ADENDA 2
PROCESO DE SELECCIÓN SELECCIÓN ABREVIADA POR SUBASTA INVERSA ELECTRÓNICA EFR-SASI-001-2025

La EMPRESA FÉRREA REGIONAL SAS- EFR, se permite informar que con ocasión a las respuestas de las observaciones recibidas y con el fin de evitar ambigüedades en los documentos del proceso, se considera necesario expedir una Adenda al proceso de **SELECCIÓN ABREVIADA POR SUBASTA INVERSA ELECTRÓNICA EFR-SASI-001-2025**, cuyo objeto es: "*ADQUISICIÓN DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL FIREWALL UTM QUE INCLUYA LOS EQUIPOS Y LICENCIAS NECESARIOS PARA SU FUNCIONAMIENTO, ASÍ COMO EL SOPORTE TÉCNICO DE ESTE.",* en el siguiente sentido:

1. **Adicionar al ANEXO COMPLEMENTARIO AL PLIEGO DE CONDICIONES, EL CAPÍTULO 9 ESPECIFICACIONES TÉCNICA**, el cual quedará de la siguiente manera:

***"CAPITULO 9* - ESPECIFICACIONES TÉCNICA**

A continuación, se describen las especificaciones técnicas mínimas que debe cumplir el contratista para la correcta ejecución del objeto contractual:

Descripción del artículo	*Cantidad*
Solución de seguridad Perimetral Firewall (Hardware)	*2*
Licenciamiento Firewall (Software)	*2*
Implementación Firewall	*1*
Garantía y Soporte	*1*

Solución de seguridad Perimetral Firewall (Hardware)

A	*SOLUCIÓN DE FIREWALL EN HA*
1	*Características base del Firewall*

1.1	*La solución debe contar con gestión de reglas de firewall e interfaz de usuario optimizada y diseñada específicamente para grandes conjuntos de reglas de un vistazo e indicadores de cumplimiento.*
1.2	*La solución debe tener soporte de autenticación en dos factores (contraseña única) para acceso de administrador, portal de usuario, IPSec y SSL VPN.*
1.3	*La solución debe tener herramientas avanzadas de resolución de problemas en GUI (por ejemplo, captura de paquetes).*
1.4	*La solución debe tener soporte de alta disponibilidad (HA) para agrupar dos dispositivos en modo activo-activo o activo-pasivo con configuración de HA rápida plug-and-play según sea requerido.*
1.5	*La solución debe tener interfaz de línea de comandos completa (CLI) accesible desde la GUI.*
1.6	*La solución debe tener administración basada en roles.*
1.7	*La solución debe realizar notificación de actualización de firmware automatizada con un sencillo proceso de actualización automática y funciones de reversión.*
1.8	*La solución debe tener definiciones de objetos del sistema reutilizables para redes, servicios, hosts, períodos de tiempo, usuarios y grupos, clientes y servidores.*
1.9	*La solución debe tener portal de usuarios de autoservicio.*
1.10	*La solución deberá permitir realizar seguimiento de cambios en configuración.*
1.11	*La solución deberá tener control de acceso de dispositivos flexible para servicios por zonas.*
1.12	*La solución deberá tener opciones de notificación por correo electrónico o SNMP.*
1.13	*La solución debe tener compatibilidad con SNMPv3 y Netflow.*
1.14	*Soporte de administración central a través de la consola unificada basada en la nube.*
1.15	*La solución debe realizar notificaciones automáticas por correo electrónico para cualquier evento importante.*
1.16	*La solución debe contar con configuraciones para copia de seguridad y restauración: localmente, vía FTP o correo electrónico; bajo demanda, diario, semanal o mensual.*
1.17	*La solución deberá tener API para integración de terceros en caso de*

