ANEXO AL INTERNO CE 17/2020
Verificación Planillas de Datos Garantizados

EVALUACION DE LA OFERTA DE TES INGENIERIA de Diego Rodriguez EN EL ITEM 1:

EVALUACION DE LA FIRMA TES INGENIERIA POR LA OFERTA DEL ÍTEM 1: TELEVISOR		PLANILLA DE DATOS GARANTIZADOS TES INGENIERIA		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
MARCA:	Indicar exactamente, de manera a comprobar en el catálogo on-line del fabricante			JAM
MODELO:	Indicar exactamente, de manera a comprobar en el catálogo on-line del fabricante			JA65UHD202
NÚMERO DE PARTE DEL FABRICANTE DEL EQUIPO	Indicar exactamente, de manera a comprobar en el catálogo on-line del fabricante			JA65UHD202
ORIGEN/PROCEDENCIA	Indicar	Exigido	CUMPLE	CHINA
CANTIDAD	1	Exigido	CUMPLE	1
TAMAÑO DE PANTALLA	65 pulgadas como mínimo	Exigido	CUMPLE	SE VERIFICA SEGÚN CATAGO WEB
TECNOLOGÍA	LED	Exigido	CUMPLE	
CALIDAD DE IMAGEN	Resolución Mínima 3840X2160	Exigido	CUMPLE	
CONEXIONES REQUERIDAS	HDMI	Exigido	CUMPLE	
	USB	Exigido	CUMPLE	
	Video Compuesto	Exigido	CUMPLE	
	Auxiliar y sonido	Exigido	CUMPLE	
	Ethernet	Exigido	CUMPLE	
	Wifi	Exigido	CUMPLE	
RESPALDO TÉCNICO	Pedestal o soporte de pie o mueble	Exigido	CUMPLE	Soporte de pie estructura metalica

EVALUACION DE LA OFERTA DE LA EMPRESA OLAM S.R.L. EN EL ITEM 3:

EVALUACION DE LA OFERTA DE LA FIRMA OLAM S.R.L. POR EL ÍTEM 3: CAMARA WEB		PLANILLA DE DATOS GARANTIZADOS OLAM S.R.L.		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
MARCA:	Indicar exactamente, de manera a comprobar en el catálogo on-line del fabricante			Argom Tech
MODELO:	Indicar exactamente, de manera a comprobar en el catálogo on-line del fabricante			Cam20
ORIGEN/PROCEDENCIA	Indicar	Exigido	CUMPLE	China
CANTIDAD	2	Exigido	CUMPLE	2
RESOLUCIÓN	720p HD como mínimo	Exigido	CUMPLE	Se verifica datos según catalogo WEB
TIPO DE CONEXIÓN:	USB	Exigido	CUMPLE	
COMPATIBILIDAD SO	Windows 7 / 8 / 10 / Linux	Exigido	CUMPLE	
CARACTERÍSTICAS	Micrófono con reducción de ruido	Exigido	CUMPLE	
PÁGINA WEB:	Indicar la página Web del fabricante para verificación de las especificaciones técnicas cotizadas.	Exigido	CUMPLE	

EVALUACION DE LA OFERTA DE LA EMPRESA TECHNOMA SACI EN EL ITEM 4:

