FICHA TÉCNICA / CONDICIONES TÉCNICAS MINIMAS - FORTINET

Las condiciones del servicio requerido para el presente proceso de selección están relacionadas con el cumplimiento del alcance descrito a continuación:

1. OBJETO.

"ADQUIRIR INFRAESTRUCTURA EN SEGURIDAD PERIMETRAL DE LA INFORMACIÓN PARA LA FEDERACIÓN COLOMBIANA DE MUNICIPIOS EN CUMPLIMIENTO DE LA FUNCIÓN PÚBLICA ASIGNADA."

2. CONDICIONES TÉCNICAS MÍNIMAS REQUERIDAS.

la Federación Colombiana de Municipios, en el marco de su estrategia de modernización tecnológica y fortalecimiento de su postura de ciberseguridad, requiere la adquisición e implementación de una solución integral de seguridad perimetral basada en tecnología Next Generation Firewall (NGFW), desplegada bajo un esquema de alta disponibilidad (HA) y complementada con una plataforma centralizada de análisis, correlación y gestión de logs, operando de forma integrada y nativa.

La infraestructura de seguridad solicitada tiene como objetivo proporcionar capacidades avanzadas de prevención, detección y respuesta ante amenazas, mediante la inspección profunda de tráfico a nivel de capa 7, control granular de aplicaciones, sistemas de prevención de intrusiones (IPS), filtrado web y DNS, descifrado de tráfico SSL/TLS y mecanismos de autenticación basados en identidad.

Asimismo, la plataforma de análisis de logs permitirá la recolección, normalización, correlación y generación de eventos de seguridad, facilitando la trazabilidad, la auditoría y el análisis forense de incidentes.

El objetivo es:

- Fortalece la postura de ciberseguridad institucional, incorporando capacidades avanzadas de prevención, detección y respuesta.
- Garantiza continuidad operativa, mediante esquemas de alta disponibilidad y redundancia.
- Mejora la visibilidad y control del tráfico, permitiendo toma de decisiones basada en analítica.
- Asegura cumplimiento normativo y mejores prácticas internacionales.
- Permite escalabilidad y adaptación tecnológica futura, alineándose con tendencias como Zero Trust y transformación digital.

Con lo expuesto anteriormente la Federación Colombiana de Municipios en cumplimiento de la función pública asignada se ve en la necesidad de estar a la vanguardia con las últimas tecnologías existentes en seguridad perimetral en mercado, se busca la adquisición de una nueva solución en seguridad perimetral, así como la renovación y actualización de los

componentes asociados, como parte de una estrategia integral de gestión de riesgos tecnológicos y continuidad del negocio.

El presente proceso se origina como consecuencia de la obsolescencia tecnológica y la finalización del ciclo de soporte de los equipos de seguridad perimetral y conectividad marca Fortinet actualmente implementados en la infraestructura tecnológica de la entidad, los cuales requieren renovación para garantizar la continuidad operativa, el rendimiento de la red y el fortalecimiento de los controles de ciberseguridad.

Los equipos objeto del presente proceso son los siguientes:

Equipo	Cantidad	Marca	Serial
Firewall-500E	**2**	**Fortinet**	**FG5H0E5819902626 FG5H0E5819902620**
Analyzer 200F	**1**	**Fortinet**	**FL-2HFTB19000015**
AP 421E	**2**	**Fortinet**	**FP421ETF19025615 FP421ETF19025613**

La infraestructura tecnológica objeto de la presente solicitud deberá garantizar, de manera nativa y sin requerir integraciones adicionales de terceros, la interoperabilidad, compatibilidad y correcta coexistencia con los equipos y componentes actualmente en operación que no serán contemplados dentro del alcance de renovación del presente proyecto.