	ser requerido.
1.18	*La solución deberá tener la opción de acceso remoto para el soporte del Fabricante.*
1.19	*La solución deberá tener la gestión de licencias basada en la nube a través de un portal de licencias del Fabricante.*
1.20	*La solución deberá tener soporte de Syslog.*
1.21	*La solución deberá tener monitoreo de flujo en tiempo real.*
1.22	*La solución deberá tener indicadores o Alertas de estilo semáforo.*
1.23	*La solución deberá tener interacción rápida y detallada con cualquier widget del centro de control.*
1.24	*La solución deberá tener SNMP con una MIB personalizada y soporte para túneles VPN IPSec.*
1.25	*La solución debe tener soporte para nuevas instancias de AWS (C5 / M5 y T3)*
1.26	*La solución debe tener soporte de zona WAN virtual en puertas de enlace personalizadas para el uso de un solo brazo posterior a la implementación.*
1.27	***La solución deberá soportar traducción de direcciones entre IPv6 e IPv4 (NAT64).***
1.28	***La solución deberá soportar DHCPv6 Prefix Delegation.***
1.29	*La solución debe contar con capacidades de protección de DNS mediante un servicio de resolución en la nube integrado con el firewall, que bloquee consultas a dominios maliciosos en puertos, protocolos y aplicaciones. Además, debe permitir aplicar políticas de seguridad y cumplimiento de forma centralizada desde la misma consola de gestión de la solución.*
1.30	***El Firewall deberá contar con funcionalidades de Web Application Firewall (WAF) y Protección de Correo Electrónico (Email Protection), disponibles nativamente o mediante licenciamiento adicional, que puedan activarse en caso de requerirse a futuro.***
1.31	***Estas funcionalidades se deben lograr dentro del mismo appliance, o que la integración pueda ser desde otros appliance adicionales (Virtual, Hardware o Cloud) para lograr dichas funcionalidades en caso de requerirse***

1.32	***firewall deberá garantizar la posibilidad de habilitar e incorporar funcionalidades de Acceso a la Red de Confianza Cero (Zero Trust Network Access, ZTNA) en caso de requerirse a futuro, sin necesidad de adquirir, instalar o desplegar un appliance, módulo o hardware adicional.*** ***La solución deberá permitir implementar políticas de acceso Zero Trust utilizando el firewall como punto de acceso / conector.***
2	***Gestión Central del Firewall***
2.1	*La solución debe permitir la gestión de los equipos Firewall y los informes de estos equipos (hasta 7 días), desde una sola consola de gestión basada en la nube, donde, además, esta consola debe de proporcionar gestión de políticas por grupos de equipos.*
2.2	*La gestión de políticas de grupo debe permitir que los objetos, la configuración y las políticas se modifiquen una vez y se sincronicen automáticamente con todos los Firewall del grupo.*
2.3	*La consola debe proporcionar una pista de auditoría histórica completa y un seguimiento del estado de los cambios en las políticas del grupo.*
2.4	*La consola además debe permitir la gestión de firmware de los equipos, así como el respaldo de los últimos cinco archivos de configuración para cada firewall.*
2.5	*Las actualizaciones de firmware se deben ofrecen al administrador de la consola de tal manera que con un solo clic se pueda aplicar dicha actualización a cualquier dispositivo manejado dentro de la consola.*
2.6	*La solución debe permitir implementaciones "Zero-Touch" desde esta consola central, permitiendo exportar la configuración para cargarla en un dispositivo desde una unidad flash, conectando así automáticamente al dispositivo a la consola Central.*
2.7	*Debe permitir la programación de actualizaciones de firmware*
2.8	*Debe permitir la generación de Informes de múltiples firewalls.*
2.9	*Debe además permitir guardar, programar y exportar informes desde esta consola central.*
2.10	*Esta Consola de gestión debe ser sin ningún costo ni tampoco debe ofertarse como "regalía".*

