Asunción, 03 de noviembre de 2025

Señores
Coordinación de Unidad Operativa de Contratación
Ministerio de Economía y Finanzas

Presente

En el marco del proceso de **Adquisición de equipos e insumos informáticos varios, servidores y licencias para el MEF**, **ID de Licitación: 457.814**, se presenta la siguiente **evaluación técnica** elaborada por técnicos integrantes del comité evaluador.

De acuerdo con los métodos y criterios de evaluación establecidos en el **Pliego de Bases y Condiciones (PBC)**, y considerando las ofertas presentadas por los distintos oferentes, se procedió a realizar la evaluación técnica correspondiente, organizada por lotes, conforme se detalla a continuación:

LOTE 2 - SOFTWARE ANTIVIRUS

Se analizó la única oferta presentada por la firma **CORPORATION SEKIURA SACEI**, en relación con las especificaciones técnicas solicitadas en el presente llamado.

Del análisis efectuado se observa que, según consta en el **SIME 86.375, Folio N.º 02**, la empresa **CORPORATION SEKIURA SACEI** manifiesta **no contar con la carta de autorización del fabricante** para el ítem 2 **(antivirus Bitdefender)**, señalando no obstante que puede adquirirlo con soporte oficial.

Dado que este requisito es **exigido** para acreditar la capacidad técnica de la oferta, se concluye que **NO CUMPLE** con lo establecido en el **Pliego de Bases y Condiciones** para el **ítem 2 del Lote 2**.

LOTE 3 CERTIFICADOS

Se evaluó la oferta más baja presentada por la firma **CORPORATION SEKIURA SACEI**, verificando su cumplimiento con las especificaciones técnicas requeridas.

ITEM 1 - Certificado tipo SSL Premium (www.paraguayconcursa.gov.py)				
ÍTEMS	**ESPECIFICACIONES TÉCNICAS**	**CARACTERÍSTICAS**	**MÍNIMO EXIGIDO**	**CUMPLE**
1	Cantidad	1	Exigido	SI, SIME 84.780 F 60-61
2	Servicio	Certificado tipo SSL Premium para el dominio www.paraguayconcursa.gov.py.	Exigido	SI, SIME 84.780 F 60-61
3	Nivel de Cifrado	Que permitan la encriptación a 256 bits.	Exigido	SI, SIME 84.780 F 60-61
4	Navegadores que Reconoce	Los certificados deben ser reconocidos por Internet Explorer, Firefox, Chrome y Safari mínimamente.	Exigido	SI, SIME 84.780 F 60-61
5	Dispositivos que reconoce	Los certificados digitales deben ser reconocidos por dispositivos con IOS y Android mínimamente.	Exigido	SI, SIME 84.780 F 60-61
6	Duración de los certificados	Los certificados deberán durar por lo menos 02 (dos) años a partir de la emisión e instalación del certificado. La emisión deberá realizarse de común acuerdo con el área de TIC.	Exigido	SI, SIME 84.780 F 60-61
7	Garantía	Se requiere una garantía de buen funcionamiento del software sea conforme a las vigencias de suscripciones (2 años)	Exigido	SI, SIME 84.780 F 60-61
8	Entrega	30 días hábiles a partir de la recepción efectiva de la orden	Exigido	SI, SIME 84.780 F 60-61