Asimismo, la solución propuesta deberá asegurar la continuidad de los servicios, la integración funcional y la estabilidad operativa de la plataforma tecnológica existente, evitando afectaciones en la conectividad, seguridad, administración y desempeño de la infraestructura.
Los equipos que permanecerán en operación y con los cuales se deberá garantizar compatibilidad e integración son los siguientes:

Equipo	Cantidad	Marca
EMS	**1**	**Fortinet**
AP 231F	**9**	**Fortinet**

Los equipos objeto de renovación deberán contar con capacidades técnicas y tecnológicas iguales o superiores a las actualmente implementadas, garantizando un mejor desempeño, mayor eficiencia operativa, compatibilidad con la infraestructura existente y fortalecimiento de la continuidad y seguridad de los servicios tecnológicos.

FICHA TÉCNICA:

A continuación, se presenta la tabla con la especificación de equipos a adquirir:

1. ADQUISICIÓN DE UNA SOLUCIÓN DE PROTECCIÓN PERIMETRAL		
Denominación técnica:		Firewall de seguridad perimetral
Cantidad:		2 equipos NGFW en HA
ÍTEM	**Característica**	**REQUERIMIENTO TÉNICOS MINIMOS**
1.1	Generalidades	Se necesita una solución de protección perimetral con una solución de propósito especifico tipo appliance en HA para la sede principal de la entidad. La solución ofertada en el presente proceso debe ser monomarca y plataforma debe integrarse de manera nativa 100% sin desarrollos adicionales con la solución WIFI que tiene la entidad desde donde se administra la solución de conectividad actual brindando acceso seguro a los usuarios de la entidad, se requiere tener una arquitectura donde se pueda tener información consolidada de topología física y lógica, amenazas existentes, y estadísticas de seguridad en general.
1.2	Características generales	La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo. Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos. 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. La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7. 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. La gestión de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red. Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding. Los dispositivos de protección de red deben soportar

		encaminamiento de multicast (PIM-SM y PIM-DM). Los dispositivos de protección de red deben soportar DHCP Relay. Los dispositivos de protección de red deben soportar DHCP Server. Los dispositivos de protección de red deben soportar sFlow. Los dispositivos de protección de red deben soportar Jumbo Frames. Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas. Debe ser compatible con NAT dinámica (varios-a-1). Debe ser compatible con NAT dinámica (muchos-a-muchos). Debe soportar NAT estática (1-a-1). Debe admitir NAT estática (muchos-a-muchos). Debe ser compatible con NAT estático bidireccional 1-a-1. Debe ser compatible con la traducción de puertos (PAT). Debe ser compatible con NAT Origen. Debe ser compatible con NAT de destino. Debe soportar NAT de origen y NAT de destino de forma simultánea. Debe soportar NAT de origen y NAT de destino en la misma política Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico. Debe ser compatible con NAT64 y NAT46. Debe implementar el protocolo ECMP. Debe soportar SD-WAN de forma nativa Debe soportar el balanceo de enlace hash por IP de origen. Debe soportar el balanceo de enlace por hash de IP de origen y destino. 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. Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales. 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. Enviar logs a sistemas de gestión externos simultáneamente. Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL. Debe soporta protección contra la suplantación de identidad

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica

		(anti-spoofing). Implementar la optimización del tráfico entre dos dispositivos. Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP). Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3). Soportar OSPF graceful restart. Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red. Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico. Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico. Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3. Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster. La configuración de alta disponibilidad debe sincronizar: Sesiones. La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red. La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN. En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace. Debe soportar la creación de sistemas virtuales en el mismo equipo. Para una alta disponibilidad, el uso de clúster virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos. 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. 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. Control, inspección y descifrado de SSL para tráfico entrante

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica

		(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). Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red. El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.
1.3	Características de Firewall	Debe soportar controles de zona de seguridad. Debe contar con políticas de control por puerto y protocolo. 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. Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad. Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad. Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall. Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública. Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF). La solución debe permitir la implementación sin asistencia de SD-WAN En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN.
1.4	Control Aplicaciones	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo. Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico.