2.11	*La solución deberá contar con un mecanismo de reversión automática (Auto-Rollback) en caso de fallo en la actualización de firmware, aplicable tanto en despliegues individuales como en alta disponibilidad.*
2.12	*La consola de administración deberá ofrecer búsqueda de referencias de objetos (Object reference lookup) de red, servicios y políticas, para identificar dependencias y limpiar configuraciones obsoletas.*
2.13	*La solución debe permitir la restauración de respaldos de configuración entre diferentes modelos de la misma plataforma, aun cuando tengan distinta cantidad o tipo de interfaces físicas, mediante un asistente que permita mapear interfaces y servicios al nuevo hardware.*
3	***Firewall, Redes y Enrutamiento***
3.1	*El Firewall debe permitir una inspección profunda de paquetes donde todos paquetes deben ser inspeccionados por los motores de IPS, web, AV, control de aplicaciones e inspección SSL, utilizando un motor DPI (Deep Packet Inspection) de transmisión de alto rendimiento y sin proxy.*
3.2	*El Firewall debe contar con Inspección TLS de alto rendimiento, debe contar con compatibilidad de TLS 3 sin degradación, políticas de nivel empresarial independientes del puerto, debe permitir una visibilidad única desde el panel de control así resolución de problemas de compatibilidad.*
3.3	*El Firewall debe contar con una tecnología que le permita descargar el tráfico de forma inteligente para transferir el tráfico confiable a altas velocidades. La descarga de este tráfico se deberá controlar mediante una política para acelerar el tráfico importante de aplicaciones en la nube, o de forma inteligente en función de las características del tráfico.*
3.4	*Debe contar con una lista de excepciones "pre empaquetada".*
3.5	*Debe cubrir todos los puertos / protocolos.*
3.6	*Debe admitir todas las suites de cifrado modernas.*
3.7	*La solución debe proporcionar políticas basadas en usuarios, grupos, horarios o redes.*
3.8	*La solución debe proporcionar políticas de tiempo de acceso por usuario / grupo.*
3.9	*La solución deberá hacer cumplir las políticas en zonas, redes o por tipo de servicio.*
3.10	*La solución deberá contar con un firewall basado en zonas.*
3.11	*Deberá proporcionar las zonas predeterminadas para LAN, WAN, DMZ,*

	LOCAL, VPN y WiFi.
3.12	*La solución debe permitir el soporte completo de VLAN.*
3.13	*Deberá permitir el aislamiento de zonas y VLAN.*
3.14	*La solución deberá permitir la microsegmentación y autoaislamiento mediante seguridad sincronizada.*
3.15	*Debe permitir personalizar zonas en LAN o DMZ.*
3.16	*La solución de Firewall debe permitir la creación de políticas NAT personalizables con enmascaramiento de IP y soporte completo de objetos para redirigir o reenviar múltiples servicios en una sola regla con un asistente de reglas para crear rápida y fácilmente reglas NAT complejas con solo unos pocos clics.*
3.17	*La solución debe contar con protección flood: bloqueo DoS, DDoS y escaneo de puertos.*
3.18	*Debe permitir el bloqueo de país por geo-IP.*
3.19	*La solución debe ofrecer enrutamiento avanzado: estático, multidifusión (PIM-SM) y dinámico (RIP, BGP, OSPF) con compatibilidad total con VLAN 801Q.*
3.20	*Debe permitir el enrutamiento de multidifusión independiente del protocolo con snooping IGMP.*
3.21	*La solución debe contar con soporte y etiquetado de VLAN DHCP.*
3.23	*La solución de Firewall debe permitir el equilibrio de enlace SD-WAN: múltiples conexiones a Internet, verificación de estado de enlace automático, conmutación por error automática, equilibrio automático y ponderado y reglas granulares de múltiples rutas.*
3.24	*La solución deberá permitir la configuración completa de DNS, DHCP y NTP.*
3.25	*Deberá permitir DNS dinámico (DDNS).*
3.26	*Deberá contar con la certificación de aprobación del programa de logotipo IPv6 Ready.*
3.27	*La solución deberá brindar soporte de tunelización IPv6 que incluye implementación rápida 6in4, 6to4, 4in6 e IPv6 (6rd) a través de IPSec.*
3.28	*La solución debe soportar enrutamiento con múltiples rutas de costo igual (ECMP).*
3.29	*La solución deberá permitir la redistribución de rutas aprendidas mediante BGP hacia OSPFv*