ITEM 2 - Certificado tipo SSL Premium Wildcard para el dominio sfp.gov.py				
ÍTEMS	**ESPECIFICACIONES TÉCNICAS**	**CARACTERÍSTICAS**	**MÍNIMO EXIGIDO**	**CUMPLE**
1	Cantidad	1	Exigido	SI, SIME 84.780 F 60-61
2	Servicio	Certificado tipo SSL Premium Wildcard para el dominio sfp.gov.py El certificado Wildcard debe cubrir en verde toda la barra de dirección del navegador. El certificado Wildcard es para todo el dominio sfp.gov.py y los sub dominios del VCHGO (servicios, inapp, datos, postulación, etc.).	Exigido	SI, SIME 84.780 F 60-61
3	Nivel de Cifrado	Que permitan la encriptación a 256 bits.	Exigido	SI, SIME 84.780 F 60-61
4	Navegadores que Reconoce	Los certificados deben ser reconocidos por Internet Explorer, Firefox, Chrome y Safari mínimamente.	Exigido	SI, SIME 84.780 F 60-61
5	Dispositivos que reconoce	Los certificados digitales deben ser reconocidos por dispositivos con IOS y Android mínimamente.	Exigido	SI, SIME 84.780 F 60-61
6	Duración de los certificados	Los certificados deberán durar por lo menos 02 (dos) años a partir de la emisión e instalación del certificado. La emisión deberá realizarse de común acuerdo con el área de TIC.	Exigido	SI, SIME 84.780 F 60-61
7	Garantía	Se requiere una garantía de buen funcionamiento del software sea conforme a las vigencias de suscripciones (2 años)	Exigido	SI, SIME 84.780 F 60-61
8	Entrega	30 días hábiles a partir de la recepción efectiva de la orden	Exigido	SI, SIME 84.780 F 60-61

Luego del análisis correspondiente, se constata que la empresa **CUMPLE** con las condiciones técnicas establecidas para el **Lote 3 – Certificados**.

LOTE 4 - LICENCIA PARA FIREWALL.

Se analizó la oferta presentada por la firma **BIGQ S.A.**, en relación con las especificaciones técnicas solicitadas.

ITEM 1- LICENCIA FORTIGATE 100E		
Serie del Equipo Fortinet 1: FG100E4Q17005280		
Serie del Equipo Fortinet 2: FG100E4Q17021564		
Cantidad: 2		
CARACTERISTICAS	**MINIMO EXIGIDO**	**CUMPLE**
Throughput de por lo menos 7 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete	Exigido	Sí, SIME 84.684 F. 31-53
Soporte a por lo menos 2M conexiones simultaneas	Exigido	Sí, SIME 84.684 F. 31-53
Soporte a por lo menos 30K nuevas conexiones por segundo	Exigido	Sí, SIME 84.684 F. 31-53
Throughput de al menos 4 Gbps de VPN IPSec	Exigido	Sí, SIME 84.684 F. 31-53
Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos	Exigido	Sí, SIME 84.684 F. 31-53
Estar licenciado para, o soportar sin necesidad de licencia, 10K túneles de clientes VPN IPSec simultáneos	Exigido	Sí, SIME 84.684 F. 31-53
Throughput de al menos 250 Mbps de VPN SSL	Exigido	Sí, SIME 84.684 F. 31-53
Soportar al menos 300 clientes de VPN SSL simultáneos	Exigido	Sí, SIME 84.684 F. 31-53
Soportar al menos 500 Gbps de throughput de IPS	Exigido	Sí, SIME 84.684 F. 31-53
Soportar al menos 190 Mbps de throughput de Inspección SSL	Exigido	Sí, SIME 84.684 F. 31-53
Throughput de al menos 250 Mbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la solución de seguridad tenga debidamente activadasy operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado múltiples números de desempeño para cualquiera de las funcionalidades, solamente el de valor más pequeño será aceptado.	Exigido	Sí, SIME 84.684 F. 31-53

Permitir gestionar al menos 32 Access Points	Exigido	Sí, SIME 84.684 F. 31-53
Tener al menos 14 interfaces 1Gbps	Exigido	Sí, SIME 84.684 F. 31-53
Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance	Exigido	Sí, SIME 84.684 F. 31-53
Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	Exigido	Sí, SIME 84.684 F. 31-53
Las funcionalidades de protección de red que conforman la plataforma de seguridad, pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;	Exigido	Sí, SIME 84.684 F. 31-53
La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
La gestión de equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;	Exigido	Sí, SIME 84.684 F. 31-53
Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;	Exigido	Sí, SIME 84.684 F. 31-53
Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;	Exigido	Sí, SIME 84.684 F. 31-53
Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;	Exigido	Sí, SIME 84.684 F. 31-53
Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);	Exigido	Sí, SIME 84.684 F. 31-53
Los dispositivos de protección de red deben soportar DHCP Relay;	Exigido	Sí, SIME 84.684 F. 31-53

