALACIÓN Y CONFIGURACIÓN DE EQUIPOS DE CONMUTACIÓN (SWITCH)"	
Descripción	**Requerimiento mínimo**
Marca	indicar
Modelo	indicar
Procedencia	indicar
Cantidad	2 (dos)
Descripción	Switch de Acceso
Tipo de configuración	Fija
Stacking/Apilamiento: máximos equipos apilables	4
Tipo de uso	Acceso a Proveedores
Interfaces y rendimiento	
Interfaces independientes 10/100/1000BaseT-Cobre UTP RJ45	24 puertos RJ45
Interfaces SFP+ independientes (1/10Gbps)	4 puertos SFP+
Puerto 10/100 BaseT Ethernet adicional e independiente para administración del	1 puerto RJ45

equipo (Out of Band Management)	
Puerto SERIAL RS-232 para ser usado como consola de administración.	1 puerto serial
Puerto USB para el almacenado y descarga de configuraciones y sistema operativo	1 puerto USB
Capacidad de conmutación de paquetes unidireccional	64 Gbps
Capacidad de conmutación de paquetes bidireccional	128 Gbps
Throughput de Capa 2/Capa 3 (Mbps)	95 Mpps
Stacking/Apilamiento	
Capacidad de backplane del Stack utilizando los puertos de UPLINK	80 Gbps
Equipos agrupados para administrar con un único acceso administrativo	4 switches
Cables de stacking proporcionados para la interconexión de equipos	1 cable DAC 10Gbps
Deberá soportar el protocolo Link Aggregation Control Protocol (LACP) IEEE 802.3ad.	Exigido
Número de grupos a soportar por todo el STACK	128
Calidad de Servicio	
Encolamiento basado en clases de servicio con priorización de tráfico – Strick priority en egreso	Exigido
Soporte de Port Shaping : puede ser usados para manjar el excesso de tráfico, esta caracteristica define el ancho de banda maximo alojado en un puerto	Exigido
Soporte de queuing shaping: puede ser usados para manjar el excesso de tráfico, esta caracteristica define el ancho de banda maximo alojado en cada cola	Exigido
Soporte de QoS en puertos LAG	Exigido
L2 QoS (classification, rewrite, queuing) Permite la clasificacio re-escritura y encolamiento de CoS en interfaces de layer 2.	Exigido
L3 QoS (classification, rewrite, queuing) Permite la clasificacio re-escritura y encolamiento de CoS en interfaces de layer 3	Exigido
Sopoorte de QoS – Clasificacion, re-write y queueing en interfaces RVI (Interface VLANs)	Exigido
Soporta el tratamiento de las colas ante congestión con los mecanismos SDWRR (Shaped deficit Weighted Round Robin) y SPQ (Strict Priority).	Exigido
Soporta el protocolo LLDP (Link Layer Discovery Protocol) IEEE 802.1AB y LLDP-MED (LLDP for Media Endpoint Device) ANSI/TIA-1057 integrado para Voice sobre IP (VoIP)	Exigido
Soporte de priorización de tráfico de salida por hardware mínimo ocho (8) colas de servicio por puerto.	Exigido
Politicas de trafico de red que limitan la velocidad de entrada y salida de una clase de tráfico con base en el criterio establecido por el usuario. Permite control la velocidad maxima de tráfico enviado o recibido en una interfaz y particionar una red en multiples nieles de clase de servicio	Exigido
Encolado estricto y de baja latencia (Strict priority queuing or Low Latency Queuing (LLQ)Strict priority queuing, or low latency queuing (LLQ): es una caracteristica usada para reeenviar de forma más rapida ciertos tipos de tráfico sensible a retardos (voz, video etc)	Exigido
Trust 802.1p/DSCP/IP Prec (ingress)	Exigido
Soporte de limitación de tráfico mediante lista de control de acceso (ACL) aplicable en los puertos fisicos o VLANs por:	
Filtros basados en direcciones MAC origen o destino	Exigido
Filtros basados en direcciones IP origen o destino	Exigido
Filtros basados en número de puerto TCP/UDP	Exigido
Cantidad de filtros de tráfico (ACL)	1500
Spanning Tree Protocol	
IEEE 802.1d.	Exigido
Rapid Spanning Tree IEEE 802.1w	Exigido

