OBJETO ADQUIRIR DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW CON INSTALACIÓN, SOPORTE Y MANTENIMIENTO INTEGRADO CON LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL ACTUAL DE LA CNSC.		
1.1. SUBÍTEM: EQUIPO SEGURIDAD PERIMETRAL		
DENOMINACIÓN TÉCNICA:		**ADQUISICION DE EQUIPOS DE SEGURIDAD PERIMETRAL DE NUEVA GENERACION, PARA EL FORTALECIMIENTO TECNOLOGICO DE LA ENTIDAD.**
CANTIDAD:		**Dos (2) FWNG + Uno (1) Gestor de Eventos**
UNIDAD DE MEDIDA:		**Unidad**
ÍTEM	**CARACTERÍSTICA**	**MINIMO REQUERIDO**
1.1.1	**EQUIPOS DE SEGURIDAD PERIMETRAL**	
1.1.1.2	**Aspectos generales**	La Comisión Nacional del Servicio Civil cuenta actualmente con dos Equipos de seguridad perimetral Fortinet 2500E, los cuales se encuentran funcionando en el siguiente esquema, uno en el Datacenter de Colombia XV donde se encuentra toda la infraestructura de servidores y servicios expuestos a Internet. El otro equipo se encuentra en la sede principal donde están los usuarios que hacen uso de los diferentes recursos tecnológicos de la Entidad y se interconectan mediante un enlace MPLS, estos dos equipos deben quedar configurados por parte del contratista en un esquema en alta disponibilidad y esta solución se dejara en el Datacenter de Colombia VX. Como complemento de la arquitectura detallada anteriormente la entidad requiere fortalecer el esquema de seguridad perimetral con la Adquisición de Dos (2) appliances con sistema operativo propietario del fabricante, que sea del tipo Firewall de Nueva Generación, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento. La solución debe estar en la capacidad de soportar alta disponibilidad y de enviar todos los logs de eventos a la solución de gestión y análisis de seguridad con la que se cuenta actualmente FAZ400E. La solución debe estar en la capacidad de soportar alta disponibilidad. El dispositivo debe ser equipos de propósito específico. El dispositivo debe contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de tráfico.

OBJETO ADQUIRIR DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW CON INSTALACIÓN, SOPORTE Y MANTENIMIENTO INTEGRADO CON LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL ACTUAL DE LA CNSC.		
1.1. SUBÍTEM: EQUIPO SEGURIDAD PERIMETRAL		
DENOMINACIÓN TÉCNICA:		**ADQUISICION DE EQUIPOS DE SEGURIDAD PERIMETRAL DE NUEVA GENERACION, PARA EL FORTALECIMIENTO TECNOLOGICO DE LA ENTIDAD.**
CANTIDAD:		**Dos (2) FWNG + Uno (1) Gestor de Eventos**
UNIDAD DE MEDIDA:		**Unidad**
ÍTEM	**CARACTERÍSTICA**	**MINIMO REQUERIDO**
1.1.1.3	**Características**	La solución deberá pertenecer al cuadrante de líder de gartner para Hybrid Mesh Firewalls (HMF). El dispositivo debe brindar las funcionalidades de: Firewall, IPS, Control de Aplicaciones, Filtrado Web, Antivirus perimetral, SDWAN, DLP, prevención de Malware en línea con base en Inteligencia Artificial, CASB inline, protección de Malware, Filtrado de URL/DNS/Video, Anti-spam, Calificaciones de seguridad, conformidad y riesgo, detección de IoT y correlación de vulnerabilidades de IoT y conector SASE para acceso privado seguro (SPA) incluidas en el licenciamiento solicitado. Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad podrá dar seguimiento a los casos abiertos por el oferente. La solución debe contar con Fuente de poder redundante incluida en la oferta no por separado. Se deberá proporcionar una cuenta de acceso al portal oficial de educación del fabricante, donde la Entidad podrá acceder, de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías del fabricante. La solución deberá estar calificada como recomendada en el SVM de firewall de NSS LABS. Los equipos deben contar con tecnología de Modulo de plataforma confiable (TPM).
1.1.1.4	**Rendimiento**	El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales: · Rendimiento de Firewall IPV4 / IPV6 139 Gbps · Rendimiento de IPS 14 Gbps · Rendimiento de NGFW (FW+IPS+ Control de Aplicaciones) 11.5 Gbps · Rendimiento Protección de amenazas (FW +IPS + Control de Aplicaciones + AntiMalware) 10.5 Gbps · Rendimiento IPSec VPN 55 Gbps · Soporte de 8 Millones sesiones concurrentes · Rendimiento de Inspección SSL 9 Gbps · Soporte de 10.000 usuarios VPN SSL concurrentes · Rendimiento de VPN SSL 4.3 Gbps · Disco duro interno SSD: minino dos (2) de 240 GB
1.1.1.5	**Conectividad**	Para los equipos en alta disponibilidad cada uno deberá contar con las siguientes interfaces de conexión: · 16 interfaces de 1 GE RJ45 · 8 interfaces de 1 GE SFP · 4 interfaces de 10 GE SFP+ · 4 interfaces de SFP28 · Incluir 12 transceivers de 10G SF

