Informe Técnico de Evaluación de la Licitación "ADQUISICIÓN DE EQUIPAMIENTO PARA EL DATACENTER DE LA DGAF (MEF)" – ID 446703

El presente informe tiene como objetivo presentar el resumen de las evaluaciones de las propuestas técnicas presentadas en respuesta a la licitación pública ID 446703, destinada a la adquisición de equipamiento para el datacenter de la Dirección General de Administración Financiera (DGAF) del Ministerio de Economía y Finanzas (MEF). Se han analizado las ofertas recibidas para los cuatro lotes, considerando las especificaciones técnicas detalladas en el pliego de bases y condiciones.

La evaluación se llevó a cabo siguiendo los criterios técnicos y administrativos establecidos en el pliego de bases y condiciones. Se realizó un análisis exhaustivo de la documentación presentada por cada oferente, verificando el cumplimiento de los requisitos técnicos y administrativos solicitados. Además, se solicitaron aclaraciones a los oferentes cuando se identificaron dudas o inconsistencias en la información proporcionada.

A continuación, se presentan los resultados del análisis de las propuestas presentadas por cada oferente, considerando los criterios técnicos y administrativos establecidos en el pliego de bases y condiciones:

LOTE 1: Servidor para Clúster
Se procede a evaluar al único oferente, la empresa SSD.

Características	Mínimo exigido	CUMPLE / NO CUMPLE
Marca	XFusion	CUMPLE
Modelo	2288H V7	CUMPLE
Origen	CHINA	CUMPLE
Cantidad	Tres (03)	CUMPLE
Factor de Forma	Rackeable de 2U máximo.	CUMPLE
Procesador	-Cantidad instalada en el equipo. 02 (dos) de última generación con año de lanzamiento 2023 en adelante. -Cantidad máxima soportada por el equipo. 2 (Dos) de última generación con año de lanzamiento 2023 en adelante. -Características de cada procesador. Cantidad de cores: 20 como mínimo. Frecuencia: 2.0 GHz como mínimo.	CUMPLE
Memoria	-Cantidad instalada. 1TB como mínimo. -Tipo de memoria. DDR5 4800 MT/s RDIMM o LRDIMM como mínimo. -Capacidad máxima de memoria soportado por el equipo. 4 TB como mínimo. -Cantidad máxima de slots soportados por el equipo. 16 slots por procesador como mínimo.	CUMPLE
Módulo de Plataforma Segura	El equipo debe soportar TPM 2.0 mínimamente.	CUMPLE
Almacenamiento	2 (DOS) unidad SSD SATA Hot-Plug Lectura Intensiva de 960 GB o superior. Capacidad de albergar hasta 8 discos SFF, con	CUMPLE

	capacidad de crecimiento a 24 bahías a futuro. El equipo debe poder soportar discos SAS, SATA y NVMe. -Controladora de discos. 2 GB de cache tipo Flash o superior. Soporte para RAID 0, 1, 10	
Ranuras de Expansión	2x16, 2x8 slots PCIe como mínimo.	CUMPLE
Interfaces de periféricos	Puertos USB: (04) cuatro unidades como mínimo, versión 2.0 Puerto VGA: una unidad. Los puertos deberán ser frontales o posteriores. Serial: con capacidad de poder agregar una unidad a futuro.	CUMPLE
Tarjeta Gráfica	Puerto grafico de 16MB integrado con resolución máxima de 1920x1200.	CUMPLE
Fuente de alimentación	Fuente de alimentación DUAL Redundante (1+1) platinum Hot Plug o similar.	CUMPLE
Comunicaciones	2 (dos) puertos de 1GbE como mínimo. 2 (dos) puertos 10GB LAN (opticos) con sus SFP+ como mínimo. 2 (dos) puertos 10GB LAN (cobre) como mínimo. 2 (dos) puertos de 32GB FC con sus SFP como mínimo.	CUMPLE
Sistema Operativo Soportados	Windows Server 2016 o superior. Red Hat Enterprise Linux 7.0 o superior. Xenserver 7.1 o superior. Huawei DCS FusionCompute 8.0 o superior. VMware vSphere 7.0 o superior.	CUMPLE
Características RAS	Diagnóstico de fallas de hardware en el equipo mediante LEDs indicadores. Además de luces LEDs indicadores de fallas, se requerirá que cuente con la descripción detallada de la alerta.	CUMPLE
Administración	Debe poseer puerto de consola dedicado y licenciamiento necesario para la administración remota del Servidor, que permita configurar, supervisar y actualizar el servidor. Debe poseer consola remota integrada y capacidad de montar medios virtuales.	CUMPLE
Kit de Montaje en Rack y Accesorios	Proporcionar el kit completo de: cables, soportes, organizadores y demás accesorios requeridos para el montaje y funcionamiento correcto del servidor en el rack.	CUMPLE
Montaje	Se deberá proveer el kit completo de montaje, cables, soportes, organizadores y demás accesorios requeridos para el montaje y funcionamiento correcto del servidor.	CUMPLE
Instalación	Todos los trabajos a ser ejecutados, deben ser presentados una vez terminados, de manera prolija y mecánicamente resistente. Proveer los accesorios necesarios para la realización de las tareas: cintas, tornillos, arandelas, etc. Además de cumplir con lo establecido en la presente documentación, las instalaciones deberán ser ejecutadas en un todo de acuerdo con los reglamentos para	CUMPLE

	instalaciones de los estándares internacionales.	
Fabricación	Todos los equipos deben ser nuevos fabricación 2024 y de la última generación disponible del fabricante con fabricación reciente y encontrarse en comercialización activa.	CUMPLE
Autorización	Carta de autorización del fabricante indicando que la empresa oferente es canal autorizado y está autorizado para presentar oferta para el presente llamado.	CUMPLE
Garantía	Carta de garantía del fabricante por 36 meses. El servicio de garantía deberá ser realizado por técnicos certificados avalado por el Fabricante.	CUMPLE
Plazo de entrega	60 (sesenta) días corridos desde la entrega de la orden de compra. El oferente deberá proveer los servicios profesionales necesarios para llevar a cabo de forma satisfactoria la migración de la infraestructura virtual Huawei DCS de su entorno de Producción del Ministerio de Economía y Finanzas a los nuevos servidores proveídos según requerimientos y para ello se solicita: La firma contratada deberá contar con al menos: 01 (uno) profesional con certificado vigente de PMP (Project Management Professional) certificado por el PMI (Project Manager Institute) o certificación vigente Scrum Master con reconocimiento internacional o certificaciones equivalentes, para la planificación, ejecución y control de los trabajos, Los cuales deberán ser verificable con la planilla de IPS y/o Estatuto de la empresa. 02 (dos) técnicos certificados por el fabricante de los equipos ofertados para la instalación física (rackeo) y configuración del arreglo raid. 02 (dos) técnicos certificados en el producto de virtualización de Huawei Virtualization Suite Platinum Edition los cuáles serán los encargados de diseñar el nuevo esquema de la infraestructura virtual Huawei DCS y el procedimiento de migración de las VMs a los nuevos servidores del Ministerio de Economía y Finanzas.	CUMPLE
Servicios e implementación.	También así realizarán la instalación de la Huawei DCS (la misma versión actualmente en producción) en los servidores nuevos. Deberá configurar en clúster de Huawei DCS los nuevos equipos con los mismos parámetros que actualmente está en producción el entorno virtual del Ministerio de Economía y Finanzas. Queda a cargo del oferente la correcta configuración de los equipos intermedios de comunicación (switches, routers, firewall, etc) para la migración y puesta en producción del nuevo clúster Huawei DCS con los equipos ofertados. Queda a cargo del oferente la correcta configuración de los switches SAN para la migración y puesta en producción del nuevo clúster Huawei DCS con los	CUMPLE