EVALUACION DE OFERTAS DE LA FIRMA TECHNOMA PARA EL ITEM 4: DISPOSITIVOS DE RED FIREWALL		PLANILLA DE DATOS GARANTIZADOS TECHNOMA SACI		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
	Se solicita la provisión, instalación y configuración llave en mano de dispositivos de RED, para reemplazar un dispositivo de Borde de menor generación Fortinet 100D, según se detalla a continuación:			
MARCA:	Indicar exactamente, de manera a comprobar en el catálogo on-line del fabricante		CUMPLE	FORTINET
MODELO:	Indicar exactamente, de manera a comprobar en el catálogo on-line del fabricante		FG-100F-BDL-950-36	FORTIGATE-100F HARDWAREPLUS 3 YEAR 24X7 FORTICARE AND FORTIGUARD UNIFIED (UTM) PROTECTION
ORIGEN/PROCEDENCIA	Indicar exactamente, de manera a comprobar en el catálogo on-line del fabricante		CUMPLE	USA
CANTIDAD REQUERIDA:	1 Unidad		CUMPLE	1
CARACTERÍSTICAS GENERALES	Throughput de por lo menos 20 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Soporte a por lo menos 1.5M conexiones simultaneas	Exigido		
	Soporte a por lo menos 56K nuevas conexiones por segundo	Exigido		
	Throughput de al menos 11 Gbps de VPN IPSec	Exigido		
	Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos	Exigido		
	Estar licenciado para, o soportar sin necesidad de licencia, 15K túneles de clientes VPN IPSec simultáneos	Exigido		
	Throughput de al menos 1 Gbps de VPN SSL	Exigido		
	Soportar al menos 500 clientes de VPN SSL simultáneos	Exigido		
	Soportar al menos 2.5 Gbps de throughput de IPS	Exigido		
	Soportar al menos 1 Gbps de throughput de Inspección SSL	Exigido		
	Soportar al menos 2 Gbps de throughput de Application Control	Exigido		
	Soportar al menos 1.5 Gbps de throughput de NGFW	Exigido		
	Soportar al menos 1 Gbps de throughput de Threat Protection	Exigido		
	La solución debe contar con funcionalidad de Controlador de red Wireless para equipos Access Point de la misma marca. Debe permitir gestionar al menos 128 Access Points.	Exigido		
	Tener al menos 12 interfaces 1Gbps RJ45 y 4 interfaces SFP	Exigido		
	Tener al menos 2 interfaces 10Gbps	Exigido		
	Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance	Exigido		
	Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance	Exigido		
REQUISITOS MÍNIMOS DE FUNCIONALIDAD				
CARACTERISTICAS	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.;	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	Exigido		
	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;	Exigido		
	La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;	Exigido		
	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;	Exigido		
	La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;	Exigido		
	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;	Exigido		
	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;	Exigido		
	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;	Exigido		
	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);	Exigido		
	Los dispositivos de protección de red deben soportar DHCP Relay;	Exigido		
	Los dispositivos de protección de red deben soportar DHCP Server;	Exigido		
	Los dispositivos de protección de red deben soportar sFlow;	Exigido		
	Los dispositivos de protección de red deben soportar Jumbo Frames;	Exigido		

EVALUACION DE OFERTAS DE LA FIRMA TECHNOMA PARA EL ITEM 4: DISPOSITIVOS DE RED FIREWALL		PLANILLA DE DATOS GARANTIZADOS TECHNOMA SACI		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;	Exigido		
	Debe ser compatible con NAT dinámica (varios-a-1);	Exigido		
	Debe ser compatible con NAT dinámica (muchos-a-muchos);	Exigido		
	Debe soportar NAT estática (1-a-1);	Exigido		
	Debe admitir NAT estática (muchos-a-muchos);	Exigido		
	Debe ser compatible con NAT estático bidireccional 1-a-1;	Exigido		
	Debe ser compatible con la traducción de puertos (PAT);	Exigido		
	Debe ser compatible con NAT Origen;	Exigido		
	Debe ser compatible con NAT de destino;	Exigido		
	Debe soportar NAT de origen y NAT de destino de forma simultánea;	Exigido		
	Debe soportar NAT de origen y NAT de destino en la misma política	Exigido		
	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;	Exigido		
	Debe ser compatible con NAT64 y NAT46;	Exigido		
	Debe implementar el protocolo ECMP;	Exigido		
	Debe soportar SD-WAN de forna nativa	Exigido		
	Debe soportar el balanceo de enlace hash por IP de origen;	Exigido		
	Debe soportar el balanceo de enlace por hash de IP de origen y destino;	Exigido		
	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;	Exigido		
	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;	Exigido		
	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;	Exigido		
	Enviar logs a sistemas de gestión externos simultáneamente;	Exigido		
	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;	Exigido		
	Debe soporta protección contra la suplantación de identidad (anti-spoofing);	Exigido		
	Implementar la optimización del tráfico entre dos dispositivos;	Exigido		
	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);	Exigido		
	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);	Exigido		
	Soportar OSPF graceful restart;	Exigido		
	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;	Exigido		
	Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;	Exigido		
	Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;	Exigido		
	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;	Exigido		
	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;	Exigido		
	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;	Exigido		
	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;	Exigido		
	La configuración de alta disponibilidad debe sincronizar: Sesiones;	Exigido		
	La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;	Exigido		
	La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;	Exigido		
	La configuración de alta disponibilidad debe sincronizar: Tablas FIB;	Exigido		
	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Debe soportar la creación de sistemas virtuales en el mismo equipo;	Exigido		
	Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;	Exigido		
	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;	Exigido		
	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;	Exigido		