OBJETO ADQUIRIR DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW CON INSTALACIÓN, SOPORTE Y MANTENIMIENTO INTEGRADO CON LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL ACTUAL DE LA CNSC.		
1.1. SUBÍTEM: EQUIPO SEGURIDAD PERIMETRAL		
DENOMINACIÓN TÉCNICA:		**ADQUISICION DE EQUIPOS DE SEGURIDAD PERIMETRAL DE NUEVA GENERACION, PARA EL FORTALECIMIENTO TECNOLOGICO DE LA ENTIDAD.**
CANTIDAD:		**Dos (2) FWNG + Uno (1) Gestor de Eventos**
UNIDAD DE MEDIDA:		**Unidad**
ÍTEM	**CARACTERÍSTICA**	**MINIMO REQUERIDO**
1.1.1.6	**Address Traslation**	La plataforma debe soportar lo siguiente tipos de traducción de direcciones: · NAT y PAT · NAT estático · NAT: destino, origen · NAT, NAT64 persistente
1.1.1.7	**Funciones básicas de Firewall**	Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. Licenciamiento mínimo de protección IPS, Malware, control de aplicaciones, filtrado de URL, DNS y Video, antispam. La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios. Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada. Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall. Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface) como por GUI (Graphical User Interface). La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces. El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico. Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis.

OBJETO ADQUIRIR DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW CON INSTALACIÓN, SOPORTE Y MANTENIMIENTO INTEGRADO CON LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL ACTUAL DE LA CNSC.		
1.1. SUBÍTEM: EQUIPO SEGURIDAD PERIMETRAL		
DENOMINACIÓN TÉCNICA:		**ADQUISICION DE EQUIPOS DE SEGURIDAD PERIMETRAL DE NUEVA GENERACION, PARA EL FORTALECIMIENTO TECNOLOGICO DE LA ENTIDAD.**
CANTIDAD:		**Dos (2) FWNG + Uno (1) Gestor de Eventos**
UNIDAD DE MEDIDA:		**Unidad**
ÍTEM	**CARACTERÍSTICA**	**MINIMO REQUERIDO**
1.1.1.8	**Conectividad Enrutamiento**	Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP La solución podrá habilitar políticas de ruteo en IPv6 La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6. La Solución deberá soportar balanceado de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes) La solución debe incluir funciones de control de acceso a la red (NAC) para perfilar y crear politicas para switches y Access point. La solución debe funcionar como un controlador de Switches y access point para crear una arquitectura SD-LAN
1.1.1.9	**VPN IPSEC**	El equipo deberá soportar las siguientes características: Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site). Soporte para IKEv2 y IKE Configuration Method. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits
1.1.1.10	**VPN SSL**	Capacidad de realizar SSL VPNs por usuarios sin incurrir en costos adicionales. Soporte a certificados PKI X.509 para construcción de VPNs SSL. Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
1.1.1.11	**Autenticación**	El dispositivo deberá manejar los siguientes tipos de autenticación: Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”. Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID. Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo.

OBJETO ADQUIRIR DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW CON INSTALACIÓN, SOPORTE Y MANTENIMIENTO INTEGRADO CON LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL ACTUAL DE LA CNSC.		
1.1. SUBÍTEM: EQUIPO SEGURIDAD PERIMETRAL		
DENOMINACIÓN TÉCNICA:		**ADQUISICION DE EQUIPOS DE SEGURIDAD PERIMETRAL DE NUEVA GENERACION, PARA EL FORTALECIMIENTO TECNOLOGICO DE LA ENTIDAD.**
CANTIDAD:		**Dos (2) FWNG + Uno (1) Gestor de Eventos**
UNIDAD DE MEDIDA:		**Unidad**
ÍTEM	**CARACTERÍSTICA**	**MINIMO REQUERIDO**
1.1.1.12	**Manejo de tráfico y calidad de servicio.**	Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de estas para la regla en general. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo
1.1.1.13	**Antimalware**	Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.MAPI El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de esta. Debe soportar la inspección de archivos comprimidos como los son: GZIP, RAR, LZH, IHA, CAB,ARJ;ZIP entre otros con el fin de proteger contra estas técnicas de evasión. El Antivirus deberá integrarse de forma nativa con una solución sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis.
1.1.1.14	**Filtrado WEB**	Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos. Debe poder categorizar contenido Web requerido mediante IPv6. Será posible exceptuar la inspección de HTTPS por categoría. Debe contar con la capacidad de bloquear contenido de youtube usando el Channel ID. El filtrado debe ser sobre tráfico http y https.