	equipos ofertados. 02 (dos) técnicos certificados en Storage Huawei de nivel profesional con certificado vigente y ID verificable los cuales serán los encargados de la creación de las LUNs necesarias para migrar y poner en producción las VM del nuevo entorno Huawei DCS. También estarán a cargo de configurar la funcionalidad Hypermetro (replica Activa-Activa entre Storage) que actualmente se encuentra en producción entre el datacenter de la DA y el datacenter de contingencia. 02 (dos) técnicos certificados VCS Veritas Backup Exec 20.1 Administrator con certificado vigente y verificable los cuales serán los encargados de migrar y poner en producción los backup de las VM del nuevo entorno Huawei DCS.	
Certificaciones técnicas.	El oferente deberá contar con al menos: 01 (uno) profesional con certificado vigente de PMP (Project Management Professional) certificado por el PMI (Project Manager Institute) o certificación vigente Scrum Master con reconocimiento internacional o certificaciones equivalentes, para la planificación, ejecución y control de los trabajos, Los cuales deberán ser verificable con la planilla de IPS y/o Estatuto de la empresa. 02 (dos) técnicos certificados por el fabricante de los equipos ofertados. La experiencia del personal en la solución ofertada deberá ser demostrable con la presentación del Certificado de Especialista emitido por el fabricante, demostrable con la planilla de IPS y/o Estatuto de la empresa. 02 (dos) técnicos certificados en el producto de virtualización de Huawei Virtualization Suite Platinum Edition, los cuales deben ser verificable la planilla de IPS y/o Estatuto de la empresa. 02 (dos) técnicos certificados en Storage Huawei de nivel profesional con certificado vigente y verificable. La experiencia del personal debe ser demostrable con la presentación del Certificado de Especialista en Storage Huawei, el personal propuesto deberá ser demostrable con la planilla de IPS y/o Estatuto de la empresa. 02 (dos) técnicos certificados en Veritas Backup Exec. la experiencia del personal deberá ser demostrable con la presentación del Certificado de Especialista en Veritas Backup, el personal propuesto deberá ser demostrable con la planilla de IPS y/o Estatuto de la empresa.	CUMPLE
Soporte	El Oferente deberá contemplar el soporte técnico por un periodo de 36 meses. Soporte on site 7 x 24 durante 3 (tres) años.	CUMPLE

Lote 1 - Item 1 - Servidor para clúster:

* La empresa SSD cumple con todos los requisitos técnicos solicitados.

LOTE 2: Sistema de Almacenamiento – Storage

Se procede a evaluar al único oferente, la empresa Datasystems.

Características	Mínimo exigido	CUMPLE / NO CUMPLE
Marca	HITACHI-VANTARA	CUMPLE
Modelo	VSP-E590	CUMPLE
Origen	JAPON	CUMPLE
Cantidad	1 (Uno)	CUMPLE
Factor de forma	Rackeable 19	CUMPLE
Protocolos Front- End Soportados por el equipo.	FC 16 Gbps. iSCSI 10 Gbps	CUMPLE
Detalles del sistema de almacenamiento	El sistema de almacenamiento debe incluir dos controladoras activas y redundantes entre sí. Cada controladora debe contar con cuatro puertos FC 16 Gbps para conectividad Front-End. Cada controladora debe contar con 384 GB de memoria caché como mínimo, totalizando 768GB. En caso de interrupción del fluido eléctrico, el equipo deberá contar con un mecanismo para mover la información de caché a disco con el fin de proteger la integridad de la información hasta que se re energice el equipo.	CUMPLE
Niveles de RAID	El sistema de almacenamiento debe incluir la capacidad de definir arreglos de discos de nivel RAID 1 o 10, 5 y 6 como mínimo.	CUMPLE
Capacidad entregada	Inicial: Al menos 40TB de capacidad útil con discos NVMe SSD configurados en RAID 6. Se deberá proveer al menos 1 disco para spare.	CUMPLE
Tipos de discos soportados.	NVMe SSD, SAS SSD y solo SAS HDD como opcional.	CUMPLE
Escalabilidad	El equipo debe tener la posibilidad de crecer hasta por lo menos 5PB RAW internamente.	CUMPLE
LUNs	Tamaño máximo de LUN: 256TB o superior. cantidad máxima de LUNs que permite realizar el Storage: 20.000 o superior.	CUMPLE
IOPS	El dispositivo de almacenamiento deberá soportar al menos 3.500.000 de IOPS.	CUMPLE
Software de Análisis y Reporte del desempeño.	El equipo ofertado deberá tener un software con la funcionalidad de enviar reportes ante cualquier eventualidad de fallo que fuera a tener el mismo. El equipo deberá estar configurado de modo a que el reporte generado sea enviado al proveedor y al fabricante al mismo tiempo de manera inmediata, para la posterior solución de la falla por parte del proveedor.	CUMPLE
Software de copia y replicación.	El sistema debe poder ser capaz de realizar copias de los volúmenes dentro del mismo sistema de almacenamiento (Snapshots y Clones). Dicha funcionalidad debe ser incluida en caso de ser una	CUMPLE

	licencia adicional. La licencia debe cubrir la capacidad total de crecimiento del dispositivo de almacenamiento	
Software de Aprovisionamiento	El sistema debe incluir el licenciamiento de software especializado que permita la provisión de capacidad física de almacenamiento en forma dinámica, la capacidad asignada no se deberá alojar en cuanto se cree el volumen, se deberá provisionar en cuanto la data sea efectivamente escrita en el volumen. (Thin- Provisioning).	CUMPLE
Disponibilidad de componentes	Las controladoras, discos, fuentes de poder y ventiladores deben ser hot-swap. Las controladoras, fuentes de poder y ventilación deben ser redundantes.	CUMPLE
Sistemas operativos de hosts compatibles	Microsoft Windows Server. Red Hat Enterprise Linux. Vmware. AIX. Huawei DCS.	CUMPLE
Técnicos y certificaciones	El oferente deberá contar con al menos 2(dos) técnicos certificados en la marca ofertada, los mismos deberán formar parte de la nómina permanente de funcionarios de la empresa inscriptos en IPS. Se deberá presentar última planilla vigente del Aporte Obrero Patronal IPS para garantizar que el personal propuesto pertenece a la nómina de funcionarios permanentes de la empresa. Además, será un requisito indispensable que la empresa oferente esté autorizada por el Fabricante a prestar el servicio técnico y el cambio de partes por garantía. Es también aceptable para la Convocante que el oferente esté debidamente autorizado y respaldado, por escrito, por la empresa prestadora de servicios y asistencia técnica de la marca ofertada en nuestro país (C.A.S.), quienes deberán contar con al menos 2 técnicos certificados. Se deberá presentar la nómina de técnicos certificados del CAS, con sus respectivas certificaciones.	CUMPLE
Experiencia	La empresa oferente deberá acreditar al menos 5 instalaciones de Storage o similares a la ofertada (atendiendo siempre que sea de la misma marca, aunque pueda variar los modelos) dentro del territorio nacional, avalados por la correspondiente factura emitida en su oportunidad y una carta de conformidad del cliente relacionado a la recepción del equipo instalado. Además, se debe presentar adjunto a cada factura, información del número telefónico de contacto y la convocante se reserva el derecho de realizar una visita al Cliente referenciado.	CUMPLE
Instalación	El dispositivo de almacenamiento deberá ser instalado en un Rack indicado por la convocante y se deberá prever los kits necesarios para el rackeo.	CUMPLE
Autorización del fabricante	El oferente deberá contar con Autorización del Representante Local de la marca en Paraguay, quien a su vez deberá estar avalado por el Fabricante.	CUMPLE
Garantía	3 (tres) años On Site. El servicio de garantía deberá ser realizado por técnicos certificados del CAS (Centro Autorizado de Servicios) avalado por el	CUMPLE

	Fabricante.	
Plazo de entrega	El equipo deberá ser entregado 60(sesenta) días posteriores a la recepción de la Orden de Compra correspondiente.	CUMPLE

Lote 2 - Item 1 - Sistema de Almacenamiento – Storage:
* La empresa Datasystems cumple con todos los requisitos técnicos establecidos para este lote.