EVALUACION DE OFERTAS DE LA FIRMA TECHNOMA PARA EL ITEM 4: DISPOSITIVOS DE RED FIREWALL		PLANILLA DE DATOS GARANTIZADOS TECHNOMA SACI		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
	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);	Exigido		
	Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;	Exigido		
	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;	Exigido		
	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;	Exigido		
	La consola de administración debe soportar como minimo, ingles, Español y Portugues.	Exigido		
	La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.	Exigido		
	La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.	Exigido		
CONTROL POR POLITICA DE FIREWALL	Debe soportar controles de zona de seguridad;	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Debe contar con políticas de control por puerto y protocolo;	Exigido		
	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;	Exigido		
	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;	Exigido		
	Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;	Exigido		
	Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;	Exigido		
	Debe soportar automatización de situaciones como deteción de equipos comprometidos, estado del sistema, cambios de onfiguración, eventos especificos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.	Exigido		
	Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);	Exigido		
	Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes	Exigido		
	Debe soportar el protocolo estándar de la industria VXLAN;	Exigido		
	La solución debe permitir la implementación sin asistencia de SD-WAN	Exigido		
	En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;	Exigido		
	la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall.	Exigido		
CONTROL DE APLICACIÓN	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Detección de miles de aplicaciones en 18 categorias, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;	Exigido		
	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;	Exigido		
	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;	Exigido		
	Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;	Exigido		
	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;	Exigido		
	Actualización de la base de firmas de la aplicación de forma	Exigido		

EVALUACION DE OFERTAS DE LA FIRMA TECHNOMA PARA EL ITEM 4: DISPOSITIVOS DE RED FIREWALL		PLANILLA DE DATOS GARANTIZADOS TECHNOMA SACI		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
	automática;			
	Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por politica de usuarios y grupos;	Exigido		
	Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;	Exigido		
	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;	Exigido		
	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;	Exigido		
	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;	Exigido		
	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;	Exigido		
	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;	Exigido		
	Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;	Exigido		
	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);	Exigido		
	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;	Exigido		
	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;	Exigido		
	Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente	Exigido		
PREVENCIÓN DE AMENAZAS	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);	Exigido		
	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;	Exigido		
	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;	Exigido		
	Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes politicas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;	Exigido		
	Deber permitir el bloqueo de vulnerabilidades y exploits conocidos	Exigido		
	Debe incluir la protección contra ataques de denegación de servicio;	Exigido		
	Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;	Exigido		
	Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;	Exigido		
	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;	Exigido		
	Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;	Exigido		
	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);	Exigido		
	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;	Exigido		
	Detectar y bloquear los escaneos de puertos de origen;	Exigido		
	Bloquear ataques realizados por gusanos (worms) conocidos;	Exigido		
	Contar con firmas específicas para la mitigación de ataques DoS y DDoS;	Exigido		
	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);	Exigido		
	Debe poder crear firmas personalizadas en la interfaz gráfica del producto;	Exigido		
	Identificar y bloquear la comunicación con redes de bots;	Exigido		
	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;	Exigido		
	Debe ser compatible con la captura de paquetes (PCAP), mediante la	Exigido		

EVALUACION DE OFERTAS DE LA FIRMA TECHNOMA PARA EL ITEM 4: DISPOSITIVOS DE RED FIREWALL		PLANILLA DE DATOS GARANTIZADOS TECHNOMA SACI		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
	firma de IPS o control de aplicación;			
	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;	Exigido		
	Los eventos deben identificar el país que origino la amenaza;	Exigido		
	Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);	Exigido		
	Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;	Exigido		
	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;	Exigido		
	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;	Exigido		
	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);	Exigido		
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);	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;	Exigido		
	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;	Exigido		
	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;	Exigido		
	Tener por lo menos 75 categorías de URL;	Exigido		
	Debe tener la funcionalidad de exclusión de URLs por categoría;	Exigido		
	Permitir página de bloqueo personalizada;	Exigido		
	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);	Exigido		
	Además del Explicit Web Proxy, soportar proxy web transparente;	Exigido		
IDENTIFICACIÓN DE USUARIOS	Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	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;	Exigido		
	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;	Exigido		
	Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;	Exigido		
	Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios;	Exigido		
	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);	Exigido		
	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;	Exigido		
	Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;	Exigido		
	Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;	Exigido		