Los dispositivos de protección de red deben soportar DHCP Server;	Exigido	Sí, SIME 84.684 F. 31-53
Los dispositivos de protección de red deben soportar sFlow;	Exigido	Sí, SIME 84.684 F. 31-53
Los dispositivos de protección de red deben soportar Jumbo Frames;	Exigido	Sí, SIME 84.684 F. 31-53
Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser compatible con NAT dinámica (varios-a-1);	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser compatible con NAT dinámica (muchos-a-muchos);	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar NAT estática (1-a-1);	Exigido	Sí, SIME 84.684 F. 31-53
Debe admitir NAT estática (muchos-a-muchos);	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser compatible con NAT estático bidireccional 1-a-1;	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser compatible con la traducción de puertos (PAT);	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser compatible con NAT Origen;	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser compatible con NAT de destino;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar NAT de origen y NAT de destino de forma simultánea;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar NAT de origen y NAT de destino en la misma política	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;	Exigido	Sí, SIME 84.684 F. 31-53

Debe ser compatible con NAT64 y NAT46;	Exigido	Sí, SIME 84.684 F. 31-53
Debe implementar el protocolo ECMP;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar el balanceo de enlace hash por IP de origen;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar el balanceo de enlace por hash de IP de origen y destino;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Enviar logs a sistemas de gestión externos simultáneamente;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soporta protección contra la suplantación de identidad (anti-spoofing);	Exigido	Sí, SIME 84.684 F. 31-53
Implementar la optimización del tráfico entre dos dispositivos;	Exigido	Sí, SIME 84.684 F. 31-53
Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);	Exigido	Sí, SIME 84.684 F. 31-53
Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);	Exigido	Sí, SIME 84.684 F. 31-53
Soportar OSPF graceful restart;	Exigido	Sí, SIME 84.684 F. 31-53
Los dispositivos de protección deben tener la capacidad de operar simultáneamente en una única instancia de servidor de seguridad,	Exigido	Sí, SIME 84.684 F. 31-53

mediante el uso de sus interfaces físicas en los siguientes modos: modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3);		
Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;	Exigido	Sí, SIME 84.684 F. 31-53
La configuración de alta disponibilidad debe sincronizar: Sesiones;	Exigido	Sí, SIME 84.684 F. 31-53
La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;	Exigido	Sí, SIME 84.684 F. 31-53
La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;	Exigido	Sí, SIME 84.684 F. 31-53
La configuración de alta disponibilidad debe sincronizar: Tablas FIB;	Exigido	Sí, SIME 84.684 F. 31-53
En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar la creación de sistemas virtuales en el mismo equipo;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53

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	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Debe soportar un tejido de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Debe soportar controles de zona de seguridad;	Exigido	Sí, SIME 84.684 F. 31-53
Debe contar con políticas de control por puerto y protocolo;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;	Exigido	Sí, SIME 84.684 F. 31-53
Firewall debe poder aplicar la inspección UTM (control de aplicaciones y filtrado web como mínimo) directamente a las políticas de seguridad en vez de usar perfil obligatoriamente;	Exigido	Sí, SIME 84.684 F. 31-53
Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar el almacenamiento de bitácoras (logs) en tiempo real tanto para entorno de la nube como entorno local (on-premise);	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);	Exigido	Sí, SIME 84.684 F. 31-53

Debe existir una manera de evitar que el almacenamiento de logs en tiempo real no supere la velocidad de subida de los mismos (upload);	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar el protocolo estándar de la industria VXLAN;	Exigido	Sí, SIME 84.684 F. 31-53
Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos;	Exigido	Sí, SIME 84.684 F. 31-53
Reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;	Exigido	Sí, SIME 84.684 F. 31-53
Debe detectar aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;	Exigido	Sí, SIME 84.684 F. 31-53
Debe hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el tráfico corresponde a la especificación del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTTP. La decodificación de protocolo también debe identificar las características específicas dentro de una aplicación, incluyendo, pero no limitado al intercambio de ficheros dentro de Webex;	Exigido	Sí, SIME 84.684 F. 31-53
Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;	Exigido	Sí, SIME 84.684 F. 31-53