Lote 3 Equipos de comunicación.

Se procede a evaluar las tres ofertas Technoma, Emotion y TEISA:

Ítem 1 - Firewall de Borde		
	Características	CUMPLE / NO CUMPLE
Cantidad	1 (Uno)	
Marca	FORTINET	
Modelo	FORTIGATE - 400F	
Origen/Procedencia	USA	
Componente	**Características**	
Características Equipo	Throughput de por lo menos 20 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6	CUMPLE
	Soporte a por lo menos 7.5M conexiones simultaneas	CUMPLE
	Soporte a por lo menos 450K nuevas conexiones por segundo	CUMPLE
	Throughput de al menos 50 Gbps de VPN IPSec	CUMPLE
	Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos	CUMPLE
	Estar licenciado para, o soportar sin necesidad de licencia, 15K túneles de clientes VPN IPSec simultáneos	CUMPLE
	Throughput de al menos 1 Gbps de VPN SSL	CUMPLE
	Soportar al menos 500 clientes de VPN SSL simultáneos	CUMPLE
	Soportar al menos 11 Gbps de throughput de IPS	CUMPLE
	Soportar al menos 1 Gbps de throughput de Inspección SSL	CUMPLE
	Soportar al menos 20 Gbps de throughput de Application Control	CUMPLE
	Soportar al menos 5 Gbps de throughput de NGFW	CUMPLE
	Soportar al menos 4 Gbps de throughput de Threat Protection	CUMPLE
	Permitir gestionar al menos 128 Access Points	CUMPLE
	Tener al menos 12 interfaces 1Gbps RJ45 y 4 interfaces SFP	CUMPLE

Características Generales	Tener al menos 2 interfaces 10Gbps	CUMPLE
	Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance	CUMPLE
	Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance	CUMPLE
	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.;	CUMPLE
	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	CUMPLE
	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;	CUMPLE
	La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;	CUMPLE
	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;	CUMPLE
	La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;	CUMPLE
	Los dispositivos de protección de red deben soportar 4000 VLANs Tags 802.1q;	CUMPLE
	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;	CUMPLE
	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;	CUMPLE
	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);	CUMPLE
	Los dispositivos de protección de red deben soportar DHCP Relay;	CUMPLE
	Los dispositivos de protección de red deben soportar DHCP Server;	CUMPLE
	Los dispositivos de protección de red deben soportar sFlow;	CUMPLE
	Los dispositivos de protección de red deben soportar Jumbo Frames;	CUMPLE
	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;	CUMPLE
	Debe ser compatible con NAT dinámica (varios-a-1);	CUMPLE
	Debe ser compatible con NAT dinámica (muchos-a-muchos);	CUMPLE
	Debe soportar NAT estática (1-a-1);	CUMPLE
	Debe admitir NAT estática (muchos-a-muchos);	CUMPLE

	Debe ser compatible con NAT estático bidireccional 1-a-1;	CUMPLE
	Debe ser compatible con la traducción de puertos (PAT);	CUMPLE
	Debe ser compatible con NAT Origen;	CUMPLE
	Debe ser compatible con NAT de destino;	CUMPLE
	Debe soportar NAT de origen y NAT de destino de forma simultánea;	CUMPLE
	Debe soportar NAT de origen y NAT de destino en la misma política	CUMPLE
	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;	CUMPLE
	Debe ser compatible con NAT64 y NAT46;	CUMPLE
	Debe implementar el protocolo ECMP;	CUMPLE
	Debe soportar SD-WAN de forma nativa	CUMPLE
	Debe soportar el balanceo de enlace hash por IP de origen;	CUMPLE
	Debe soportar el balanceo de enlace por hash de IP de origen y destino;	CUMPLE
	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;	CUMPLE
	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;	CUMPLE
	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;	CUMPLE
	Enviar logs a sistemas de gestión externos simultáneamente;	CUMPLE
	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;	CUMPLE
	Debe incluir el registro y análisis centralizado de basado en la nube.	CUMPLE
	De incluir el almacenamiento de registro y análisis centralizados basados en la nube como mínimo de 5Gb por día.	CUMPLE
	Debe soporta protección contra la suplantación de identidad (anti-spoofing);	CUMPLE
	Implementar la optimización del tráfico entre dos dispositivos;	CUMPLE
	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);	CUMPLE
	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);	CUMPLE
	Soportar OSPF graceful restart;	CUMPLE

	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;	CUMPLE
	Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;	CUMPLE
	Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;	CUMPLE
	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;	CUMPLE
	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;	CUMPLE
	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;	CUMPLE
	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster;	CUMPLE
	La configuración de alta disponibilidad debe sincronizar: Sesiones;	CUMPLE
	La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;	CUMPLE
	La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;	CUMPLE
	La configuración de alta disponibilidad debe sincronizar: Tablas FIB;	CUMPLE
	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;	CUMPLE
	Debe soportar la creación de sistemas virtuales en el mismo equipo;	CUMPLE
	Para una alta disponibilidad, el uso de clústeres virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	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);	CUMPLE
	Debe soportar una malla de seguridad para proporcionar una	CUMPLE

	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;	CUMPLE
	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;	CUMPLE
	La consola de administración debe soportar como mínimo, inglés, español y portugués.	CUMPLE
	La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad	CUMPLE
	La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.	CUMPLE
	Debe soportar controles de zona de seguridad;	CUMPLE
	Debe contar con políticas de control por puerto y protocolo;	CUMPLE
Control por Política de Firewall	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;	CUMPLE
	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;	CUMPLE
	Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;	CUMPLE
	Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;	CUMPLE
	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.	CUMPLE
	Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);	CUMPLE
	Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes	CUMPLE
	Debe soportar el protocolo estándar de la industria VXLAN;	CUMPLE
	La solución debe permitir la implementación sin asistencia de SD-WAN	CUMPLE
	En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;	CUMPLE

	la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.	CUMPLE
	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;	CUMPLE
Control de Aplicación	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;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de palead para permitir la identificación de firmas de la aplicación conocidas por el fabricante;	CUMPLE
	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;	CUMPLE
	Actualización de la base de firmas de la aplicación de forma automática;	CUMPLE
	Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;	CUMPLE
	Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;	CUMPLE
	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;	CUMPLE
	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;	CUMPLE
	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc.) permitiendo granularidad de control/reglas para el mismo;	CUMPLE
	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;	CUMPLE
	Debe permitir la diferenciación y manejo de las aplicaciones de	CUMPLE

	chat; por ejemplo, permitir a Hangouts el chat pero impedir la llamada de video;	
	Debe permitir la diferenciación de aplicaciones Proxis (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;	CUMPLE
	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);	CUMPLE
	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;	CUMPLE
	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;	CUMPLE
	Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente	CUMPLE
Prevención de Amenazas	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;	CUMPLE
	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);	CUMPLE
	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;	CUMPLE
	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;	CUMPLE
	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;	CUMPLE
	Deber permitir el bloqueo de vulnerabilidades y exploits conocidos	CUMPLE
	Debe incluir la protección contra ataques de denegación de servicio;	CUMPLE
	Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;	CUMPLE
	Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;	CUMPLE
	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;	CUMPLE
	Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;	CUMPLE
	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);	CUMPLE
	Debe ser inmune y capaz de prevenir los ataques básicos, tales como	CUMPLE