3.30	*La solución deberá permitir que clientes con conectividad únicamente IPv6 puedan acceder a recursos en IPv4 mediante el uso de proxy explícito*
4	***SD-WAN:***
4.1	*La solución debe permitir el soporte para múltiples opciones de enlace WAN, incluyendo VDSL, DSL, cable y celular 3G / 4G / LTE con monitoreo esencial, balanceo, failover y fail- back".*
4.2	*SD-WAN sincronizada: La solución de firewall debe garantizar la integración con el Antivirus del mismo fabricante permitiendo sincronizar la seguridad de ambos componentes para así aprovechar la claridad y confiabilidad de la identificación de aplicaciones que viene con el intercambio de información entre los puntos finales administrados y el firewall.*
4.3	*La solución debe permitir el enrutamiento sincronizado de aplicaciones SD-WAN a través de enlaces preferidos a través de reglas de firewall o enrutamiento basado en políticas.*
4.4	*Debe permitir la implementación asequible, flexible y sin intervención o con poca intervención.*
4.5	*Debe contar con soporte VPN robusto que incluye IPSec y SSL VPN*
4.6	*Debe permitir la orquestación de VPN centralizada*
4.7	***Integración con Azure Virtual WAN para una red de superposición SD-WAN completa.***
5	***Cuotas y configuración de Traffic Shaping.***
5.1	*La solución debe permitir configurar "Traffic Shaping (QoS) en la red o basado en el usuario (con opciones mejoradas de tráfico web y de aplicaciones incluidas con la suscripción del mismo fabricante).*
5.2	*Debe permitir establecer cuotas de tráfico basadas en el usuario en carga / descarga o tráfico total y cíclico o no cíclico.*
5.3	*Deberá permitir la optimización de VoIP en tiempo real.*
5.4	***Seguridad inalámbrica***
5.5	*Puente de AP a LAN, VLAN o una zona separada con opciones de aislamiento de clientes.*
5.6	*Deberá poseer la compatibilidad con varios SSID por radio, incluidos los SSID ocultos.*

5.07	*Deberá brindar soporte para los últimos estándares de seguridad y cifrado, incluidos WPA2 Personal y Enterprise.*
5.08	*Debe permitir la opción de selección de ancho de canal.*
5.09	*Deberá permitir el soporte para IEEE 801X (autenticación RADIUS) con soporte para servidor primario y secundario.*
5.10	*Deberá permitir el soporte para 8011r (transición rápida).*
5.11	*La solución deberá permitir la creación de cupones (personalizados), contraseña del día o aceptación de T&C.*
5.12	*Debe permitir el acceso a Internet de invitados con acceso a la red inalámbrica basada en el tiempo.*
5.13	*La solución deberá permitir el modo de red en malla y repetición inalámbrica con AP admitidos.*
5.14	*Debe optimizar la selección automática de canales.*
5.15	*Debe contar con soporte para inicio de sesión HTTPS.*
5.16	***La solución debe tener la capacidad de detección de puntos de acceso no autorizados.***
6	***Autenticación:***
6.1	*La solución deberá permitir la autenticación a través de: Active Directory, eDirectory, RADIUS, LDAP y TACACS +.*
6.2	*Deberá brindar agentes de autenticación para Active Directory, SSO, STAS, SATC.*
6.3	*La solución deberá contar con un inicio de sesión único: Active Directory, eDirectory, RADIUS.*
6.4	*La consola deberá permitir la autenticación de dos factores (2FA).*
6.5	*Deberá permitir la compatibilidad con los agentes de autenticación de cliente para Windows, Mac OS X, Linux 32/64*
6.6	*Deberá contar con la autenticación SSO del navegador: autenticación de proxy transparente (NTLM) y Kerberos.*
6.7	*Deberá brindar un portal cautivo de inicio de sesión en los navegadores.*
6.8	*La solución deberá contar con certificados de autenticación para iOS y Android.*
6.9	*Deberá permitir servicios de autenticación para IPSec, SSL, L2TP*
6.10	*Deberá contar con soporte de autenticación de Google Chromebook para entornos con Active Directory y Google G Suite.*