Actualización de la base de firmas de la aplicación de forma automática;	Exigido	Sí, SIME 84.684 F. 31-53
Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos;	Exigido	Sí, SIME 84.684 F. 31-53
Los dispositivos de protección de red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario;	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser posible añadir múltiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas;	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;	Exigido	Sí, SIME 84.684 F. 31-53
Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP;	Exigido	Sí, SIME 84.684 F. 31-53
El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;	Exigido	Sí, SIME 84.684 F. 31-53
Debe alertar al usuario cuando sea bloqueada una aplicación;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;	Exigido	Sí, SIME 84.684 F. 31-53

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	Sí, SIME 84.684 F. 31-53
Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente	Exigido	Sí, SIME 84.684 F. 31-53
Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti- spyware integrado en el propio equipo;	Exigido	Sí, SIME 84.684 F. 31-53
Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);	Exigido	Sí, SIME 84.684 F. 31-53
Las características de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;	Exigido	Sí, SIME 84.684 F. 31-53
Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;	Exigido	Sí, SIME 84.684 F. 31-53
Debe implementar los siguientes tipos de acciones a las amenazas detectadas por IPS: Permitir, permitir y generar registro, bloquear, bloquear IP del atacante durante un tiempo y enviar tcp-reset;	Exigido	Sí, SIME 84.684 F. 31-53
Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo;	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad;	Exigido	Sí, SIME 84.684 F. 31-53
Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas;	Exigido	Sí, SIME 84.684 F. 31-53
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;	Exigido	Sí, SIME 84.684 F. 31-53
Deber permitir el bloqueo de vulnerabilidades;	Exigido	Sí, SIME 84.684 F. 31-53

Debe permitir el bloqueo de exploits conocidos;	Exigido	Sí, SIME 84.684 F. 31-53
Debe incluir la protección contra ataques de denegación de servicio;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;	Exigido	Sí, SIME 84.684 F. 31-53
Detectar y bloquear los escaneos de puertos de origen;	Exigido	Sí, SIME 84.684 F. 31-53
Bloquear ataques realizados por gusanos (worms) conocidos;	Exigido	Sí, SIME 84.684 F. 31-53
Contar con firmas específicas para la mitigación de ataques DoS y DDoS;	Exigido	Sí, SIME 84.684 F. 31-53
Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);	Exigido	Sí, SIME 84.684 F. 31-53
Debe poder crear firmas personalizadas en la interfaz gráfica del producto;	Exigido	Sí, SIME 84.684 F. 31-53

Debe permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar el bloqueo de archivos por tipo;	Exigido	Sí, SIME 84.684 F. 31-53
Identificar y bloquear la comunicación con redes de bots;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir la captura de paquetes por tipo de firma IPS y definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la alerta, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Los eventos deben identificar el país que origino la amenaza;	Exigido	Sí, SIME 84.684 F. 31-53
Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);	Exigido	Sí, SIME 84.684 F. 31-53
Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
El Firewall debería permitirle analizar la implementación del tejido de seguridad para identificar posibles vulnerabilidades y resaltar las mejores prácticas que podrían utilizarse para mejorar la seguridad y el rendimiento general de su red;	Exigido	Sí, SIME 84.684 F. 31-53
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	Exigido	Sí, SIME 84.684 F. 31-53

donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;		
Los recursos de postura de seguridad deben existir para permitir que el software de seguridad de endpoint aplique protección en tiempo real, antivirus, filtrado de Web y control de aplicaciones en el punto final;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory y la base de datos local;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Tener por lo menos 60 categorías de URL;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener la funcionalidad de exclusión de URLs por categoría;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir página de bloqueo personalizada;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Además del Explicit Web Proxy, soportar proxy web transparente;	Exigido	Sí, SIME 84.684 F. 31-53

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	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Debe tener integración y soporte para Microsoft Active Directory para los siguientes sistemas operativos: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la política/control basados en usuarios y grupos de usuarios;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;	Exigido	Sí, SIME 84.684 F. 31-53
Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53

Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;	Exigido	Sí, SIME 84.684 F. 31-53
En QoS debe permitir la definición de tráfico con ancho de banda garantizado;	Exigido	Sí, SIME 84.684 F. 31-53
En QoS debe permitir la definición de tráfico con máximo ancho de banda;	Exigido	Sí, SIME 84.684 F. 31-53
En QoS debe permitir la definición de colas de prioridad;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar marcación de paquetes DiffServ, incluso por aplicación;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar la modificación de los valores de DSCP para Diffserv;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);	Exigido	Sí, SIME 84.684 F. 31-53
Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;	Exigido	Sí, SIME 84.684 F. 31-53
Permite la creación de filtros para archivos y datos predefinidos;	Exigido	Sí, SIME 84.684 F. 31-53

Los archivos deben ser identificados por tamaño y tipo;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);	Exigido	Sí, SIME 84.684 F. 31-53
Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir la visualización de los países de origen y destino en los registros de acceso;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;	Exigido	Sí, SIME 84.684 F. 31-53
Soporte VPN de sitio-a-sitio y cliente-a-sitio;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar VPN IPSec;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar VPN SSL;	Exigido	Sí, SIME 84.684 F. 31-53
La VPN IPSec debe ser compatible con 3DES;	Exigido	Sí, SIME 84.684 F. 31-53
La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;	Exigido	Sí, SIME 84.684 F. 31-53
La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;	Exigido	Sí, SIME 84.684 F. 31-53
La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);	Exigido	Sí, SIME 84.684 F. 31-53

La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);	Exigido	Sí, SIME 84.684 F. 31-53
La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;	Exigido	Sí, SIME 84.684 F. 31-53
Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;	Exigido	Sí, SIME 84.684 F. 31-53
La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web;	Exigido	Sí, SIME 84.684 F. 31-53
Las características de VPN SSL se deben cumplir con o sin el uso de agentes;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Asignación de DNS en la VPN de cliente remoto;	Exigido	Sí, SIME 84.684 F. 31-53
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	Sí, SIME 84.684 F. 31-53
Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir la visualización de los dispositivos inalámbricos conectados por usuario;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir la visualización de los dispositivos inalámbricos conectados por IP;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir la visualización de los dispositivos inalámbricos conectados por canal;	Exigido	Sí, SIME 84.684 F. 31-53

Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar Fast Roaming en autenticación con portal cautivo;	Exigido	Sí, SIME 84.684 F. 31-53
Debe soportar configuración de portal cautivo por SSID;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico;	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP;	Exigido	Sí, SIME 84.684 F. 31-53
Debe ser compatible con el protocolo 802.1x RADIUS;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DNS;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Broadcast;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Multicast;	Exigido	Sí, SIME 84.684 F. 31-53

La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue);	Exigido	Sí, SIME 84.684 F. 31-53
La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora deberá contar con mecanismos de protección de tramas de administración de acuerdo a las especificaciones de la alianza Wi-Fi y estándar 802.11ac;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge;	Exigido	Sí, SIME 84.684 F. 31-53
Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas;	Exigido	Sí, SIME 84.684 F. 31-53

Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh;	Exigido	Sí, SIME 84.684 F. 31-53
Ofrecer un mecanismo de creación automática y/o manual de usuarios visitantes y contraseñas, que puedan ser enviados por correo electrónico o SMS a los usuarios, con ajuste de tiempo de expiración de la contraseña;	Exigido	Sí, SIME 84.684 F. 31-53
La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS;	Exigido	Sí, SIME 84.684 F. 31-53
Debe tener un mecanismo de ajuste automático de potencia de la señal con el fin de reducir la interferencia entre canales entre dos puntos de acceso administrados;	Exigido	Sí, SIME 84.684 F. 31-53
Ofrecer un mecanismo de balanceo de tráfico/usuarios entre Puntos de acceso;	Exigido	Sí, SIME 84.684 F. 31-53
Proporcionar un mecanismo de balanceo de tráfico/usuarios entre frecuencias y/o radios de los Puntos de Acceso;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión;	Exigido	Sí, SIME 84.684 F. 31-53
Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados;	Exigido	Sí, SIME 84.684 F. 31-53