	inundaciones (flood) de SYN, ICMP , UDP, etc;	
	Detectar y bloquear los escaneos de puertos de origen;	CUMPLE
	Bloquear ataques realizados por gusanos (worms) conocidos;	CUMPLE
	Contar con firmas específicas para la mitigación de ataques DoS y DDoS;	CUMPLE
	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);	CUMPLE
	Debe poder crear firmas personalizadas en la interfaz gráfica del producto;	CUMPLE
	Identificar y bloquear la comunicación con redes de bots;	CUMPLE
	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;	CUMPLE
	Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;	CUMPLE
	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;	CUMPLE
	Los eventos deben identificar el país que origino la amenaza;	CUMPLE
	Debe incluir protección contra virus en contenido HTML y JavaScript, software espía (spyware) y gusanos (worms);	CUMPLE
	Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	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);	CUMPLE
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);	CUMPLE
	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	CUMPLE

	local, en modo de proxy transparente y explícito;	
	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;	CUMPLE
	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;	CUMPLE
	Tener por lo menos 75 categorías de URL;	CUMPLE
	Debe tener la funcionalidad de exclusión de URLs por categoría;	CUMPLE
	Permitir página de bloqueo personalizada;	CUMPLE
	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);	CUMPLE
	Además del Explicit Web Proxy, soportar proxy web transparente;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc.;	CUMPLE
Identificación de Usuarios	Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios;	CUMPLE
	Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios;	CUMPLE
	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);	CUMPLE
	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;	CUMPLE
	Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;	CUMPLE

	Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;	CUMPLE
	Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;	CUMPLE
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;	CUMPLE
	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;	CUMPLE
	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;	CUMPLE
	Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;	CUMPLE
	Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;	CUMPLE
	Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;	CUMPLE
	En QoS debe permitir la definición de tráfico con ancho de banda garantizado;	CUMPLE
	En QoS debe permitir la definición de tráfico con máximo ancho de banda;	CUMPLE
	En QoS debe permitir la definición de colas de prioridad;	CUMPLE
	Soportar marcación de paquetes DiffServ, incluso por aplicación;	CUMPLE
	Soportar la modificación de los valores de DSCP para Diffserv;	CUMPLE
	Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);	CUMPLE
	Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;	CUMPLE
	Permite la creación de filtros para archivos y datos predefinidos;	CUMPLE
Filtro de Datos	Los archivos deben ser identificados por tamaño y tipo;	CUMPLE
	Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;	CUMPLE
	Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;	CUMPLE
	Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;	CUMPLE

	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;	CUMPLE
Geo Localización	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;	CUMPLE
	Debe permitir la visualización de los países de origen y destino en los registros de acceso;	CUMPLE
	Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;	CUMPLE
VPN	Soporte VPN de sitio-a-sitio y cliente-a-sitio;	CUMPLE
	Soportar VPN IPSec;	CUMPLE
	Soportar VPN SSL;	CUMPLE
	La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512	CUMPLE
	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;	CUMPLE
	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);	CUMPLE
	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);	CUMPLE
	Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;	CUMPLE
	Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;	CUMPLE
	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;	CUMPLE
	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;	CUMPLE
	Deberá mantener una conexión segura con el portal durante la sesión;	CUMPLE
	El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible	CUMPLE

	con al menos Windows y Mac OS.	
	Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);	CUMPLE
	Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;	CUMPLE
	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;	CUMPLE
	La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;	CUMPLE
	El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;	CUMPLE
Wireless Controller	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;	CUMPLE
	Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points;	CUMPLE
	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;	CUMPLE
	Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	La solución debe permitir definir qué redes serán tuneladas hasta la controladora y qué redes serán conmutadas directamente por la	CUMPLE

	interfaz del punto de acceso;	
	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;	CUMPLE
	La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE

	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;	CUMPLE
	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; Debe permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;	CUMPLE CUMPLE
	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;	CUMPLE
	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; La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectada mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos; La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica;	CUMPLE CUMPLE CUMPLE
	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;	CUMPLE
	La solución debe implementar técnicas de Call Admission Control para limitar el número de llamadas simultáneas; La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica e informar 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; 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; La solución debe permitir la configuración de los data rates que se activarán en la herramienta y las que se deshabilitar para las frecuencias de 2.4 y 5GHz y los estándares 802.11a / b / g / n / ac;	CUMPLE CUMPLE CUMPLE CUMPLE
	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	CUMPLE

	el consumo de Airtime;	
	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;	CUMPLE
	La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz;	CUMPLE
	La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;	CUMPLE
	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;	CUMPLE
	La solución debe implementar la función de web filtering para controlar los sitios que se accede a la red inalámbrica. 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;	CUMPLE
	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;	CUMPLE
	La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil y quinientas) aplicaciones;	CUMPLE
	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;	CUMPLE
	La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;	CUMPLE
	La solución debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica. Al menos los siguientes ataques deben ser identificados: - 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.	CUMPLE
	La solución debe implementar mecanismos de protección para	CUMPLE

	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	
	La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;	CUMPLE
	La solución debe monitorear y clasificar el riesgo de las aplicaciones accesadas por los clientes inalámbricos;	CUMPLE
	Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;	CUMPLE
	Debe implementar la autenticación administrativa a través del protocolo RADIUS;	CUMPLE
	En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);	CUMPLE
	En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;	CUMPLE
	La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	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;	CUMPLE
	La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;	CUMPLE
	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;	CUMPLE
	La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico;	CUMPLE
	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;	CUMPLE
	La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;	CUMPLE
	La solución debe permitir que la página de autenticación se quede	CUMPLE

	alojada en un servidor externo;	
	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;	CUMPLE
	La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6;	CUMPLE
	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;	CUMPLE
	Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;	CUMPLE
	La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;	CUMPLE
	La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;	CUMPLE
	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;	CUMPLE
	La solución debe permitir la configuración de redes Mesh entre los puntos de acceso administrados por ella;	CUMPLE
	La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;	CUMPLE
	La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;	CUMPLE
	La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;	CUMPLE
	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;	CUMPLE
	La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;	CUMPLE
	La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);	CUMPLE
	La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato .pcap;	CUMPLE
	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;	CUMPLE
	La solución debe presentar gráficamente la topología lógica de la	CUMPLE

	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;	
	La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;	CUMPLE
	La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;	CUMPLE
	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;	CUMPLE
	La solución debe tener herramientas de diagnóstico y depuración;	CUMPLE
	La solución debe soportar la comunicación con elementos externos a través de las API;	CUMPLE
	La solución deberá ser compatible y administrar los puntos de acceso de este proceso;	CUMPLE
Servicios y garantía	El equipo debe contar con soporte, servicios y garantía del fabricante por 36 meses	CUMPLE
	Las capacidades UTM deben estar presentes en los equipos y será decisión del contratante su adquisición	CUMPLE
Plazo de entrega	El equipo deberá ser entregado 60(sesenta) días posteriores a la recepción de la Orden de Compra correspondiente.	CUMPLE

Ítem 2 - Punto de Acceso - WIFI		
Componente	**Características**	**Requerido**
Cantidad	30 (treinta)	
Marca	FORTINET	
Modelo	FORTIAP- FAP-231G	
Origen/Procedencia	USA	
Características Equipo	Debe ser del tipo Indoor	CUMPLE
	Soportar 3 radios wireless + 1 radio BLE	CUMPLE
	Deberá soportar fuente de alimentación AC	CUMPLE
	Soportar 512 usuarios totales conectados	CUMPLE
	Implementar las tecnologías 802.11 a/b/g/n/ac/ax	CUMPLE
	Operar en las frecuencias de 2.4 / 5 GHz	CUMPLE
	Deberá operar en las bandas 2.4002.4835, 5.1505.250, 5.2505.350, 5.4705.725,5.7255.850	CUMPLE
	Implementar UL MU-MIMO 802.11ax mode y DL-MU-MIMO	CUMPLE
	Implementar 802.11ax	CUMPLE
	Soportar al menos 16 SSID simultáneos	CUMPLE
	La radio 1 debe operar en 2.4 GHz 20/40 MHz (1024 QAM)	CUMPLE
	La radio 2 debe operar en 5.0 GHz 20/40/80 MHz (1024 QAM)	CUMPLE
	La radio 3 debe operar en 2.4GHz, 5.0GHz, 6GHz 20/40/80/160MHz (1024 QAM)	CUMPLE
	La radio 1 debe soportar velocidad de datos de al menos 570 Mbps	CUMPLE
	La radio 2 debe soportar velocidad de datos de al menos 1200 Mbps	CUMPLE
	La radio 3 debe soportar velocidad de datos de al menos 2400 Mbps	CUMPLE
	Deberá soportar un MTBF superior a 20000 horas	CUMPLE
	El AP deberá contar con al menos una interfaz 10/100/1000 Base-T RJ45 y una interfaz 100/1000/2500 Base-T RJ45 las cuales deben soportar alimentación via PoE 802.3at	CUMPLE
	Deberá operar en temperaturas entre 00 y 45 grados celsius y humedad entre 5 y 90% non-condensing	CUMPLE
	Deberá soportar EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST	CUMPLE