OBJETO ADQUIRIR DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW CON INSTALACIÓN, SOPORTE Y MANTENIMIENTO INTEGRADO CON LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL ACTUAL DE LA CNSC.		
1.1. SUBÍTEM: EQUIPO SEGURIDAD PERIMETRAL		
DENOMINACIÓN TÉCNICA:		**ADQUISICION DE EQUIPOS DE SEGURIDAD PERIMETRAL DE NUEVA GENERACION, PARA EL FORTALECIMIENTO TECNOLOGICO DE LA ENTIDAD.**
CANTIDAD:		**Dos (2) FWNG + Uno (1) Gestor de Eventos**
UNIDAD DE MEDIDA:		**Unidad**
ÍTEM	**CARACTERÍSTICA**	**MINIMO REQUERIDO**
1.1.1.15	**Protección contra intrusos (IPS)**	El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. Capacidad de detección de más de 7000 ataques. El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.
1.1.1.16	**Control de Aplicaciones**	La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección de este. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión. Debe ser posible inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos.

OBJETO ADQUIRIR DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW CON INSTALACIÓN, SOPORTE Y MANTENIMIENTO INTEGRADO CON LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL ACTUAL DE LA CNSC.		
1.1. SUBÍTEM: EQUIPO SEGURIDAD PERIMETRAL		
DENOMINACIÓN TÉCNICA:		**ADQUISICION DE EQUIPOS DE SEGURIDAD PERIMETRAL DE NUEVA GENERACION, PARA EL FORTALECIMIENTO TECNOLOGICO DE LA ENTIDAD.**
CANTIDAD:		**Dos (2) FWNG + Uno (1) Gestor de Eventos**
UNIDAD DE MEDIDA:		**Unidad**
ÍTEM	**CARACTERÍSTICA**	**MINIMO REQUERIDO**
1.1.1.17	**Inspección de Contenido SSL/SSH**	La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad. La inspección deberá realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection.
1.1.1.18	**Alta Disponibilidad**	El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico. El equipo debe soportar hasta 4 equipos en esquema de HA.
1.1.1.19	**Visibilidad**	La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma. De las aplicaciones Cloud como Dropbox que permiten compartir archivos, debe ser posible ver que archivos fueron subidos y descargados por los usuarios.
1.1.1.20	**Características de Administración**	Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS). Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos. Debe tener la capacidad de gestionar todas las políticas de seguridad, incluir la facilidad de administrar Switches y Access Point del mismo fabricante dentro de una única consola de gestión o desde el Firewall. Debe estar en capacidad de administrar switches y Access point para generar una red SD-LAN administrada y gestionada desde el mismo Firewall.

OBJETO ADQUIRIR DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW CON INSTALACIÓN, SOPORTE Y MANTENIMIENTO INTEGRADO CON LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL ACTUAL DE LA CNSC.		
1.1. SUBÍTEM: EQUIPO SEGURIDAD PERIMETRAL		
DENOMINACIÓN TÉCNICA:		**ADQUISICION DE EQUIPOS DE SEGURIDAD PERIMETRAL DE NUEVA GENERACION, PARA EL FORTALECIMIENTO TECNOLOGICO DE LA ENTIDAD.**
CANTIDAD:		**Dos (2) FWNG + Uno (1) Gestor de Eventos**
UNIDAD DE MEDIDA:		**Unidad**
ÍTEM	**CARACTERÍSTICA**	**MINIMO REQUERIDO**
1.1.1.21	**Virtualización**	El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains” Debe soportar e incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer. Cada instancia virtual debe poder tener un administrador independiente
1.1.1.22	**Licenciamiento y actualizaciones**	El licenciamiento de todas las funcionalidades debe ser Ilimitado en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering.
1.1.1.23	**Licenciamiento SASE**	Se deben incluir 50 licencias completamente integradas nativamente con la solución de SD-WAN y Firewall y del mismo fabricante, que tenga incorporados los siguientes servicios: IPS, Web, DNS, SSL, Anti-Malware, CASB más integraciones con la solución ofertada de NOC/SOC. Debe proveer funciones de acceso seguro privado (Secure Private Access SPA). Debe tener un único agente que incluya SASE, ZTNA, Antivirus. Debe tener la posibilidad de realizar SWG sin agente instalado. Includes 3 devices per-user Antivirus, AntiSpam, IPS, Application Control y URL Filtering. Cada licencia de SASE debe permitir al usuario conectar hasta tres (3) dispositivos. Todos los servicios SASE como Antivirus, ZTNA, control de aplicaciones deben ser del mismo fabricante. No se admite que los servicios sean una integración con otros fabricantes o reenvío hacia otros PoPs.