La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones;	Exigido	Sí, SIME 84.684 F. 31-53
la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico;	Exigido	Sí, SIME 84.684 F. 31-53
El controlador inalámbrico debe tener interfaz de administración integrado en el mismo equipo;	Exigido	Sí, SIME 84.684 F. 31-53
El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica deberá soportar aceleración de túnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica debe soportar protocolo LLDP;	Exigido	Sí, SIME 84.684 F. 31-53

Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC adyacente;	Exigido	Sí, SIME 84.684 F. 31-53
Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas;	Exigido	Sí, SIME 84.684 F. 31-53
La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada;	Exigido	Sí, SIME 84.684 F. 31-53
Deberá soportar la conversión de Multicast a Unicast para mejorar el rendimiento del tiempo de aire;	Exigido	Sí, SIME 84.684 F. 31-53
Debe proporcionar la capacidad de crear varias claves pre-compartidas de acceso protegido WiFi (WPA-PSK) para que no sea necesario compartir PSK entre dispositivos;	Exigido	Sí, SIME 84.684 F. 31-53
Garantía: Se requiere una garantía de buen funcionamiento del software por el periodo de 1 año	Exigido	Sí, SIME 84.684 F. 31-53
Plazo de entrega: 30 días hábiles a partir de la recepción efectiva de la orden	Exigido	Sí, SIME 84.684 F. 31-53

Tras la verificación realizada, se concluye que la firma **BIGQ S.A. CUMPLE** con las especificaciones técnicas para el **Lote 4 – Licencia para Firewall**.

LOTE 8 EQUIPOS DE COMUNICACIÓN.

Se evaluó la única oferta presentada por la firma **BIGQ S.A.**, verificando su correspondencia con las especificaciones técnicas solicitadas en el llamado.

ITEM 1 - SWITCH 48 PUERTOS			
Características	**Especificaciones**	**Requerimiento**	**Cumple**
Cantidad:	02 unidades	Exigido	Sí, SIME 86.684 F. 54,68
Total de Interfaces de Red	48x GE RJ45 y 4x GE SFP.	Exigido	Sí, SIME 86.684 F. 54,68
Puerto Dedicado de Administración 10/100	1.	Exigido	Sí, SIME 86.684 F. 54,68
Puerto Serial de Consola RJ-45	1.	Exigido	Sí, SIME 86.684 F. 54,68
Factor de Forma	1 RU Rack Mount.	Exigido	Sí, SIME 86.684 F. 54,68
Tiempo medio de fallos	> 10 años.	Exigido	Sí, SIME 86.684 F. 54,68
Capacidad de conmutación	104 Gbps. O SUPERIOR	Exigido	Sí, SIME 86.684 F. 54,68
Paquetes por Segundo	155 Mpps.	Exigido	Sí, SIME 86.684 F. 54,68
Almacenamiento de direcciones MAC	16K.	Exigido	Sí, SIME 86.684 F. 54,68
Latencia de Red	< 1µs.	Exigido	Sí, SIME 86.684 F. 54,68
Soporte de VLANs	4K.	Exigido	Sí, SIME 86.684 F. 54,68
IPv4/IPv6 Equipamiento listo para enrutamiento de pilas duales	SI.	Exigido	Sí, SIME 86.684 F. 54,68
Enlaces de Tamaño de Grupo Agregado	8.	Exigido	Sí, SIME 86.684 F. 54,68
Total, de Enlaces de Grupos Agregados	26.	Exigido	Sí, SIME 86.684 F. 54,68
Paquetes de Buffers	MÍNIMO 1.5 MB.	Exigido	Sí, SIME 86.684 F. 54,68
DRAM	512 MB.	Exigido	Sí, SIME 86.684 F. 54,68
FLASH	128 MB.	Exigido	Sí, SIME 86.684 F. 54,68
Energía Requerida	100 - 240V AC, 50 - 60 Hz.	Exigido	Sí, SIME 86.684 F. 54,68
Fuente de Alimentación	AC built in.	Exigido	Sí, SIME 86.684 F. 54,68
Consumo de Energía (Máximo)	39.19 W.	Exigido	Sí, SIME 86.684 F. 54,68
Humedad	10 - 90% Sin Condensación.	Exigido	Sí, SIME 86.684 F. 54,68
Compatibilidad:	compatible con estándares de red IEEE	Exigido	Sí, SIME 86.684 F. 54,68
Requisitos para implementación	Mínimamente deberá cumplir con los siguientes puntos: · Eliminación de credenciales predeterminadas y configuración inicial con contraseñas robustas.	Exigido	Sí, SIME 86.684 F. 54,68