	Deberá soportar WPA™, WPA2™, and WPA3™ with 802.1x or preshared key, WEP, Web Captive Portal, MAC blocklist & allowlist	CUMPLE
	Deberá soportar los estandares IEEE 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az	CUMPLE
	Deberá soportar los modos Local-Bridge, Tunnel, Mesh	CUMPLE
Funcionalidades Generales	Punto de acceso (AP) que permita el acceso de los dispositivos a la red a través de la wireless y que posea todas sus configuraciones centralizadas en controlador inalámbrico;	CUMPLE
	Debe soportar el modo de operación centralizado, o sea, su operación depende del controlador inalámbrico que es responsable de gestionar las políticas de seguridad, calidad de servicio (QoS) y monitoreo de la radiofrecuencia;	CUMPLE
	Debe identificar automáticamente el controlador inalámbrico al que se conectará;	CUMPLE
	Debe permitir administrarse remotamente a través de links WAN;	CUMPLE
	Debe poseer capacidad dual-band con radios 2.4GHz, 5GHz y 6 GHz operando simultáneamente, además de permitir configuraciones independientes para cada radio;	CUMPLE
	El 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 encapsulados hasta el controlador inalámbrico;	CUMPLE
	Cuando sea encapsulado, el tráfico debe ser encriptado a través de DTLS o IPSEC;	CUMPLE
	Debe permitir el tráfico de los dispositivos conectados a la red inalámbrica de forma distribuida (local switching), o sea, el tráfico debe ser conmutado localmente en la interfaz LAN del punto de acceso y no necesitará ser encapsulado hasta el controlador inalámbrico;	CUMPLE
	Cuando el tráfico sea distribuido y la autenticación con 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;	CUMPLE
	En conjunto con el controlador inalámbrico, debe optimizar el rendimiento y la cobertura inalámbrica (RF), realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados;	CUMPLE
	Deberá soportar la funcionalidad de ajuste automático de potencia para extender la cobertura en caso de falla del punto de acceso vecino gerenciado por la misma controladora;	CUMPLE
	Debe soportar mecanismos para la detección y mitigación de	CUMPLE

	puntos de acceso no autorizados, también conocidos como Rogue APs;	
	En conjunto con el controlador inalámbrico, debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica (wIDS / wIPS);	CUMPLE
	En conjunto con el controlador inalámbrico, debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red;	CUMPLE
	En conjunto con el controlador inalámbrico, debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios en función de los atributos proporcionados por los servidores RADIUS;	CUMPLE
	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;	CUMPLE
	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 el roaming;	CUMPLE
	Debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectadas mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;	CUMPLE
	Debe implementar el estándar IEEE 802.11e;	CUMPLE
	Debe implementar el estándar IEEE 802.11h;	CUMPLE
	El punto de acceso deberá soportar agregación de paquetes A-MPDU y A-MSDU;	CUMPLE
	El punto de acceso deberá soportar (LPDC) - Low Density Parity Check;	CUMPLE
	El punto de Acceso deberá soportar (MLD) - Maximum Likelihood Demodulation;	CUMPLE
	El Punto de Acceso deberá soportar metodo de diversidad (MRC) Maximum Ratio Combining;	CUMPLE
	Debe tener indicadores luminosos (LED) para indicación de estado;	CUMPLE
	Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;	CUMPLE
	Debe poseer un certificado emitido por la Wi-Fi Alliance;	CUMPLE
Capacidad Técnica del oferente	El oferente deberá contar con herramientas de hardware y Software dedicadas para el diseño e implementación de la red Wireless. Se aceptarán las herramientas conocidas en la industria Wireless tales como; AirCheck G2 y/o Ekahau Survey y/o AirMagnet Survey PRO y/o Hamina Wireless Planner Network y/o otros de igual	CUMPLE

	características. Además se deberá presentar 1 (un) técnico con certificación vigente en la herramienta del tipo Diseñador de Red inalámbrica con capacidades de optimizar y solucionar problemas de WI-FI tipo Enterprise y/o Profesional.	
	La herramienta deberá poder generar la documentación correspondiente al diseño predictivo (Antes de la implementación) y Survey activo del sitio posterior a la implementación de la red Wireless, esto abrirá el camino al proceso de implementación real, donde el oferente deberá incluir información real medida del sitio a fin de ajustar la configuración para prevenir posibles interferencias tanto adyacentes de propios APs como externos	CUMPLE
	El Hardware de medición debe incorporar arreglos de antenas en 2,4/5/6 GHz como también un analizador de espectro en dichas frecuencias	CUMPLE
	Contar con 1 (un) Técnico Certificado del tipo Enterprise Wireless Implementación o certificado de tipo profesional enfocado en implementaciones Wireless, para Implementar, proteger y configurar una infraestructura de red inalámbrica personalizada.	CUMPLE
garantía	36 meses	CUMPLE
Plazo de entrega	El equipo deberá ser entregado 60(sesenta) días posteriores a la recepción de la Orden de Compra correspondiente.	CUMPLE

Ítem 3 Clientes VPN y solución de Seguridad para estaciones de trabajo		
Componente	**Características**	**Requerido**
Cantidad	**500 (quinientas) estaciones de trabajo**	
Marca	FORTINET	
Modelo	FORTICLIENT SERIES	
Origen/Procedencia	USA	
Funcionalidades generales	Debe permitir gestión centralizada de endpoint	CUMPLE
	Debe permitir la gestión del cliente de seguridad de endpoint desde una consola central del fabricante	CUMPLE
	Debe permitir la configuración de perfiles en función de estados asignados por el servidor DHCP presente en el firewall de administración centralizada del mismo fabricante;	CUMPLE
	El licenciamiento debe estar basado en la cantidad de clientes registrados en la consola de gestión central del mismo fabricante	CUMPLE
	Debe ser compatible con los siguientes sistemas operativos: Microsoft Windows: 7 (32 y 64 bits), 8 (32 y 64 bits), 8.1 (32 y 64 bits), 10 (32 e 64 bits), 11(64 bits); Microsoft Windows Server: 2012 y superior; Mac OS: 10.14, 10.15 y 11+, IOS 9 o superior, Android 5 o superior, Linux Ubuntu 16.04 y superior, Red Hat 7.4 y superior, CentOS 7.4 y superior.	CUMPLE
	Debe tener interfaz gráfica de usuario al menos en el idioma	CUMPLE