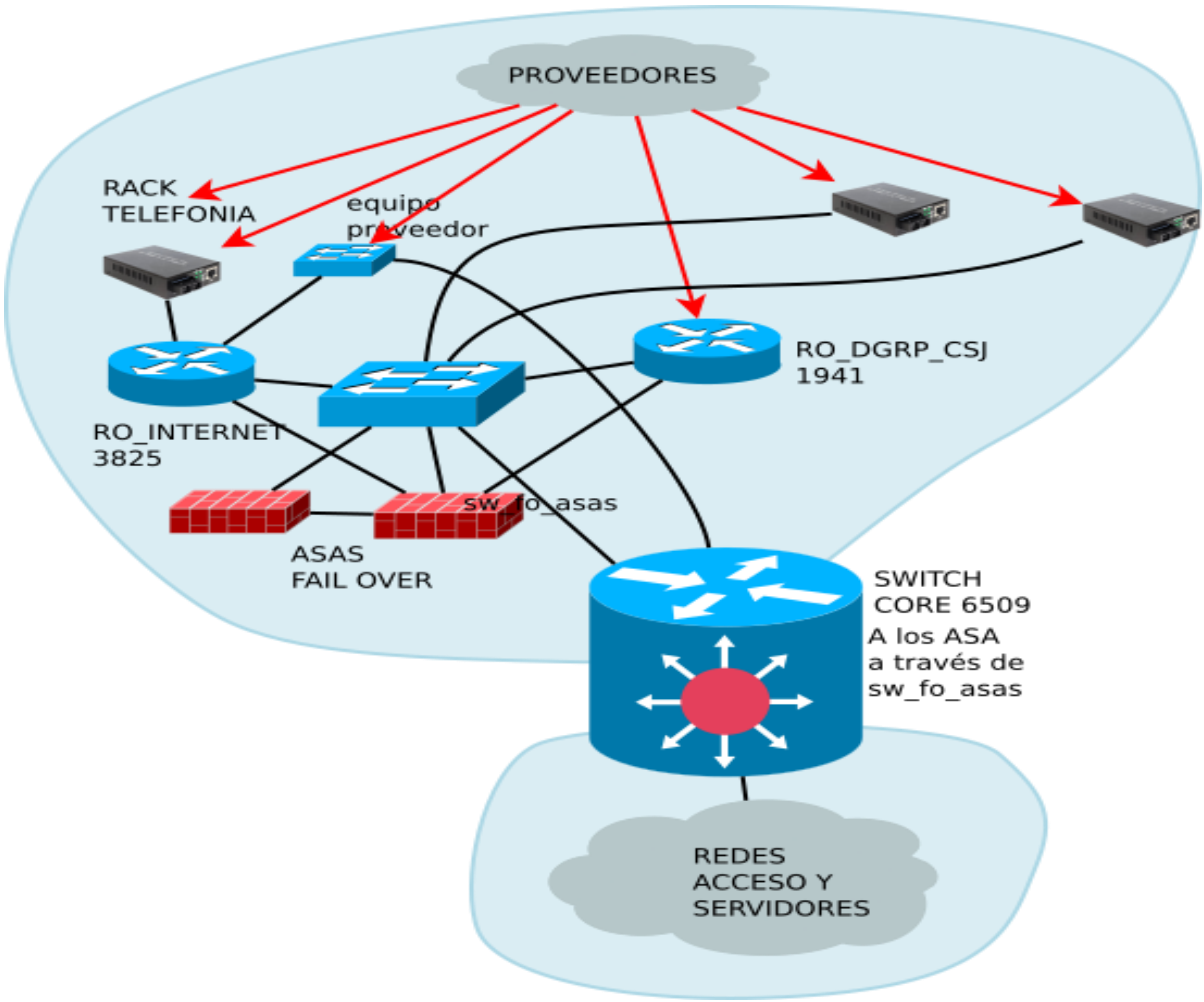
Multiple Spanning Tree Protocol IEEE 802.1s.	Exigido
Soporte de Time Domain Reflectometry para detectar las fallas en cables UTP	Exigido
Soporte de ruteo layer 3 por medio de los siguientes protocolos:	
Rutas Estáticas	Exigido
Soporte maximo de rutas IPv4	512 prefijos; 4096 rutas
Soporte de IEEE802.1ag Ethernet OAM connectivity fault management (CFM)	Exigido
Soporte de Ethernet ring protection switching (ERPS, G.8032/Y.1344)	Exigido
Soporte de TDR (Time Domain Reflectometry). Una tecnologia que permite el segumiento y senializacion de fallas en los cables o conectores de redes de computadoras. Los puertos deben ser capaces de generar un pulso electromagnético, cuando este pulso alcanza un obstáculo o el fin del cable se genera un eco que es traducido en la distancia a la falla.	Exigido
RIP v1/v2	Exigido
RIPng	Exigido
Soporte OSPF	Exigido
Soporte de Layer 2 protocol tunneling (L2PT)	Exigido
Soporte de ARP (número de entradas)	1024
Funcionalidades layer 2	
Soporte máximo de direcciones MAC de red.	16000
Soporte de tramas Jumbo	Exigido
Soporte de IEEE 802.1X para VLAN VoIP.	Exigido
Port-based VLAN	Exigido
MAC-based VLAN	Exigido