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica

		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. 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. 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. Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas. Actualización de la base de firmas de la aplicación de forma automática. Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos. Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas. 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. El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos. Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo. Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo. Debe permitir la diferenciación y manejo de las aplicaciones de chat. por ejemplo, permitir a Hangouts el chat pero impedir la llamada de video. Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo. 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,

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica

		Browse Based, Network Protocol, etc.). Debe ser posible crear grupos dinámicos de aplicaciones basados en características de estas, tales como: Nivel de riesgo de la aplicación. Debe ser posible crear grupos estáticos de aplicaciones basadas en características de estas, tales como: Categoría de Aplicación. Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente.
1.5	Prevención de Amenazas	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo. Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware). 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. Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad. 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. Deber permitir el bloqueo de vulnerabilidades y exploits conocidos Debe incluir la protección contra ataques de denegación de servicio. Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo. Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo. Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP. Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP. Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets). Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc. Detectar y bloquear los escaneos de puertos de origen. Bloquear ataques realizados por gusanos (worms) conocidos. Contar con firmas específicas para la mitigación de ataques DoS y DDoS.

		Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow). Debe poder crear firmas personalizadas en la interfaz gráfica del producto. Identificar y bloquear la comunicación con redes de bots. 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. Debe ser compatible con la captura de paquetes (PCAP), mediante la 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. Los eventos deben identificar el país que origino la amenaza. Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms). Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP. 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.
1.6	Filtrado 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). 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. Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL. 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. Tener por lo menos 75 categorías de URL. Debe tener la funcionalidad de exclusión de URLs por categoría. Permitir página de bloqueo personalizada. Permitir bloqueo y continuación (que permita al usuario acceder

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

		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). Además del Explicit Web Proxy, soportar proxy web transparente.
1.7	Identidad de Usuario	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. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc. Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios. Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios. 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). 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. Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD. Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
1.8	Calidad de Servicio (QoS y 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. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino. Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo. Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube. Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto. En QoS debe permitir la definición de tráfico con ancho de banda garantizado. En QoS debe permitir la definición de tráfico con máximo ancho de banda. En QoS debe permitir la definición de colas de prioridad. Soportar marcación de paquetes DiffServ, incluso por aplicación. Soportar la modificación de los valores de DSCP para Diffserv. Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service). Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.
1.9	DLP	Permite la creación de filtros para archivos y datos predefinidos. Los archivos deben ser identificados por tamaño y tipo. Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones. Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
1.10	Geo IP	Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países. Debe permitir la visualización de los países de origen y destino en los registros de acceso. Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.
1.11	VPN	Soporte VPN de sitio-a-sitio y cliente-a-sitio. Soportar VPN IPSec. Soportar VPN SSL.

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica

		La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512 La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14. La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2). La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard). Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec. Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting. 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. 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. Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL. Deberá mantener una conexión segura con el portal durante la sesión.
1.12	Características Firewall	FW Throughput (64 bytes) [Gbps]: 144 IPS Throughput (Gbps): 37 Concurrent Sessions (TCP): 27 Millon New Sessions/Second (TCP): 690.000 IPsec VPN Throughput (512 byte) [Gbps]: 55 Gateway-to-Gateway IPsec VPN Tunnels: 2000 Client-to-Gateway IPsec VPN Tunnels: 50000 SSL-VPN Throughput [Gbps]: 7,6 Gbps IPS Throughput (Enterprise Mix): 38 Gbps SSL Inspection Throughput (IPS, avg. HTTPS) [Gbps]: 14 Application Control Throughput (HTTP 64K) [Gbps]: 48 NGFW Throughput [Gbps]: 29 Threat Protection Throughput [Gbps]: 25 Interfaces Rj45: 8 Interfaces 1GE SFP: 16 Interfaces 10GE SFP+: 4 25/10GE SFP Interfaces: 4 Doble Fuente de poder Certificado USGv6/IPv6