	inglés, portugués y español;	
	Debe permitir la copia de seguridad del archivo de configuración del endpoint	CUMPLE
	El cliente de seguridad debe poder generar bitácora (logs) sobre las funcionalidades instaladas y configuradas	CUMPLE
	Por lo menos los siguientes niveles de log deben estar disponibles: emergencia, alerta, crítico, error, aviso, informativo;	CUMPLE
	El cliente de seguridad debe poder enviar los registros (logs) a la consola de gestión central	CUMPLE
	El cliente se seguridad debe permitir la configuración local via XML (eXtensible Markup Language);	CUMPLE
Funcionalidades de Provisionamiento de Clientes	El cliente se seguridad debe poder se integrado con tecnologías de Sandboxing del mismo fabricante; la solución debe incluir la opción de suscripción de Sandbox sCloud	CUMPLE
	El fabricante debe proveer un portal para descargar el cliente seguridad y permitir la instalación local	CUMPLE
	Debe ser compatible con la instalación vía Active Directory de Microsoft	CUMPLE
	La consola de gestión central debe ser capaz de instalar el cliente de seguridad en computadoras Windows asociadas a un dominio Microsoft	CUMPLE
	El cliente de seguridad debe ser capaz de inspeccionar archivos ejecutables, librerías y drivers en busca de virus	CUMPLE
Funcionalidades de Antivirus	El cliente de seguridad debe ser capaz de buscar actualizaciones de firmas automáticamente	CUMPLE
	El cliente de seguridad debe ser capaz de enviar archivos para ser inspeccionados en sistemas de Sandboxing del mismo fabricante	CUMPLE
	El cliente de seguridad debe bloquear canales de comunicación usados por hackers o atacantes	CUMPLE
	El cliente de seguridad debe notificar localmente cuando se detecta un virus	CUMPLE
	El cliente de seguridad debe permitir que el usuario comience un escaneo bajo demanda	CUMPLE
	El cliente de seguridad debe permitir que se comience escaneo de virus de forma automática regularmente	CUMPLE
	El cliente de seguridad debe permitir visualizar los archivos puestos en cuarentena	CUMPLE
	Debe permitir la configuración del perfil antivirus desde la consola central del mismo fabricante	CUMPLE
	Debe permitir la configuración del perfil de filtro de web desde	CUMPLE

	la consola central del mismo fabricante	
	El fabricante debe disponibilizar consultas en línea desde el cliente de seguridad sobre la categoría de determinada web (por ej. Interés general, tecnología, hacking, pornografía, etc.) para aplicar política de control de acceso a internet	CUMPLE
Funcionalidades de Firewall de Aplicación	El cliente de seguridad debe admitir reglas estáticas de acceso a internet basado en expresiones regulares	CUMPLE
	Para una URL determinadas las acciones deben ser: permitir, bloquear, alertar o monitorear	CUMPLE
	El cliente de seguridad debe admitir perfiles de Control de Aplicaciones creados centralmente desde la consola de gestión del mismo fabricante	CUMPLE
	El fabricante debe disponibilizar consultas en línea desde el cliente de seguridad sobre la categoría de determinada aplicación a modo de ser usada en la política de control de acceso	CUMPLE
	Debe ser reconocido más de 2800 aplicaciones por el cliente para ser usadas en reglas de control de acceso	CUMPLE
Funcionalidades de VPN SSL	Debe permitir que el usuario cree nuevas VPN SSL	CUMPLE
	Debe permitir que existan varias VPN SSL definidas simultáneamente	CUMPLE
	Debe permitir la personalización del puerto TCP en el que funciona la VPN SSL	CUMPLE
	Debe permitir la autenticación usando usuario y clave	CUMPLE
	Debe permitir la autenticación de dos factores provisto por el mismo fabricante	CUMPLE
	Debe permitir la autenticación usando certificados digitales	CUMPLE
Funcionalidades de VPN IPSec	Debe permitir que el usuario cree nuevas VPN IPSEC	CUMPLE
	Debe permitir que existan varias VPN IPSEC definidas simultáneamente	CUMPLE
	Debe permitir la autenticación usando usuario y clave	CUMPLE
	Debe permitir la autenticación usando certificados digitales	CUMPLE
	Debe permitir la selección de Modo Main y Agressive;	CUMPLE
	Debe permitir la configuración de DHCP sobre IPSec;	CUMPLE
	Debe permitir el uso de NAT Traversal;	CUMPLE
	Debe permitir la elección de grupos Diffie-Hellman (1,2,5 e 14);	CUMPLE
	Debe permitir la configuración de expiración de claves IKE;	CUMPLE
	Debe permitir el uso de Perfect Forward Secrecy;	CUMPLE

Funcionalidades de la Solucion	Debe permitir la autenticación de dos factores provisto por el mismo fabricante	CUMPLE
	Debe gestionar de manera transparente para el usuario la selección del Gateway.	CUMPLE
	Debe gestionar la salud del Endpoint, la telemetría, la identidad del usuario y los certificados.	CUMPLE
	Debe continuamente chequear la postura de seguridad del endpoint.	CUMPLE
	Debe funcionar en modo Proxy para conexiones HTTPS y/o modo transparente TCP	CUMPLE
	Debe soportar integración con Multi Factor de Autenticacion	CUMPLE
	Debe brindar funcionalidades de (CASB) Cloud Access Security Broker en línea.	CUMPLE
Funcionalidades de Scanner de Vulnerabilidades	El cliente de seguridad debe tener integrado un módulo de búsqueda de vulnerabilidades y permitir la gestión central desde la consola del mismo fabricante	CUMPLE
	Debe permitir que el usuario comience un análisis de vulnerabilidades bajo demanda	CUMPLE
	Las vulnerabilidades encontradas deben ser mostradas localmente con un vínculo para visualizar información desde una base de datos en internet. Debe tener al menos: nombre, severidad y detalles	CUMPLE
	Debe permitir la instalación sobre Microsoft Windows Server 2012 o superior y/o Sistema Operativo Linux.	CUMPLE
	Debe permitir adicionar clientes mediante la adición de licencias	CUMPLE
	Debe tener interfaz de gestión gráfica	CUMPLE
Funcionalidades de Gestión	Debe tener la funcionalidad de backup	CUMPLE
	Debe permitir la creación de usuarios de diferente perfil administrativo	CUMPLE
	Debe permitir importar información desde Active Directory mediante LDAP	CUMPLE
	El registro manual de estaciones debe permitir el uso de clave	CUMPLE
	Debe permitir la creación de grupos de clientes para facilitar la gestión	CUMPLE
	Debe permitir la configuración de clientes medinate definición XML	CUMPLE
	Debe permitir la importación de configuración de perfiles desde firewall de mismo fabricante	CUMPLE
	Debe permitir configuración de diferentes grupos y perfiles para facilitar la administración	CUMPLE

	Debe permitir la configuración de perfiles de antivirus, webfilter, control de aplicaciones, scanner de vulnerabilidades y VPN	CUMPLE
	Debe permitir habilitar la protección en tiempo real	CUMPLE
	Debe permitir configurar la busqueda de virus y vulnerabilidades de forma programada	CUMPLE
	Debe permitir ejecutar escaneo total y escaneo rapido	CUMPLE
	Debe permitir configurar filtro de URLs provisto por el fabricante con al menos las siguientes acciones: bloquear, advertir, permitir y monitorar;	CUMPLE
	Debe permitir configurar filtro de URLs basado en wildcards o expresiones regulares con las siguientes acciones: bloquear ou permitir;	CUMPLE
	Debe permitir al usuario configurar VPNs localmente	CUMPLE
	Debe permitir al usuario desconectar una VPN	CUMPLE
	Debe permitir la conexión de VPN antes de login	CUMPLE
	Debe permitir conexión automática de VPN	CUMPLE
	Específico y general para VPN IPSec (al menos):	CUMPLE
	Uso de certificados o usario y clave para autenticación	CUMPLE
	Uso de certificados en smartcard	CUMPLE
	Verificación de checksum	CUMPLE
	Bloqueo de tráfico IPv6	CUMPLE
	Específico a SSL VPN (al menos):	CUMPLE
	Especificación de la IP del concentrador	CUMPLE
	Especificación del puerto del concentrador	CUMPLE
	Opción para que el usuario pueda acceder a la configuración del cliente mediante contraseña	CUMPLE
	Envio de logs hacia sistemas de logs externos del mismo fabricante	CUMPLE
	Registro junto al sistema de gerencia de forma silenciosa (de forma que sea no perceptible para el usuário);	CUMPLE
	Instalación de certificado digital en el cliente	CUMPLE
	Debe permitir habilitar funcionalidades de Single Sign On	CUMPLE
	El sistema de gestión central debe tener disponible información sobre: Cantidad de dispositivos gestionados, Versión de Sistema Operativo, Perfil aplicado, Usuario, Versión de firmas de Antivirus	CUMPLE
	Estado del cliente de seguridad: Registrado o no registrado	CUMPLE