Soporte IEEE 802.1Q-in-Q: VLAN Stacking	Exigido
IEEE 802.1ak: Multiple VLAN Registration Protocol (MVRP)	Exigido
Compatible with Per-VLAN Spanning Tree Plus	Exigido
Soporte de interfaces RVI (Routed VLAN Interfaces)	Exigido
Capacidad de soportar definición de dominios de broadcast VLANs (Virtual LANs) en todos los puertos según IEEE 802.1 p/Q.	Exigido
Numero de VLANs configurables en el Virtual Chasis	4092
VLANS en equipo individual	4092
Posible rango de VLAN-ID para configurar	1 - 4092
Soporte de DHCP Relay y DHCP helper	Exigido
Soporte de DHCP Server sobre interfaces RVI	Exigido
Voice VLAN fallback	Exigido
Multicast	
Soporte protocolo IGMP-Snooping	Exigido
Soporte PIM-SM, PIM-SSM, PIM-DM	Exigido
Soporte IGMP: v1, v2, v3	Exigido
Administracion / Management	
Deberá soportar Simple Network Management Protocol versión SNMP v2c, SNMP v3.	Exigido
Capacidad de proveer los bloques de información de management (MIBs) necesarios.	Exigido
Capacidad de Remote Monitoring (RMON), deberá soportar al menos cuatro (4) grupos (statistics, history, alarm, events).	Exigido
sFlow	Exigido
Soporte de registro remoto (SysLog).	Exigido
Soporte de traffic mirroring por puerto o por VLAN.	Exigido