6.11	*Deberá contar con autenticación basada en API.*
6.12	*Soporte para crear usuarios con formato UPN para autenticación RADIUS.*
6.13	*La solución deberá integrarse con Microsoft Entra ID (Azure Active Directory) para habilitar inicio de sesión único (SSO) en la consola de administración y en el portal de VPN.*
7	***Opciones de VPN base:***
7.1	*La solución de Firewall debe permitir crear túneles VPN IPSec y SSL ilimitados.*
7.2	*La solución de Firewall debe permitir crear VPN de sitio a sitio: SSL, IPSec, AES / 3DES de 256 bits, PFS, RSA, certificados X.509, con clave previamente compartida.*
7.3	***Debe brindar soporte a protocolos L2TP***
7.4	*Debe permitir las VPN basada en rutas.*
7.5	*Debe permitir el acceso remoto con: SSL, IPsec, iPhone / iPad / Cisco / Soporte de cliente VPN de Android.*
7.6	*Debe brindar soporte al protocolo IKEv2 que se utiliza para negociar una asociación de seguridad al principio de una sesión.*
7.7	*La solución debe permitir a los usuarios la descarga del cliente SSL para Windows y la descarga de la configuración a través del portal de usuarios del mismo fabricante.*
7.8	***La solución debe permitir la aplicación de TLS 1.2 y TLS 1.3 para túneles VPN de acceso remoto y sitio a sitio SSL.***
7.9	***La solución debe permitir monitorear el estado de los túneles VPN a través del protocolo SNMP.***
7.10	***La solución debe soportar grupos de intercambio de claves DH14 - DH19 – DH20 - Group 27-30 / RFC6954 para VPNs IPSEC.***
7.11	***La solución debe permitir el uso de claves precompartidas únicas por cada túnel de VPN, de modo que la exposición de una clave no comprometa la seguridad de los demás enlaces.***
7.12	***La funcionalidad de SSL VPN deberá soportar FQDN como host/grupo y establecer TLS 1.2 y TLS 1.3 por defecto en los túneles.***
8	***Cliente VPN***
8.1	*El cliente VPN debe permitir el soporte de IPSec y SSL.*

8.2	*El cliente de VPN debe aprovisionarse e implementarse de una manera sencilla.*
8.3	*La solución de Firewall debe permitir el uso de licencias de acceso remoto SSL ilimitadas incluidas sin cargo adicional.*
8.4	*Debe contar con un túnel dividido inteligente para un enrutamiento óptimo del tráfico.*
8.5	*Debe permitir el soporte NAT-transversal.*
8.6	*El cliente VPN debe permitir al cliente descripción gráfica del estado de la conexión.*
8.7	*El cliente VPN debe contar con soporte para sistema operativos Mac y Windows.*
8.8	*Debe contar con aprovisionamiento de políticas IPSec de acceso remoto con el cliente VPN del mismo fabricante.*
8.09	*La solución debe con soporte grupal para el cliente VPN del mismo fabricante que permita importaciones desde AD / LDAP, etc.*
9	**Prevención de intrusiones (IPS)**
9.1	*La solución deberá proveer un motor de inspección profunda de paquetes IPS de próxima generación y alto rendimiento con patrones IPS selectivos que se permitan aplicar sobre la base de una regla de firewall para obtener el máximo rendimiento y protección.*
9.2	*La solución deberá proveer la protección contra amenazas de día cero.*
9.3	*La solución deberá permitir el soporte para firmas IPS personalizadas.*
9.4	*La solución deberá permitir filtros inteligentes de políticas IPS, esto permite a las políticas dinámicas actualizarse automáticamente a medida que se agregan nuevos patrones.*
10	**Protección Web**
10.1	*La solución debe proveer una protección completamente transparente para antimalware y filtrado web.*
10.2	*La solución debe contar con la protección avanzada contra amenazas mejorada.*
10.3	*La solución debe proveer una base de datos de filtrado de URL con millones de sitios en 92 categorías respaldados por OEMLabs.*
10.4	*La solución debe permitir configurar políticas de tiempo de cuota de navegación por usuario / grupo*
10.5	*La solución debe permitir configurar políticas de tiempo de acceso por*