	Información sobre el sistema operativo en el que está instalado el cliente	CUMPLE
	Perfil de seguridad creados y/o aplicados	CUMPLE
	Funcionalidades de seguridad aplicadas: antivirus, filtro web, VPN, firewall de aplicaciones;	CUMPLE
garantía	36 meses	CUMPLE
Plazo de entrega	La herramienta deberá ser entregado 60(sesenta) días posteriores a la recepción de la Orden de Compra correspondiente.	CUMPLE

Ítem 4 -Analizador de tráfico y seguridad		
Componente	**Características**	**Requerido**
Cantidad	1 (Uno)	
Marca	FORTINET	
Modelo	FORTIANALYZER	
Origen/Procedencia	USA	
Características del equipo	La solución debe ser del tipo Virtual Appliance para implementarse on premise.	CUMPLE
	La solución no debe tener restricciones en la capacidad de almacenamiento en disco.	CUMPLE
	Debe recibir y procesar logs de todos los SDWAN y Next Generation Firewall solicitados en el presente pliego.	CUMPLE
Licenciamiento	La solución debe presentar un esquema de licenciamiento por suscripción.	CUMPLE
	Se debe licenciar la cantidad de GB por día de logs que puede recibir la solución.	CUMPLE
	La solución debe tener capacidad de recibir y procesar al menos 10 GB de logs diarios.	CUMPLE
	La suscripción debe incluir análisis de Indicadores de Compromisos, con inteligencia provista y actualizada periódicamente por el fabricante.	CUMPLE
	La suscripción debe incluir un dashboard de SoC donde se permitan realizar tareas automatizadas a partir de diversos inputs preconfigurados.	CUMPLE
Requerimientos funcionales	La solución debe permitir la virtualización en los siguientes hipervisores: VMware ESX/ESXi 5.5/6.0/6.5/6.7/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+ y KVM sobre Redhat 6.5+.	CUMPLE
	La solución no debe tener limitaciones en cuanto a la asignación de	CUMPLE

	vCPU.	
	La solución no debe tener limitaciones en cuanto a la asignación de memoria.	CUMPLE
	Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución.	CUMPLE
	Contar con comunicación cifrada y autenticación con usuario y contraseña para su administración, tanto en interface gráfica (GUI) como vía línea de comandos.	CUMPLE
	Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.	CUMPLE
	Soporte SNMP versión 2 y 3.	CUMPLE
	Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH.	CUMPLE
	Debe permitir la autenticación de usuarios de acceso a la plataforma vía LDAP.	CUMPLE
	Debe permitir la autenticación de usuarios de acceso a la plataforma vía Radius.	CUMPLE
	Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos.	CUMPLE
	Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.	CUMPLE
	Generación de informes en tiempo real de tráfico, en formato de gráfica de tabla	CUMPLE
	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.	CUMPLE
	Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.	CUMPLE
	Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado.	CUMPLE
	Contar con mecanismos de borrado automático de logs antiguos.	CUMPLE
	Permitir la importación y exportación de reportes.	CUMPLE
	Debe contar con la capacidad de crear informes en formato HTML/PDF/XML/CSV.	CUMPLE
	Debe permitir exportar los logs en formato CSV.	CUMPLE
	Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.	CUMPLE
	Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución	CUMPLE

	debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.	
	La solución debe contar con reportes predefinidos.	CUMPLE
	Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución.	CUMPLE
	Debe ser posible la duplicación de reportes existentes para su posterior edición.	CUMPLE
	Debe tener la capacidad de personalizar la portada de los reportes obtenidos.	CUMPLE
	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.	CUMPLE
	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.	CUMPLE
	Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas.	CUMPLE
	Debe poseer mecanismo de Drill-Down para navegar en los reportes de tiempo real.	CUMPLE
	Tener la capacidad de generar y enviar reportes periódicos automáticamente.	CUMPLE
	Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.	CUMPLE
	Permitir el envío por email de manera automática de reportes.	CUMPLE
	Debe permitir que el reporte a enviar por email sea al destinatario específico.	CUMPLE
	Permitir la programación de reportes, conforme a un calendario definido por el administrador.	CUMPLE
	Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.	CUMPLE
	Debe permitir el uso de filtros en los reportes.	CUMPLE
	Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.	CUMPLE
	Permitir especificar el idioma de los reportes creados.	CUMPLE
	Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.	CUMPLE
	Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.	CUMPLE
	Debe ser capaz de crear consultas SQL o similar dentro de las	CUMPLE

	bases de datos de logs, para uso en gráficas y tablas en reportes.	
	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.	CUMPLE
	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.	CUMPLE
	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.	CUMPLE
	Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.	CUMPLE
	Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.	CUMPLE
	Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.	CUMPLE
	Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos	CUMPLE
	Debe permitir visualizar en tiempo real los logs recibidos.	CUMPLE
	Debe permitir el reenvío de logs en formato syslog.	CUMPLE
	Debe permitir el reenvío de logs en formato CEF (Common Event Format).	CUMPLE
	Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para la red.	CUMPLE
	Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en la red.	CUMPLE
	Debe incluir dashboard para operaciones SOC que monitorea el tráfico en la red.	CUMPLE
	Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en la red.	CUMPLE
	Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en la red (sandboxing).	CUMPLE
	Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en la red.	CUMPLE
	Debe incluir dashboard para operaciones SOC que monitorea actividad VPN en la red.	CUMPLE
	Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs	CUMPLE
	Debe incluir dashboard para operaciones SOC que monitorea	CUMPLE

	rendimiento de recursos local de la solución (CPU, Memoria).	
	Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC.	CUMPLE
	Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3.	CUMPLE
	Debe permitir generar alertas de eventos a partir de logs recibidos.	CUMPLE
	Debe permitir crear incidentes a partir de alertas de eventos para endpoint.	CUMPLE
	Debe permitir la integración al sistema de tickets ServiceNow.	CUMPLE
	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.	CUMPLE
	Debe soportar el estándar SAML para autenticación de usuarios administradores.	CUMPLE
	Reportes de Firewall	CUMPLE
	Debe contar con reporte de cumplimiento de PCI DSS	CUMPLE
	Debe contar con reporte de utilización de aplicaciones SaaS	CUMPLE
	Debe contar con reporte de prevención de perdida de datos (DLP)	CUMPLE
	Debe contar con reporte de VPN	CUMPLE
	Debe contar con reporte de Sistema de prevención de intrusos (IPS)	CUMPLE
	Debe contar con reporte de reputación de cliente	CUMPLE
	Debe contar con reporte de análisis de seguridad de usuario	CUMPLE
	Debe contar con reporte de análisis de amenaza cibernética	CUMPLE
	Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad	CUMPLE
	Debe contar con reporte de tráfico DNS	CUMPLE
	Debe contar con reporte tráfico de correo electrónico	CUMPLE
	Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red	CUMPLE
	Debe contar con reporte de Top 10 de Websites utilizadas en la red	CUMPLE
	Debe contar con reporte de uso de redes sociales	CUMPLE
Garantía	36 meses	CUMPLE
Plazo de entrega	La herramienta deberá ser entregado 60(sesenta) días posteriores a la recepción de la Orden de Compra correspondiente.	CUMPLE

Capacidad Técnica para el Lote 3

Los mantenimientos deberán ser brindados por personal certificado especializado de los equipos involucrados en esta contratación. El Oferente adjudicado deberá presentar los avales correspondientes, que indiquen que los mismos se encuentran en condiciones de llevar a cabo dichos servicios.