EVALUACION DE OFERTAS DE LA FIRMA TECHNOMA PARA EL ITEM 4: DISPOSITIVOS DE RED FIREWALL		PLANILLA DE DATOS GARANTIZADOS TECHNOMA SACI		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
	Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;	Exigido		
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;	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;	Exigido		
	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;	Exigido		
	Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;	Exigido		
	Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;	Exigido		
	Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;	Exigido		
	En QoS debe permitir la definición de tráfico con ancho de banda garantizado;	Exigido		
	En QoS debe permitir la definición de tráfico con máximo ancho de banda;	Exigido		
	En QoS debe permitir la definición de colas de prioridad;	Exigido		
	Soportar marcación de paquetes DiffServ, incluso por aplicación;	Exigido		
	Soportar la modificación de los valores de DSCP para Diffserv;	Exigido		
	Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);	Exigido		
	Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;	Exigido		
FILTRO DE DATOS	Permite la creación de filtros para archivos y datos predefinidos;	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Los archivos deben ser identificados por tamaño y tipo;	Exigido		
	Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;	Exigido		
	Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;	Exigido		
	Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;	Exigido		
	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;	Exigido		
GEO LOCALIZACIÓN	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Debe permitir la visualización de los países de origen y destino en los registros de acceso;	Exigido		
	Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;	Exigido		
VPN	Soporte VPN de sitio-a-sitio y cliente-a-sitio;	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Soportar VPN IPSec;	Exigido		
	Soportar VPN SSL;	Exigido		
	La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512	Exigido		
	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;	Exigido		
	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);	Exigido		
	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);	Exigido		
	Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;	Exigido		
	Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;	Exigido		
	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;	Exigido		
	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;	Exigido		
	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;	Exigido		
	Suportar autenticación vía AD/LDAP, Secure id, certificado y base de	Exigido		

EVALUACION DE OFERTAS DE LA FIRMA TECHNOMA PARA EL ITEM 4: DISPOSITIVOS DE RED FIREWALL		PLANILLA DE DATOS GARANTIZADOS TECHNOMA SACI		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
	usuarios local;			
	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;	Exigido		
	Deberá mantener una conexión segura con el portal durante la sesión;	Exigido		
	El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.	Exigido		
	Numero de Instancias virtuales: 10	Exigido		
WIRELESS CONTROLLER	Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;	Exigido		
	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;	Exigido		
	La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;	Exigido		
	El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;	Exigido		
	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;	Exigido		
	Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points;	Exigido		
	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;	Exigido		
	Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;	Exigido		
	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;	Exigido		
	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;	Exigido		
	La solución debe permitir definir qué redes serán tuneladas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso;	Exigido		
	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;	Exigido		
	La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz;	Exigido		
	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;	Exigido		
	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;	Exigido		
	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;	Exigido		
	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	Exigido		

EVALUACION DE OFERTAS DE LA FIRMA TECHNOMA PARA EL ITEM 4: DISPOSITIVOS DE RED FIREWALL		PLANILLA DE DATOS GARANTIZADOS TECHNOMA SACI		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
	cuando el MAC Address de la interfaz LAN es ligeramente diferente (adyacente) del MAC Address de la interfaz WLAN;			
	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;	Exigido		
	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;	Exigido		
	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;	Exigido		
	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;	Exigido		
	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;	Exigido		
	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;	Exigido		
	Debe permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;	Exigido		
	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;	Exigido		
	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;	Exigido		
	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;	Exigido		
	La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica;	Exigido		
	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;	Exigido		
	La solución debe implementar técnicas de Call Admission Control para limitar el número de llamadas simultáneas;	Exigido		
	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;	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	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;	Exigido		
	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;	Exigido		
	La solución debe tener capacidad capaz de convertir paquetes Multicast en paquetes Unicast cuando se reenvían a los dispositivos que están conectados a la infraestructura inalámbrica, mejorando así el consumo de Airtime;	Exigido		
	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;	Exigido		
	La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz;	Exigido		