Deberá soportar Network Timing Protocol (NTP).	Exigido
Creación de 20 perfiles de administrador con facultadas específicas de modificar la configuración o solo acceder a vistas de la misma y listado de comandos disponibles para ejecutar por cada perfil	Exigido
Las passwords (claves) de administrador almacenadas localmente deben estar encriptadas usando hash MD5 o SHA1	Exigido
Soporte de MIB para la información de media attachment unit (MAU)	Exigido
Fuente para AC	Exigido
Accesorios necesarios para montar en racks estándar de 19”.	Exigido
Seguridad, mecanismos soportados	
Central Web authentication	Exigido
Deberá soportar autentificación 802.1X. para diferentes VLANs por puerto.	Exigido
Soporte de IEEE 802.1X con soporte de VLANs de invitados (Guest VLAN)	Exigido
MAC Radius Authentication con 802.1X	Exigido
Soporte de protocolo EAP-PAP para MAC RADIUS authentication	Exigido
Soporte de seguridad del puerto mediante filtrado por dirección MAC. En caso de violación del puerto deberá poder enviarse una alerta al administrador y deshabilitar el puerto.	Exigido
Soporte de limitación de direcciones MAC por puerto.	Exigido
Soporte de Persistent MAC learning o sticky MAC	Exigido
DHCP Snooping.	Exigido
Dynamic ARP inspection (DAI)	Exigido
Proxy ARP	Exigido
Static ARP support	Exigido
IP source guard	Exigido
Orden de autenticación flexible	Exigido
IPv6 Neighbor Discovery inspection	Exigido
Servicio de configuración por medios seguros:	
Soporte Telnet / Secure Shell (SSH) versión 2 para conexión remota vía interfaz línea de comando (CLI).	Exigido
Soporte vía Web con SSL. (HTTPS)	Exigido
Soporte de creación de Certificados locales para conexión HTTPs	Exigido
Almacenamiento de sistema operativo y configuración en memoria Flash reescribible.	2 GB
Roll-back a varias configuraciones anteriores almacenadas en el equipo (mínimo 3 configuraciones) o una configuración de rescate almacenada especialmente por el administrador	Exigido
Mecanismos de automatización mediante scripts o similares que permitan chequear el cumplimiento y administrar los cambios de configuraciones, aplicar configuraciones predefinidas, visualizar conjuntos de comandos para el diagnóstico, análisis y administración de eventos, y generar respuestas predefinidas a eventos.	Exigido
Servicio de configuración por medio de consola serial RS-232 asincrónica	Exigido
La unidad deberá ser entregada con 1 (un) juego de manuales de configuración de hardware y software. Estos manuales podrán ser entregados de manera impresa o bien en medio digital.	Exigido
Equipos alimentados con 220 V - 50 Hz, monofásico con toma de 3 patas, sin necesidad de requerir un transformador adicional.	Exigido
Troubleshooting	
Debugging: CLI via console, telnet, or SSH	Exigido
Diagnostics: Show and debug command statistics	Exigido