	usuario / grupo
10.6	*La solución debe permitir configurar el escaneo de malware para bloquear todas las formas de virus, malware web, troyanos y spyware en HTTP / S, FTP y correo electrónico basado en la web.*
10.7	*Protección avanzada contra malware web con emulación de JavaScript.*
10.8	*Búsquedas en la nube en tiempo real para obtener la inteligencia de amenazas más reciente.*
10.9	***La solución deberá permitir Sandbox / Análisis dinámico de malware.***
10.10	*La solución debe permitir el escaneo en tiempo real o en modo por lotes.*
10.11	*La solución debe permitir configurar el escaneo HTTP y HTTPS por usuario o por política de red con reglas y excepciones personalizables.*
10.12	*La solución debe permitir el almacenamiento en caché de contenido web de alto rendimiento.*
10.13	*Filtrado de tipo de archivo por tipo mime, extensión y tipos de contenido activo (por ejemplo, Activex, applets, cookies, etc.)*
10.14	*La solución debe permitir configurar SafeSearch (basada en DNS) para los principales motores de búsqueda por política (usuario / grupo).*
10.15	*La solución debe permitir el bloqueo de aplicaciones potencialmente no deseadas (PUA)*
10.16	*La solución debe permitir configurar el filtrado web automático de sitios identificados por Internet Watch Foundation (IWF) que contienen abuso sexual infantil.*
11	***Visibilidad de Aplicaciones en la Nube***
11.1	*El Firewall deberá mostrar la cantidad de datos cargados y descargados en aplicaciones en la nube categorizadas como nuevas, autorizadas, no autorizadas o toleradas.*
11.2	*La solución debe permitir obtener detalles sobre usuarios, tráfico y datos de una manera profunda.*
11.3	*La solución debe permitir el acceso con un clic a las políticas de configuración del tráfico.*
11.4	*La solución deberá permitir el filtro para el uso de aplicaciones en la nube por categoría o volumen*
11.5	*La solución brindará un informe detallado y personalizable de uso de aplicaciones en la nube para informes históricos.*

11.6	*La solución debe permitir aplicar restricciones de acceso a YouTube en modo educativo por políticas de usuario y grupo.*
12	***Protección y Control de Aplicaciones***
12.1	*La solución debe permitir el control de aplicaciones para identificar, clasificar y controlar automáticamente todas las aplicaciones desconocidas de Windows y Mac en la red al compartir información entre los puntos finales y el firewall.*
12.2	*La solución debe permitir el control de aplicaciones basado en firmas con patrones para miles de aplicaciones.*
12.3	*La solución brindará visibilidad y control de aplicaciones en la nube.*
12.4	*La solución debe permitir configurar filtros inteligentes de control de aplicaciones que habilitan políticas dinámicas que se actualizan automáticamente a medida que se agregan nuevos patrones.*
12.5	*La solución debe permitir configurar control de aplicaciones basado en categoría, características (por ejemplo, ancho de banda y consumo de productividad), tecnología (por ejemplo, P2P) y nivel de riesgo.*
12.6	*La solución debe permitir la aplicación de políticas de control de aplicaciones por reglas de usuario o de red.*
12.7	*La solución debe garantizar la integración con el Endpoint del mismo fabricante con el fin de identificar y sincronizar aplicaciones "desconocidas" que se estén ejecutando en la red permitiendo la administración y control de la misma. El firewall debe permitir al administrador cambiar el nombre y personalizar esas aplicaciones. Asignar aplicaciones a filtros de aplicaciones para controlar su tráfico.*
12.8	*La solución debe permitir aplicar políticas de control de acceso a internet y aplicaciones por usuario o grupo en dispositivos Chromebook.*
12.9	*La solución debe soportar la autenticación con Google Workspace vía LDAP*
12.10	*La solución debe proporcionar mecanismos de descubrimiento y control granular de micro-aplicaciones para mejorar la visibilidad y gestión del tráfico en la red.*
12.11	*La solución debe permitir la limpieza automática de aplicaciones descubiertas que no hayan tenido uso.*
13	***Informes en la Caja***