EVALUACION DE OFERTAS DE LA FIRMA TECHNOMA PARA EL ITEM 4: DISPOSITIVOS DE RED FIREWALL		PLANILLA DE DATOS GARANTIZADOS TECHNOMA SACI		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
	La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;	Exigido		
	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;	Exigido		
	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;	Exigido		
	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;	Exigido		
	La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil y quinientas) aplicaciones;	Exigido		
	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;	Exigido		
	La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;	Exigido		
	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.	Exigido		
	La solución debe implementar mecanismos de protección para mitigar ataques a la infraestructura inalámbrica. Al menos ataques de denegación de servicio deben ser mitigados por la infraestructura a través del envío de paquetes de deauthentication	Exigido		
	La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;	Exigido		
	La solución debe monitorear y clasificar el riesgo de las aplicaciones accesadas por los clientes inalámbricos;	Exigido		
	Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;	Exigido		
	Debe implementar la autenticación administrativa a través del protocolo RADIUS;	Exigido		
	En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);	Exigido		
	En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;	Exigido		
	La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;	Exigido		
	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;	Exigido		
	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;	Exigido		
	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;	Exigido		
	La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;	Exigido		
	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;	Exigido		
	La solución debe permitir el hospedaje del captive portal en la	Exigido		

EVALUACION DE OFERTAS DE LA FIRMA TECHNOMA PARA EL ITEM 4: DISPOSITIVOS DE RED FIREWALL		PLANILLA DE DATOS GARANTIZADOS TECHNOMA SACI		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
	memoria interna del controlador inalámbrico;			
	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;	Exigido		
	La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;	Exigido		
	La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;	Exigido		
	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;	Exigido		
	La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6;	Exigido		
	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;	Exigido		
	Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;	Exigido		
	La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;	Exigido		
	La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;	Exigido		
	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;	Exigido		
	La solución debe permitir la configuración de redes Mesh entre los puntos de acceso administrados por ella;	Exigido		
	La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;	Exigido		
	La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;	Exigido		
	La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;	Exigido		
	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;	Exigido		
	La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;	Exigido		
	La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);	Exigido		
	La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato .pcap;	Exigido		
	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;	Exigido		
	La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos;	Exigido		
	La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;	Exigido		
	La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;	Exigido		
	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;	Exigido		
	La solución debe tener herramientas de diagnóstico y depuración;	Exigido		
	La solución debe soportar la comunicación con elementos externos a través de las API;	Exigido		
	La solución deberá ser compatible y administrar los puntos de acceso de este proceso;	Exigido		
SERVICIO:	El costo debe incluir la instalación, migración de reglas, políticas, conexiones VPN, y configuraciones del equipo a reemplazar de menor generación y garantizar su puesta en funcionamiento, Así como capacitación con énfasis a certificación para 1 funcionario de la institución, con profesionales de la marca ofertada	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
GARANTÍA:	El equipo debe contar con una garantía de 3 años	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN

EVALUACION DE OFERTAS DE LA FIRMA TECHNOMA PARA EL ITEM 4: DISPOSITIVOS DE RED FIREWALL		PLANILLA DE DATOS GARANTIZADOS TECHNOMA SACI		
		Mínimo Exigido	Cumple con las especificaciones requeridas (SI/NO)	OBSERVACIONES Detalle adicional a especificaciones técnicas
				DOCUMENTACION PRESENTADA
AUTORIZACION DEL FABRICANTE	El oferente deberá demostrar ser Vendedor autorizado del fabricante para la República del Paraguay Deberá ser Partner Certificado por la Marca.	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA
	La empresa debe contar con al menos 2 (Dos) técnicos certificados en la Marca	Exigido		
	Presentar documentación emitida por el fabricante donde avale al oferente ser Partner Certificado.	Exigido		
ANTIGÜEDAD EXPERIENCIA	Acreditar una antigüedad no menor de 5 años en el mercado del Paraguay en actividades relativas al ramo de Telecomunicaciones o Internetworking. El oferente deberá comprobar experiencia en proyectos de implementación de Firewalls en el sector público y/o privado paraguayo, de al menos 5 proyectos en los últimos 5 años.	Exigido	CUMPLE	SE VERIFICAN LOS PARAMETROS REQUERIDOS EN DOCUMENTACION PRESENTADA

LIC. JOSÉ MARTÍNEZ, MSc
Jefe CTIC