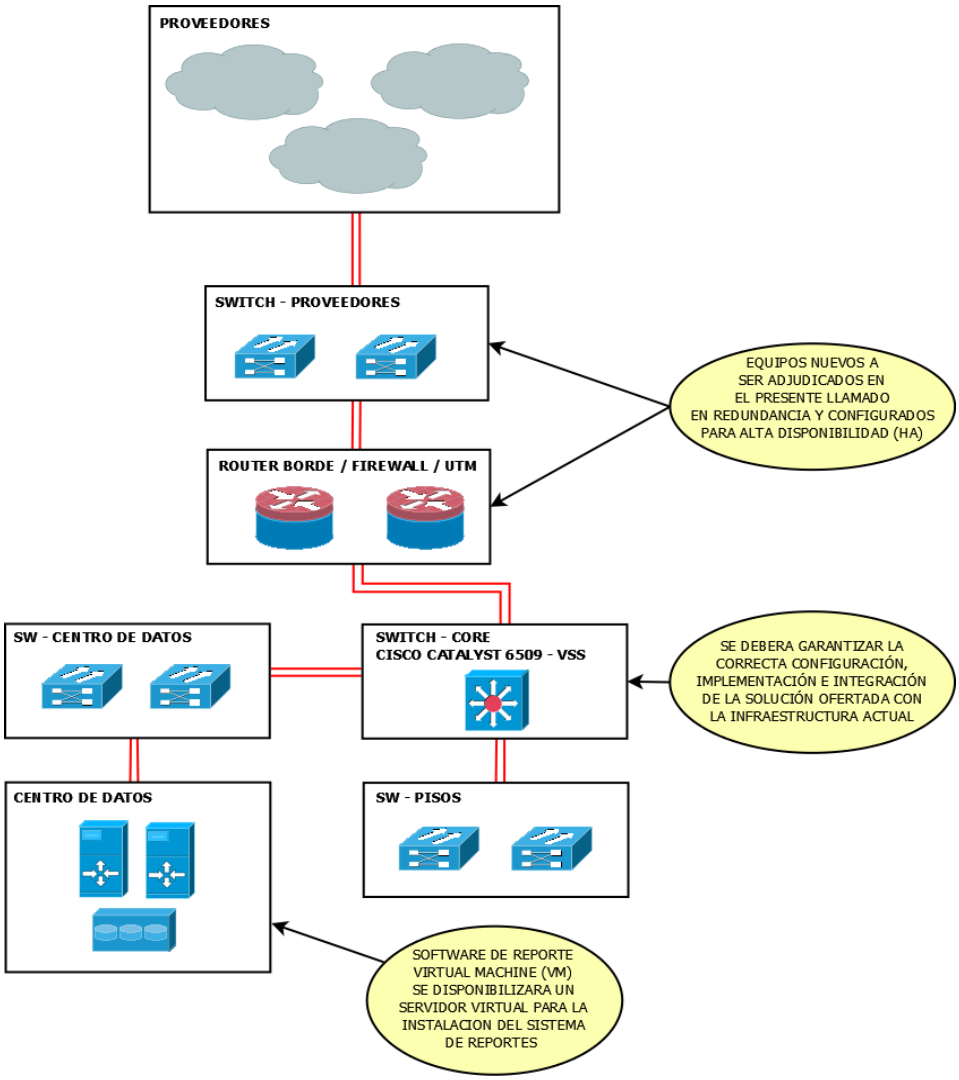
Traffic mirroring (port)	Exigido
Traffic mirroring (VLAN)	Exigido
ACL-based mirroring	Exigido
Mirroring destination ports per system	Exigido
LAG port monitoring	Exigido
Multiple destination ports monitored to 1 mirror (N:1)	Exigido
Maximum number of mirroring sessions	Exigido
Mirroring to remote destination (over L2)	Exigido
IP tools: Extended ping and trace	Exigido
Alta disponibilidad	
Soporte de Link Aggregation	Exigido
802.3ad (LACP) support: Number of LAGs supported	128
Maximum number of ports per LAG:	8
LAG sharing algorithm—Routed Multicast Traffic:	
Tagged ports support in LAG	Exigido
Uplink Failure Detection (UFD)	Exigido
Soporte para equipos con dos Routing engines, configurar al Routing engine de respaldo para asumir el rol de master sin causar interrupcion en el reenvio.	Exigido
Soporte VRRP (Virtual Router Redundancy Protocol)	Exigido
Alimentación Eléctrica, Ventilación y dimensiones.	
Tensión de operación Fuente de Alimentación 100-120V / 200-240V auto detectable.	Exigido
Cumplimiento de ROHS	Exigido
Temperatura de operación: 0°C a 45°C	Exigido
Humedad de operación: 10% a 85% de humedad relativa máxima, sin condensación.	Exigido
Montaje en rack de 19”	Exigido
Cantidad de Unidad de Rack del Equipo	1U
MTBF	260.000 hs
Instalación, configuración y garantía.	
Instalación: El equipo deberá ser configurado, instalado y probado de acuerdo a las indicaciones de la Convocante, por personal técnico del oferente.	Exigido
Actualización de software: El sistema operativo deberá ser actualizado a la última versión disponible a pedido del cliente durante la duración del contrato.	Exigido
Plazo de garantía del fabricante	36 meses