13.1	*El equipo debe ofrecer como característica el Servicio de correlacionador de eventos en el mismo dispositivo de forma embebida, sin incurrir en un costo adicional. El sistema reportería y correlacionamiento debe residir en el mismo appliance Firewall, no se permitirá una licencia adicional ni ningún equipo (Virtual, Hardware o Cloud) para lograr esta funcionalidad.*
13.2	*Debe contar con informes integrados con opción de personalizar: paneles (tráfico, seguridad y cociente de amenazas del usuario), aplicaciones (riesgo de aplicaciones, aplicaciones bloqueadas, aplicaciones sincronizadas, motores de búsqueda, servidores web, coincidencia de palabras clave web, FTP), red y amenazas (IPS, ATP, inalámbrico, Security Heartbeat, Sandstorm), VPN, correo electrónico, cumplimiento (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)*
13.3	*Monitoreo de actividad actual: estado del sistema, usuarios en vivo, conexiones IPSec, usuarios remotos, conexiones en vivo, clientes inalámbricos, cuarentena y ataques DoS.*
13.4	*Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles.*
13.5	*Capacidad de exportar informes como HTML, PDF, Excel (XLS).*
13.6	*Personalización de la retención de registros por categoría*
13.7	*Visor de registro en vivo con todas las funciones con vista de columna y vista detallada con potentes opciones de búsqueda y filtro, ID de regla con hipervínculo y personalización de la vista de datos*
13.8	*Capacidad de visualizar y almacenar desde la misma consola del firewall*
13.9	*Reporte del nivel de riesgo por usuario, calificando dicho nivel de riesgo en base al comportamiento en Internet del usuario, y al estar ligado a la autenticación, debe poder mostrar el detalle de la información del usuario y su actividad.*
14	**Características Mínimas de Hardware**
14.1	*Memoria de 8 GB DDR4*
14.2	*Disco de Estado Solido (SSD) de al menos 64 GB.*
14.3	*El equipo deberá disponer de un mínimo de 4 puertos Ethernet Gigabit (GE 10/100/1000).*
14.4	*1 x USB 0 en el frente y 1 x USB 0 en la parte trasera.*
14.5	*1 x puerto Consola RJ4*

14.6	*1 x Puerto de administración Micro USB.*

Licenciamiento Firewall (Software)

1	**Características Mínimas de Software**
1.2	*Rendimiento del firewall: 30000 Mbps*
1.3	*Rendimiento del IPS: 6000 Mbps*
1.4	*Rendimiento de la protección contra amenazas: 5000 Mbps*
1.5	*Conexiones concurrentes: 6,5 millones*
1.6	*Nuevas conexiones por segundo: 105000*
1.7	*Inspección SSL/TLS: 1100 Mbps*
2	**Fortalecimiento de la Postura de Seguridad**
2.1	***La solución deberá contar con la capacidad de integrarse o interoperar con la estrategia de seguridad institucional, lo cual deberá permitir: La identificación, análisis y priorización de brechas o vulnerabilidades para un mínimo de 100 activos (entendiendo por activos todos los dispositivos que tengas asignada una dirección IP) presentes en la infraestructura tecnológica de la entidad, tener capacidades para la evaluación continua del riesgo y la visibilidad sobre los activos críticos, permitir la priorización de los hallazgos de seguridad con base en una evaluación dinámica del nivel de riesgo y probabilidad de explotación, correlacionar la información de vulnerabilidades con fuentes de inteligencia de amenazas actualizadas, contar con un API que permita hacer integraciones programáticas y con otras soluciones para intercambio de información.***
2.2	*La solución para el fortalecimiento de la postura de seguridad deberá permitir la configuración de reglas de escaneo avanzadas con soporte para reglas YARA, y contar con mecanismos de autenticación compatibles con estándares de federación y control de acceso, incluyendo SAML 2.0 (por ejemplo, Okta o OneLogin) y Shibboleth 1.3, garantizando una integración segura y centralizada con los sistemas de identidad institucionales.*