1.1.1.24	**Gestor de eventos**	Se requiere un equipo tipo appliance físico que permita registrar cada transacción de la plataforma de seguridad perimetral de la entidad, para poder identificar y reaccionar a cualquier informe emitido por un log o registro de los dispositivos de seguridad perimetral ofertados tales como el Firewall de Nueva Generación, capacidad de logs de swtiches, access point, sistemas MFA, NAC, entre otros. El equipo deberá recolectar y emitir el reporte de eventos, actividades y tendencias ocurridas en las plataformas de seguridad perimetral tales como el Firewall de Nueva Generación, NAC, switches y Access point. Debe ser de la misma marca que todas las soluciones ofrecidas para garantizar optima seguridad e integración nativa entre todos los componentes **Desempeño** La solución de análisis de logs debe dar soporte a las siguientes características: Capacidad de recibir hasta 200 GB de logs diarios. Capacidad de Almacenamiento de16 Terabytes Cuatro (4) interfaces de red de 1Gbps Mbps Cobre Capacidad de recibir logs hasta de 800 equipos sin necesidad de licencias adicionales Los discos deben soportar arreglos de RAID 0/1,1s/5,5s/10 **Funciones y configuraciones requeridas para el analizador de red** Visor de tráfico en tiempo real. Visor de tráfico histórico. Visor personalizado de log de tráfico El licenciamiento debe incluir Indicadores de compromiso, servicios de automatización y servicios de Outbreak. Herramienta de búsqueda sobre los logs de tráfico. **Análisis de logs y reportes requeridos** Vista de búsqueda y manejo de logs. Reportes basados en perfiles. Inventario de plantillas predefinidas para reportes regulares. Debe soportar de forma predefinida los reportes: Eventos del sistema Análisis de riesgo y aplicaciones Reporte de Aplicaciones y Ancho de Banda Reputación de Clientes Análisis de seguridad Reporte de Amenazas Reportes de VPN Reportes de uso de Web Reportes de WiFi Debe ser posible calendarizar los reportes

OBJETO ADQUIRIR DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW CON INSTALACIÓN, SOPORTE Y MANTENIMIENTO INTEGRADO CON LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL ACTUAL DE LA CNSC.		
1.1. SUBÍTEM: EQUIPO SEGURIDAD PERIMETRAL		
DENOMINACIÓN TÉCNICA:		**ADQUISICION DE EQUIPOS DE SEGURIDAD PERIMETRAL DE NUEVA GENERACION, PARA EL FORTALECIMIENTO TECNOLOGICO DE LA ENTIDAD.**
CANTIDAD:		**Dos (2) FWNG + Uno (1) Gestor de Eventos**
UNIDAD DE MEDIDA:		**Unidad**
ÍTEM	**CARACTERÍSTICA**	**MINIMO REQUERIDO**
		La plataforma deberá permitir integrar los logs de las plataformas de Firewall ofertadas. La solución debe incluir servicios de Indicadore de compromiso, servicio de automatización y servicio de Outbreak.

SUBITEM 3.1. SERVICIOS		
3.1.1.1	Soporte y Garantía	Se debe brindar el soporte y garantía para cualquier evento o incidente, en un esquema 7x24, por dos años y directamente con fabricante. El contratista debe adjuntar certificación por parte de fabricante donde se evidencie que la Entidad cuenta con soporte directo de fábrica.
3.1.1.2	Licenciamiento Firewall	Todo el Licenciamiento y servicio requerido se debe proveer por dos (2) año en un esquema de soporte 7x24 ante el fabricante sin costo adicional para la Entidad con el fin de mantener la solución actualizada a las últimas versiones. Esto incluye los equipos de seguridad que hacen parte de la infraestructura actual, Fortigate 2500E y para el gestor de eventos.
3.1.1.4	Servicio de Instalación	El contratista deberá realizar la instalación y configuración de la solución ofrecida y su integración e interoperabilidad con la arquitectura de Seguridad perimetral, conectividad y monitoreo, lo anterior con el fin de implementar la arquitectura requerida por la Entidad. El contratista debe contar con personal experto certificado por fabricante de la solución a implementar, deberá presentar con la firma del acta de inicio las hojas de vidas con las certificaciones de fábrica.