ITEM 4. – “SERVICIO DE CAPACITACIÓN”	
Descripción	**Requerimiento mínimo**
Servicio de capacitación, para al menos 5 (CINCO) funcionarios, con una duración mínima de 30 horas (reloj), por cada ítem solicitado (1, 2 y 3), en modalidad presencial, en las oficinas de la Convocante, en horario de oficina y con entrega de certificados.	REQ UERIDO

ESQUEMA ACTUAL DE RED https://ibb.co/M6WYjQF



ESQUEMA REQUERIDO DE RED https://ibb.co/DwXYfBg



Switch de acceso a Proveedores
Equipos dedicados a concentrar los servicios de los proveedores. Los mismos estarán en redundancia, garantizando alta disponibilidad, distribuyendo las conexiones hasta los equipos de borde.

Enrutador / Firewall UTM de Borde
Dispositivo del tipo UTM en el esquema borde; el cual pueda gestionar todo el tráfico interno y externo, brindando de esta manera una capa de seguridad mejorada. Los mismos estarán en redundancia, garantizando alta disponibilidad.

Software de Reportes
Herramienta dedicada a la gestión de registros, análisis e informes, con capacidad de permitir operaciones de seguridad, identificación proactiva y corrección de riesgos, y visibilidad completa de todo el panorama de ataques en la red.

SON PROVEEDORES EN EL BORDE DE COMUNICACIONES:
PROVEEDOR DE INTERNET A
Acceso a Internet
Enlace punto a punto entre la DGRP y la CSJ

PROVEEDOR DE INTERNET B
Acceso a Internet

CSJ
Enlace propio que conecta a la DGRP con la CSJ.

MITIC
Enlace para el Servicio de Intercambio de Información (SII) entre Organismos y Entidades del Estado (OEE)

SNC
Enlace propio que conecta a la DGRP con la SNC.

PLAN DE ENTREGAS

ÍTEM	DESCRIPCIÓN DEL BIEN	CANTIDAD	UNIDAD DE MEDIDA	LUGAR DE ENTREGA DE LOS BIENES	FECHA(S) FINAL(ES) DE EJECUCIÓN DE LOS BIENES
1	TODOS LOS ÍTEMS	SEGÚN LAS EETT	SEGÚN LAS EETT	El oferente adjudicado deberá entregar los bienes (equipos de conmutación, seguridad de red de datos y software de reportes), como también, el cronograma, contenido y fechas tentativas para la realización de la capacitación dentro de los 60 (sesenta) días hábiles posteriores a la firma del contrato, y dispondrá, de otros 30 (treinta) días hábiles, posteriores a la entrega de los bienes, para realizar la planificación, instalación, configuración e implementación de los ítems adjudicados. Todo esto, debe ser entregado, instalado, configurado, implementado y realizado en el edificio de la Dirección General de los Registros Públicos, sito en Avda. Eusebio Ayala casi Capitán Román García, de lunes a viernes de 07:15 hs a 13:00 hs, salvo los feriados oficiales y de conformidad al horario normal y diferenciado de los funcionarios de la DGRP. La emisión del Acta de Recepción Total dada por la Contratante, significará el cumplimiento por parte del Proveedor de sus obligaciones contractuales y le facultará a solicitar el pago de la misma.	36 (TREINTA Y SEIS) MESES, CONTADOS DESDE LA FIRMA DEL CONTRATO.

INDICADORES DE CUMPLIMIENTO DE CONTRATO

- El documento requerido para acreditar el cumplimiento contractual, será: **Acta de recepción Definitiva.**
- **Serán presentados:** 1 (un) Acta Final por la entrega efectuada.
- **Frecuencia:** Conforme se establece en el Plan de Entrega de bienes establecido en el PBC.

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
Acta de Recepción Definitiva.	Acta	90 (noventa) días hábiles, computados a partir de la fecha de la firma del contrato