	· Aplicación de configuraciones seguras (hardening) según buenas prácticas del fabricante. · Documentación y entrega de respaldos cifrados de la configuración inicial. · Segmentación lógica de red desde el momento de la instalación, con implementación de VLANs. · Verificación de integridad del firmware instalado y aseguramiento del uso de la versión estable más reciente. · Desactivación de servicios y protocolos inseguros por defecto. · Asegurar la trazabilidad mediante la habilitación de logs de administración y cambios de configuración. · Hardening del sistema operativo utilizado. · Cifrado de datos en tránsito y en reposo. · Registro, retención y revisión de logs de auditoría. · Segmentación lógica de red que asegure el aislamiento del servidor. · Implementación de respaldos periódicos cifrados y verificados. · Restricción de acceso remoto únicamente mediante mecanismos seguros, tales como VPN empresarial o soluciones de acceso adaptativo tipo Zero Trust, según compatibilidad con el entorno de la entidad.		
Garantía (escrita)	Mínimo de 24 meses. Incluye: Soporte de atención de Hardware, Mano de Obra y Repuestos incluyendo traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del proveedor. Si la reparación implica la indisponibilidad del equipo por más de 5 días, el proveedor deberá comunicar por escrito el motivo de la demora y proporcionar un equipo de reemplazo de similar o mejor característica del equipo con fallas, hasta concluir las tareas y reponer operativamente el equipo en	Exigido	Sí, SIME 86.684 F. 54,68

	reparación sin costo para la institución.		
Respaldo Técnico	Para garantizar a la institución, la garantía, así como la asistencia técnica especializada, será un requisito indispensable que la garantía pueda ser ejecutada en cualquiera de los CAS del país. El oferente deberá indicar cuáles son los CAS que existen en el país. La gestión de la ejecución de la garantía, deberá poder ser hecha, directamente a través de cualquiera de los CAS del país, o en su defecto, a través del Oferente, corriendo en su caso, por cuenta del Oferente que resulte adjudicado, la gestión de dicha ejecución.	Exigido	Sí, SIME 86.684 F. 54,68
Plazo de entrega	30 días hábiles a partir de la recepción efectiva de la orden	Exigido	Sí, SIME 86.684 F. 54,68

Posteriormente, se constató que la empresa **BIGQ S.A. CUMPLE** con las especificaciones técnicas requeridas para el **Lote 8 – Equipos de Comunicación**

Finalmente, se presenta a continuación un cuadro resumen en el que se detallan las conclusiones obtenidas por lote:

LOTE	OFERENTE	CUMPLE (SI/NO)
LOTE 2 SOFTWARE ANTIVIRUS	CORPORATION SEKIURA SACEI	**NO**
LOTE 3 CERTIFICADOS	CORPORATION SEKIURA SACEI	**SI**
LOTE 4 - LICENCIA PARA FIREWALL	BIGQ S.A.	**SI**
LOTE 8 EQUIPOS DE COMUNICACIÓN	BIGQ S.A.	**SI**

Es nuestro informe.

Firmado digitalmente por:
OSVALDO VERA MENDOZA
Técnico en Soporte
Dirección General de Administración y Finanzas
Dpto. de Informática - C.R.A.
Ministerio de Economía y Finanzas

Firmado digitalmente por:
GUSTAVO DAVID AMARILLA BOGADO
Jefe Interino – Departamento de Informática - CITI
Dirección General de Gabinete
Viceministerio de Economía y Planificación
Ministerio de Economía y Finanzas