2. ADQUISICIÓN DE UNA SOLUCIÓN DE ANÁLISIS DE LOGS		
Denominación técnica:		Solución de Análisis de Logs
Cantidad:		1 equipo hardware de análisis de logs.
ÍTEM	**Característica**	**REQUERIMIENTO TÉNICOS MINIMOS**
2.1	Generalidades	• Sistema de almacenamiento de logs y reportes con Sistema operativo propietario, interfaz gráfica vía HTTPS y acceso CLI por SSH. • Capacidad de definir dominios administrativos (ADOMs) y múltiples roles de administradores para segmentar la operación. • Integración segura de dispositivos Firewall del mismo fabricante. • Arquitectura escalable con roles de recolector y analizador para optimizar el manejo y procesamiento de logs. • Posibilidad de asignar espacio de almacenamiento específico a cada instancia (virtual o física) y alertas cuando se alcanza un umbral. • Visualización en tiempo real de logs y exportación en formatos • Generación de bitácoras de auditoría con cambios administrativos y hora. • Capacidad de replicar reportes existentes para modificarlos, exportar logs, crear filtros y personalizar gráficos y tablas. • Envío automático de logs a servidores externos (FTP/SFTP) y notificaciones de eventos por correo electrónico, SNMP o Syslog. • Dashboards personalizables que muestren tráfico, categorías de URL, amenazas y servicios, con indicadores de compromiso para usuarios finales. • Herramientas de diagnóstico de rendimiento y visualización del estado del sistema • Compatibilidad con IPv4 e IPv6 y con formatos de registro estándar como syslog, CEF y LEEF. • Políticas de retención de datos configurables por tipo de log y por dispositivo. • Sincronización horaria con NTP y registro de logs con sello de tiempo preciso. • Soporte para autenticación externa mediante LDAP/Active Directory o RADIUS.

		• Integración con SNMP para envío de traps y supervisión por herramientas de monitoreo.
2.2	Generación de reportes	• Personalizar el contenido de los reportes (tablas y gráficos) y criterios de filtrado (fuentes, destinos, servicios, periodos relativos y absolutos). • Programar reportes y enviarlos automáticamente a múltiples destinatarios por correo electrónico. • Disponibilidad de exportación en formatos PDF y/ó HTML y/ó XML y/ó CSV y envío a repositorios externos. • Soporte de múltiples idiomas (español e inglés) y personalización de portada, logotipos, colores y diseño (gráficos, texto, imágenes). • Capacidad de clonar y modificar reportes existentes para ajustarlos a las necesidades del cliente. • Reportes de utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y servicios con mayor consumo. • Reportes de ataques detectados/detenidos con mayor frecuencia, por fuente y/o destino. • Reportes de páginas y categorías de URL visitadas con mayor frecuencia. • Reportes sobre virus detectados/removidos a nivel de red, por fuente y/o destino. • Reportes de actividades administrativas (ingresos de administradores, cambios de configuración). • Personalización de criterios de obtención de reportes: fuentes, destinos, servicios, fechas y días de la semana. • Especificación de periodos de tiempo (hoy, ayer, esta semana, semana pasada, mes actual, mes anterior) o periodos absolutos. • Capacidad de calendarizar reportes con periodicidad variable (horaria, diaria, semanal, mensual). • Envío automático de reportes a servidores SFTP o FTP o correo . • Inclusión de gráficos variados: barras, líneas, pastel y tablas comparativas. • Reportes de rendimiento de dispositivos, top aplicaciones y usuarios con mayor ancho de banda. • Reportes de reputación de IP/URL y seguridad web. • Reportes de tráfico VPN (usuarios conectados, duración de sesiones). • Reportes de uso de aplicaciones SaaS y seguridad de correo electrónico. • Reportes de sandboxing, antispam e integridad de