- El oferente deberá presentar certificación de 1 (Un) Técnico nivel Asociado o similar de la marca ofertada.
- El oferente deberá presentar certificación de 01 (Un) Técnico nivel Profesional o similar de la marca ofertada.
- El oferente deberá presentar certificación de 01 (Un) Técnico nivel Especialista o similar de la marca ofertada.
- El oferente deberá presentar certificación de 01 (Un) profesional con certificación internacional con más de 7 años de vigencia en el nivel experto en redes informáticas radicado en el país.
- El oferente deberá presentar certificación de 01 (Un) técnico certificado a nivel profesional en Gestión de Proyectos (ITIL v4) o SCRUM Master o PMP que interactuará y dará soporte al personal asignado al proyecto.
- Los técnicos deberán ser staff permanente de la empresa y estar en la planilla de IPS y/o Estatuto de la empresa. Comprobada con constancia emitida por el IPS (Instituto de Previsión Social) y/o Estatuto de la empresa.
- El Oferente debe demostrar experiencia en la provisión e instalación de Routers/Firewalls durante el periodo 2020 2023 demostrado de la siguiente manera: Copias de Facturaciones y/o contratos de haber proveído a Entidades Públicas y/o Privadas por lo menos el 50% (cincuenta por ciento) del monto de la oferta presentada.

Autorización del fabricante para el Lote 3

Autorización del fabricante, con ID del llamado, se verificará al momento de la apertura de ofertas.

Lote 3 - Equipos de comunicación: todos los oferentes cumplen con las especificaciones técnicas de los equipos a ser proveídos, en los 4 ítems.
* Item 1 - Firewall de Borde.
* Item 2 - Punto de Acceso – WIFI.
* Item 3 - Cliente VPN y solución de seguridad para estaciones de trabajo.
* Item 4 - Analizador de tráfico y Seguridad.
Pero en el análisis de la documentación de la capacidad técnica de las empresas, se encontraron estas falencias:
* Technoma: No cumple con el requisito de presentar la certificación de un profesional experto en redes informáticas con al menos 7 años de experiencia.
* Emotion: No cumple con la certificación ISO 9001:2015 requerida para garantizar la calidad de los servicios.
* Teisa: No cumple con el requisito de presentar la certificación de un profesional experto en redes informáticas con al menos 7 años de experiencia. El oferente presenta certificado de nivel Especialista, no de Experto como se solicita. https://www.juniper.net/us/en/training/certification.html
De igual manera en la verificación de los precios unitarios de cada ítem, se puede verificar que:
* Technoma: Corresponde a la primera oferta y que el precio unitario del ítem 1 y el item 3 exceden significativamente el precio referencial.
* Teisa: Corresponde a la tercera oferta y que el precio unitario del ítem 3 excede significativamente el precio referencial.

* Conclusión: Dada la no conformidad de todas las empresas, con los requisitos técnicos y precios establecidos, se recomienda declarar desierto el Lote 3.

LOTE 4: Módulos SFP

Se procede a evaluar la menor oferta, la empresa Technoma.

Ítem 1 - Módulo SFP para fibra óptica Mono Modo (SMF)		
Características	Características	CUMPLE / NO CUMPLE
Cantidad	10 (Diez)	CUMPLE
Marca	FS	CUMPLE
Modelo	SFP-10G-LR-COMPATIBLE	CUMPLE
Origen	USA	CUMPLE
Velocidad de datos	10Gbps	CUMPLE
Longitud de onda	1310nm	CUMPLE
Conector	LC Dúplex	CUMPLE
Distancia de Cable	10 Km	CUMPLE
Factor de forma	Small Form-Factor Pluggable (SFP)	CUMPLE
Plataformas compatibles	Cisco ASR 1000 Series Router, Cisco Catalyst 3850 Series Switches, Cisco Catalyst 4500 and 4500-X Series Switches, Cisco Catalyst 2960-X Series Switches	CUMPLE
Garantía	12 meses	CUMPLE
Plazo de entrega	Deberá ser entregado 30(treinta) días posteriores a la recepción de la Orden de Compra correspondiente.	CUMPLE

Ítem 2 - Módulo SFP para fibra óptica Multi Modo (MMF)		
Características	Características	CUMPLE / NO CUMPLE
Cantidad	8 (Ocho)	CUMPLE
Marca	FS	CUMPLE
Modelo	SFP-10G-SR-COMPATIBLE	CUMPLE
Origen/Procedencia	USA	CUMPLE
Velocidad de datos	10Gbps	CUMPLE
Longitud de onda	850nm	CUMPLE
Conector	LC Duplex	CUMPLE
Distancia de cable	300m	CUMPLE
Factor de forma	Small Form-Factor Pluggable (SFP)	CUMPLE
Plataformas compatibles	Cisco ASR 1000 Series Router, Cisco Catalyst 3850 Series Switches, Cisco Catalyst 4500 and 4500-X Series Switches, Cisco Catalyst 2960-X Series Switches	CUMPLE
Garantía	12 meses	CUMPLE
Plazo de entrega	Deberá ser entregado 30(treinta) días posteriores a la recepción de la Orden de Compra correspondiente.	CUMPLE

Ítem 3 - Módulo SFP para fibra óptica Multi Modo (MMF)		
Características	Características	CUMPLE / NO CUMPLE
Cantidad	6 (Seis)	CUMPLE
Marca	FS	CUMPLE
Modelo	GLC-SX-MMD-COMPATIBLE	CUMPLE
Origen/Procedencia	USA	CUMPLE
Velocidad de datos	1Gbps	CUMPLE
Longitud de onda	850nm	CUMPLE
Conector	LC Duplex	CUMPLE
Distancia de cable	300m	CUMPLE
Factor de forma	Small Form-Factor Pluggable (SFP)	CUMPLE
Plataformas compatibles	Cisco ASR 1000 Series Router, Cisco Catalyst 3850 Series Switches, Cisco Catalyst 4500 and 4500-X Series Switches, Cisco Catalyst 2960-X Series Switches	CUMPLE
Garantía	12 meses	CUMPLE
Plazo de entrega	Deberá ser entregado 30(treinta) días posteriores a la recepción de la Orden de Compra correspondiente.	CUMPLE

Lote 4 - Módulos SFP:
* Item 1, Módulo SFP para fibra óptica Mono Modo (SMF) 10 Gb.
* Item 2, Módulo SFP para fibra óptica Multi Modo (MMF) 10 Gb.
* Item 3, Módulo SFP para fibra óptica Multi Modo (MMF) 1 Gb.
  * La empresa Technoma cumple con todos los requisitos técnicos solicitados para este lote.

De acuerdo con la documentación presentada por los oferentes y los análisis realizados a los mismos, se determina lo siguiente:

* Es viable la adjudicación del Lote 1 a la Empresa SSD.
* Es viable la adjudicación del Lote 2 a la Empresa Datasystems.
* Lote 3: Dada la no conformidad de todas las empresas con los requisitos técnicos establecidos, se recomienda declarar desierto el Lote 3.
* Es viable la adjudicación del Lote 4 a la Empresa Technoma.

Firmado digitalmente por:
JAVIER VEGA
Técnico Redes, Infraestructura y Seguridad
CRA/Departamento de Informática
Dirección General de Administración y Finanzas
Gerencia General
Ministerio de Economía y Finanzas

RICHARD ERNESTO SCHITTNER RAMIREZ

Firmado digitalmente por RICHARD ERNESTO SCHITTNER RAMIREZ
Fecha: 2025.03.05 11:59:20 -03'00'