2.3	*Debe proporcionarse la capacidad de ejecutar escaneos de auditoría de cumplimiento de configuraciones usando plantillas incluidas por defecto al menos para los siguientes tipos de sistemas: Adtran AOS, Alcatel TiMOS, Amazon AWS, Arista EOS, Blue Coat Proxy SG, Brocade Fabric OS, Check Point GAiA, Cisco ACI, Cisco Firepower, Cisco IOS, Citrix XenServer, Database, Dell Force10 FTOS, Extreme XOS, F5, FireEye, Fortigate Forti OS, HP Procurve, Huawei VRP, IBM iSeries, Juniper Junos, Microsoft Azure, Mobile Device Manager, Mongo DB, NetApp API, Office 365, OpenStack, NetApp Data ONTAP, PAN OS, Rackspace, RHEV, Salesforce.com, SonicWall SonicOS, Unix, VMWare vCenter/vSphere, Watchguard, Windows, ZTE Rosng.*

Implementación Firewall

1	***IMPLEMENTACIÓN***
1.1	*La solución del Firewall debe ser totalmente implementada y configurada.*
1.2.	*Se deberá realizar capacitación a dos (2) usuarios administradores.*
2.	***Equipo de trabajo necesario para la implementación***
2.1	***Gerente de Proyectos: Profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software o áreas afines, con una experiencia general mínima de 3 años, contada a partir de la expedición de la tarjeta profesional, y con especialización en Gestión de Proyectos de Ingeniería o disciplinas relacionadas.*** ***Así mismo, deberá acreditar al menos dos (2) de las siguientes certificaciones vigentes:*** ***-Certificación como gerente de proyectos PMP-PMI*** ***-Certificación en gestión de riesgos PMI-RMP*** ***-Auditor Líder ISO 27001:2022.***

2.2	***Ingeniero de Ciberseguridad: Profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software o áreas afines, con una experiencia general mínima de cinco (5) años, contada a partir de la expedición de la tarjeta profesional.*** ***Deberá contar con al menos dos (2) de las siguientes certificaciones:*** ***-CCNP (Cisco Certified Network Professional).*** ***-Certificación en Control de Riesgos y Sistemas de Información*** ***-Certificación en Web Application Scanner*** ***-Certificación en Vulnerability Management Detection and Response*** ***-Certificación en operación y/o administración de firewalls emitida por el fabricante de soluciones de ciberseguridad.***
2.3	***Ingeniero de Soporte:*** *Profesional con título profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software o profesiones afines, con experiencia profesional general mínima de tres (3) años, contados a partir de la fecha de expedición de la tarjeta profesional..* *Deberá contar con al menos dos (2) de las siguientes certificaciones:* *-Certificación en operación y/o administración de firewalls emitida por el fabricante de soluciones de ciberseguridad.* *-Certificación como especialista en seguridad en la nube emitida por fabricante de soluciones de ciberseguridad.* *-Formación como Auditor ISO 27001:2022 o ISO 20000 o CTIA*

<u>Garantía y Soporte</u>

1.	***Garantía y Soporte***
1.1	*Garantía de hardware y RMA con intercambio avanzado.*
1.2	*Soporte 24x7 por teléfono y correo electrónico.*
1.3	*Actualizaciones y mejoras GRATUITAS de funciones de software*
1.4	*El fabricante de las soluciones deberá proveer soporte 7x24 con*

	escalamiento técnico y de producto.
1.5	*Deberá contar con soporte y licenciamiento por un periodo de veinticuatro (24) meses.*

.”.

Las demás estipulaciones del Documento Adicional y demás documentos publicados NO MODIFICADOS, se mantienen como se expidieron originalmente.

Dado en Bogotá D.C., el 21 de noviembre de 2025.

YANNY LUGDY CARRION PEDRAZA
Directora Administrativa y Financiera
Ordenadora del Gasto

Proyectó: Juan José Hernández Acosta- Abogado - Contratista
Revisó: Sol Ángel Cala Acosta – Directora de Contratación.
Revisó: Darío Sotelo – DAF