		archivos. • Reportes de actividad de usuarios privilegiados y contraseñas débiles. • Capacidad de generar informes de tendencias y pronósticos a partir de datasets • Exportación de datos a plataformas de Business Intelligence para análisis adicional. • Creación de bibliotecas de reportes reutilizables y compartirlas entre administradores.
2.3	Características mínimas de desempeño	• Soporte para compresión de logs y cifrado de datos en reposo. • Purgado automático de logs según políticas de ciclo de vida y requisitos regulatorios. • Visualización del uso de disco por tipo de log y por dominio administrativo, con alertas de espacio disponible. • Notificaciones cuando el almacenamiento disponible alcance umbrales configurables. Integración con soluciones de respaldo para copias periódicas de datos. • Programación de tareas de limpieza y optimización de índices fuera de horario productivo. • Registro de metadatos asociados a cada log almacenado (origen, destino, tamaño, duración u otros atributos disponibles). • Monitorización del rendimiento del almacenamiento y del sistema. • Capacidad de procesamiento de logs hasta 100 GB por día.
2.4	Almacenamiento	• Debe contar con almacenamiento local de alto desempeño y políticas de retención configurables. • Storage: 8 TB (2x 4 TB) • Storage usable después de RAID 4
2.5	Características FAZ	• GB/ day of Logs: 100 • Máximo número de días de analítica: 50 • Storage: 8 TB (2x 4 TB) • Storage usable después de RAID 4 TB • El equipo debe ser monomarca y con Integración Nativa con equipos de seguridad perimetral Next Generation Firewall • Indicadores de Compromiso

3. ADQUISICIÓN DE UNA SOLUCIÓN DE ACCESS POINTS

Denominación técnica:		Equipos AP (Access Points o Puntos de Acceso)
Cantidad:		2 equipos AP
ÍTEM	**Característica**	REQUERIMIENTO TÉNICOS MINIMOS
3.1	Generalidades	equipos existen 2 equipos que deben ser actualizados tecnológicamente ya que se encuentran en fin de ciclo de vida. • FP421ETF19025615 • FP421ETF19025613 Estos dos (2) equipos deben ser actualizados tecnológicamente y se esperan como mínimo las siguientes capacidades. • Tipo: Indoor AP • Numero de Radios: 3 Wi-Fi + 1BLE • Numero de Antenas: 6. x2 Dual band Wi-Fi + x2 6GHz band Wi-Fi + x1 BLE/ ZigBee antenna + x1 GPS antena • 2x2 Indoor Tri-radio 11be 6Ghz Capable AP • Velocidad de datos máxima: Banda 2.4GHz: Hasta 688 Mbps. Banda 5.0GHz: Hasta 2.882 Gbps. Banda 6.0GHz: Hasta 5.765 Gbps • Interfaces: x1 100M/1000M/2.5G/5.0G Multigigabit Ethernet (RJ45) x1 RS 232 RJ45 Serial Port. • SSID simultáneos: Hasta 8 por radio cliente (7 si el escaneo en segundo plano está habilitado). • Tipos de EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST, EAP-TTLS/PAP. • Autenticación de usuario/dispositivo: WPA™, WPA2™ y WPA3™ con 802.1x o clave precompartida, WEP, portal cautivo web, lista negra y lista blanca de direcciones MAC. • Capacidad de clientes por radio: Hasta 512 clientes por radio (Radio1, Radio2, and Radio3) • Potencia máxima de transmisión (conducida): 2.4GHz band: 26 dBm/400 mW (2 cadenas combinadas) 5.0GHz band: 23 dBm/200 mW (2 cadenas combinadas) 6.0GHz band: 22 dBm/158 mW (2 cadenas combiandas@320MHz BW) • Estándares IEEE: 802.11a, 802.11b, 802.11be, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.11ax, 802.11mc, 802.1X, 802.3af, 802.3at, 802.3bt, 802.3az, 802.1Q, 802.11u, 802.11w, 802.3bz • CPU/RAM: Quad-core ARM Cortex-A53 1.5GHz / 2

		GB • Wi-Fi7 Certified: Certificado. • DFS: Europe, FCC, Japan, Australia, N, Taiwan, S. Korea, India. • Los equipos deben ser mono marca y con Integración Nativa con equipos de seguridad perimetral Next Generación Firewall. • El equipo debe ser mono marca y con Integración Nativa con equipos de seguridad perimetral Next Generation Firewall, con el beneficio de poder ser gestionados y administrados desde un único punto.
3.2	LICENCIAMIENTO Y SOPORTE PARA PROTECCION DE ENDPOINT	12 meses

4. SERVICIOS DE IMPLEMENTACION Y SOPORTE		
Denominación técnica:		CONFIGURACIÓN, INSTALACIÓN Y PUESTA EN MARCHA.
Cantidad:		12 meses
ÍTEM	**Característica**	REQUERIMIENTO TÉNICOS MINIMOS
4.1	SOPORTE Y GARANTÍA DE FÁBRICA	Se requiere contrato de soporte y mantenimiento directo con fábrica en la modalidad 7X24 para cada una de las tecnologías ofertadas por 1 año. El soporte debe ser en un esquema 7x24 incluyendo actualizaciones de firmware, acceso al portal de soporte del fabricante y recursos técnicos y base de conocimiento del Fabricante.
4.2	SERVICIOS DE SOPORTE LOCAL POR EL CONTRATISTA	El contratista deberá atender y resolver cualquier problema técnico de la solución, en un esquema de atención 7X24 (telefónico, e-mail, acceso remoto o presencial en caso de que así se requiera), este soporte deberá ser suministrado por personal especializado en la herramienta ofertada. El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil. Para ello debe contar con un centro de servicio que cumpla con mínimo: Software de Mesa de Servicio, donde se puedan registrar casos o incidentes de forma web, correo o teléfono.

		Nivel de soporte 1 para atención remota, 2 para atención en sitio y 3 para soporte de especialista y escalamiento a fábrica. Al finalizar cada visita correctiva y el contratista generará un informe de servicio con las evidencias de estas actividades. De igual forma quedará constancia en la misma acta o informe de servicio si hubo cambio de software y/o en alguna configuración.
4.3	SERVICIOS DE IMPLEMENTACIÓN	El contratista deberá realizar el levantamiento de información, arquitectura e implementación, y puesta en producción de las herramientas ofertadas. Se deberá definir la arquitectura de la implementación con el supervisor del contrato o el personal de apoyo a la supervisión. Se deben realizar las respectivas pruebas de funcionalidad y operatividad de todos los elementos ofertados. El contratista deberá presentar un plan y cronograma de trabajo de acuerdo con la arquitectura aprobada con el supervisor del contrato o el personal de apoyo a la supervisión. **Transferencia de conocimiento:** El contratista deberá realizar una trasferencia de conocimiento a los Ingenieros de la dirección de tecnología de la entidad de las tecnologías ofertadas.

3. LA FORMA DE PAGO:

La Federación Colombiana de Municipios cancelará el valor total del contrato, así:

El valor del contrato será pagado por la Federación Colombiana de Municipios al Contratista en un solo pago, una vez el supervisor del contrato recibe los bienes, certificación del licenciamiento y soporte contratado de los equipos tecnológica por un año, adquirida por la Federación Colombiana de Municipios en cumplimiento de la función pública asignada.

4. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de DOS (2) MESES de ejecución, contado a partir del cumplimiento de los requisitos de ejecución, sin que sobrepase el 27 de diciembre de 2026.

El acceso al licenciamiento debe ser de doce (12) meses, contados a partir del recibo a satisfacción por parte del supervisor del contrato, una vez se reciban los equipos.

5. CLASIFICADOR DE BIENES Y SERVICIOS – UNSPSC

El bien o servicio objeto del presente proceso de selección está codificado en el clasificador de Bienes y Servicios UNSPSC, como se indica a continuación:

SEGMENTO	FAMILIA	CLASE	NOMBRE
43	4323	43233200	Software de seguridad y protección

43	4322	43222500	Equipos de seguridad red

6. GARANTÍAS.

- Cumplimiento del contrato: Equivalente al diez por ciento (10%) del valor total del contrato, por un término igual al plazo del contrato y seis (6) meses más.

- Calidad y correcto funcionamiento de los bienes: Equivalente al diez por ciento (10%) del valor total del contrato, por un término igual al plazo del contrato y seis (6) meses más.

- Calidad del servicio: Equivalente al diez por ciento (10%) del valor total del contrato, por un término igual al plazo del contrato y seis (6) meses más.

- Pago de salarios, prestaciones sociales e indemnizaciones laborales: Equivalente al cinco por ciento (5%) del valor total del contrato, por un término igual al plazo del mismo y tres (3) años más.

I) OBLIGACIONES DEL CONTRATISTA

a) Obligaciones Generales

1) Cumplir con el objeto contratado de acuerdo con los requerimientos definidos por la Entidad.
2) Cumplir oportunamente con todas las exigencias y procedimientos establecidos para la firma electrónica de los contratos y sus modificaciones en la plataforma de SECOP II.
3) Publicar para cada pago en la plataforma del Sistema Electrónico de Contratación Pública SECOP II los informes y/o productos de ejecución contractual, con los soportes, si hubiere lugar a ellos, de acuerdo con lo estipulado en la Ley 1712 de 2014, o en la plataforma que corresponda.
4) Asistir a las reuniones programadas, relacionadas con la ejecución del objeto contractual.
5) Presentar los informes que el supervisor del contrato solicite en desarrollo del objeto contractual.
6) Acatar las directrices establecidas por la Federación Colombiana de Municipios la Función Pública en cuanto a los trámites para el cobro de los valores pactados en el presente contrato, cumpliendo los requisitos y fechas definidas por la entidad.
7) Mantener al día sus pagos en el Sistema General de Seguridad Social Integral y entregar antes de cada pago, copia de la planilla correspondiente al supervisor del contrato, si se trata de personas naturales, o entregar para cada pago, la certificación suscrita por el representante legal o revisor fiscal, que acredite el cumplimiento del pago de aportes al Sistema de Seguridad Social Integral, parafiscales, ICBF, SENA y cajas de compensación familiar de los últimos seis (6) meses.
8) Aplicar durante la ejecución del contrato, los lineamientos establecidos en el Sistema de de Calidad de la Entidad.
9) Reportar al supervisor del contrato, novedades o anomalías relacionadas con la ejecución contractual.

10) Responder por las actuaciones u omisiones derivadas de la celebración del contrato y de la ejecución del mismo, de conformidad con lo establecido en la Ley 80 de 1993.
11) No acceder a peticiones o amenazas de quienes actúen por fuera de la Ley con el fin de obligarlos a hacer u omitir cualquier acto o hecho.
12) Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y entrabamientos que puedan presentarse y, en general, cumplir con lo establecido en la Ley 80 de 1993, la Ley 1150 de 2007, Ley 1474 de 2011, sus reformas y decretos reglamentarios.
13) EL CONTRATISTA autoriza a LA FEDERACIÓN l tratamiento de datos personales para dar cumplimiento con lo establecido en la Ley 1581 de 2012, reglamentada parcialmente por los Decretos 1377 de 2013 y 1081 de 2015, y el Decreto 255 de 2022 y demás normas que los modifiquen, complementen o sustituyan; en total conocimiento, entendimiento y aceptación de la política de datos, disponible en https://www.fcm.org.co/politica-de-datos/
En consecuencia, autoriza de manera libre, expresa, voluntaria y debidamente informada a LA FEDERACIÓN para dar tratamiento a los datos que han sido suministrados y que se han incorporado en las distintas bases de datos con el ánimo de garantizar la seguridad de su información y el ejercicio de sus derechos y el desarrollo de su actividad.
14) Las demás que se deriven del artículo 5° de la Ley 80 de 1993, así como todas aquellas que señalen la Constitución y la Ley y que tengan relación directa con el objeto del contrato.

a) Obligaciones Especificas

1) El proveedor se compromete a entregar los equipos y a habilitar el licenciamiento y acceso al hardware y entregar las credenciales de acceso correspondientes dentro de un plazo no mayor a cuarenta y cinco días hábiles siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato. la entrega de los equipo, así como la habilitación del licenciamiento y el acceso se considerará como entrega.
2) El oferente deberá suministrar, instalar, configurar y poner en operación la totalidad de la infraestructura tecnológica requerida, garantizando el cumplimiento integral de las especificaciones técnicas mínimas establecidas en la presente solicitud de cotización.
3) El oferente deberá garantizar que la solución ofertada sea monomarca y cuente con integración nativa con la infraestructura Fortinet actualmente implementada en la entidad, asegurando interoperabilidad, compatibilidad y coexistencia operativa sin requerir desarrollos adicionales de terceros.
4) El oferente deberá implementar la solución de seguridad perimetral bajo un esquema de alta disponibilidad (HA), garantizando redundancia, continuidad operativa y sincronización de configuraciones, sesiones y políticas de seguridad entre los equipos instalados.
5) El oferente deberá realizar el levantamiento de información, validación de arquitectura, diseño técnico, parametrización, migración, pruebas funcionales y puesta en producción de la solución ofertada, minimizando riesgos e impactos sobre la operación de los servicios tecnológicos de la entidad.
6) El oferente deberá garantizar que todos los equipos, licencias, suscripciones y componentes suministrados sean nuevos, originales, no remanufacturados y provenientes directamente del fabricante o de canales autorizados, incluyendo el respectivo soporte y garantía de fábrica.

7) El oferente deberá prestar soporte técnico especializado en modalidad 7x24 durante la vigencia contractual, incluyendo atención remota y presencial, escalamiento a fábrica, actualización de firmware, soporte correctivo, resolución de incidentes y acompañamiento técnico especializado
8) El oferente deberá suministrar y mantener vigentes durante el tiempo contratado las licencias, suscripciones, firmas de seguridad, servicios de actualización, soporte técnico y demás componentes requeridos para el correcto funcionamiento de la solución de ciberseguridad implementada.
9) El oferente deberá ejecutar pruebas de funcionamiento, rendimiento, conectividad, seguridad, alta disponibilidad, integración y estabilidad de la solución instalada, entregando las respectivas evidencias técnicas y actas de aceptación por parte de la supervisión del contrato.
10) El oferente deberá entregar la documentación técnica y administrativa de la solución implementada, incluyendo diagramas de arquitectura física y lógica, configuraciones aplicadas, direccionamiento, políticas de seguridad, respaldos de configuración, manuales técnicos y memorias de implementación.
11) El oferente deberá realizar transferencia de conocimiento y capacitación técnica al personal certificada por el fabricante, designado por la Federación Colombiana de Municipios, respecto a la administración, operación, monitoreo, soporte y buenas prácticas de la solución tecnológica implementada
12) El oferente se compromete al cumplimiento incondicional de la ficha técnica de los requerimiento establecidos en la ficha técnica.

b) OBLIGACIONES DE LA FEDERACIÓN:

1) Pagar a EL CONTRATISTA el valor convenido posterior a la presentación de cada entregable y cumplimiento de actividades, previa verificación y certificación por parte del supervisor.
2) Entregar oportunamente o poner a disposición de EL CONTRATISTA los elementos, documentos, datos e informes necesarios para el eficiente y eficaz cumplimiento del objeto contractual.
3) Exigir a EL CONTRATISTA la calidad en los servicios prestados objeto del contrato.
4) Exigir a EL CONTRATISTA la ejecución idónea y oportuna del objeto del contrato.
5) Adelantar las gestiones necesarias para el reconocimiento y pago de las sanciones pecuniarias y garantías a que hubiere lugar.

Nota: Cuando haya lugar a la modificación del plazo o valor consignado en el contrato LA CONTRATISTA deberá constituir los correspondientes certificados o anexos de modificación de las garantías, sin perjuicio de la obligación que le asiste al tomador de mantener informada a la aseguradora de cualquier modificación del estado de riesgo amparado. Así mismo, será de cargo de LA CONTRATISTA el pago de todas las primas y demás erogaciones de constitución, mantenimiento y restablecimiento inmediato de su monto, cada vez que se disminuya o agote por razón de las sanciones que se impongan, por sus prórrogas o suspensiones.