3.1.1.5	Personal Equipo Mínimo Solicitado para la gestión e implementación del Proyecto	**Coordinador del proyecto** **Profesión:** Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. **Especialista:** Gerencia de Proyectos o Gerencia de Proyectos en Ingeniería de Telecomunicaciones o Administración de Empresas con Especialidad en Dirección de Proyectos. **Certificaciones:** -PMP - Project Management Professional o Prince -CISM Certified Information Security Manager o CISSP Certified Information Systems Segurity Professional **Experiencia general:** 6 años como profesional ejecutando proyectos y/o labores como director o gerente de proyectos en el sector de tecnología. **Experiencia especifica**: 3 años en proyectos infraestructura de seguridad perimetral **Ingeniero Experto** **Profesión:** Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. **Especialista:** Seguridad de la información o Seguridad informática o Seguridad de Redes Telemáticas o Seguridad Física y de la informática. **Certificaciones:** Certificación LACNIC avanzado Certified Professional Security Operations Certified Solution Specialist Security Operations (Security Operations Architect) **Experiencia general:** 6 años como profesional ejecutando proyectos y/o labores consultor especialista en seguridad de la información o Ciberseguridad. **Experiencia especifica:** 3 años en implementación y/o Despliegue de herramientas firewall. **Ingeniero Implementador** **Profesión:** Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. **Certificaciones:** Certified Professional Security Operations (FortiGate Admin) -Scrum Fundamentals Certified Seguridad en BGP con RPKI e IRR LACNIC

		Experiencia general: 5 años como profesional ejecutando proyectos y/o labores como consultor en Seguridad o Ciberseguridad o seguridad informática. **Experiencia especifica:** 3 años en la implementación de firewall del fabricante ofertado.
3.1.1.6	Nivel de Membresía	El contratista debe ser Partner y/o distribuidor y/o proveedores autorizados por fabricante con el nivel más alto de membresía del programa de Partner del fabricante, y que cuente con las especializaciones o competencias técnicas vigentes en SD-WAN y Security Operations, o equivalentes, que le permitan diseñar, implementar y soportar dichas soluciones.
	Certificaciones o Acreditaciones.	Entregar con la firma del Acta de Inicio, las certificaciones o acreditaciones vigentes que respalden su capacidad para ejecutar el objeto contractual. Estas deberán ser emitidas por un Organismo de Certificación (CB) que esté acreditado por el Organismo Nacional de Acreditación de Colombia – ONAC o por un Organismo de Acreditación (AB) signatario de acuerdos multilaterales de reconocimiento (MLA/MRA) a nivel internacional. Las certificaciones deberán permanecer vigentes durante toda la ejecución del contrato. El alcance de las certificaciones deberá cubrir explícitamente algunos de los servicios descritos: SOC/NOC, consultoría en ciberseguridad, ethical hacking y vulnerabilidades, Zero Trust y SASE, así como el diseño e implementación de soluciones físicas y lógicas de seguridad informática. La Entidad no limita la certificación a una norma o denominación específica. Se aceptarán todas las certificaciones/acreditaciones que cumplan con el alcance detallado, independientemente del nombre comercial o marco de referencia utilizado por el organismo emisor.
3.1.1.7	Niveles de Servicio	El contratista debe colocar a disposición del contratante, durante el tiempo de Soporte y Garantía, el recurso físico y humano necesario, para cumplir con los niveles de servicio y compromisos para los bienes adquiridos, en un modelo de 7*24*365*4, es decir, los siete días de la semana, las veinticuatro horas del día todos los días del año y con un máximo tiempo de respuesta de cuatro (4) horas en sitio y tiempo de solución de 8 horas hábiles a partir de la solicitud de servicio, para atender los requerimientos de la Entidad, tras haberse solicitado por el Supervisor del Contrato
3.1.1.8	Mantenimiento Preventivo	Como mínimo dos (2) Durante el periodo del soporte y garantía, según cronograma que se establecerá al inicio del contrato por el responsable de control de ejecución por parte de los contratantes en estas visitas se llevarán a cabo todas las labores pertenecientes a este tipo de mantenimiento tales como limpieza general de las partes y diagnósticos de la solución objeto del contrato. El servicio no deberá significar costo alguno para los contratantes y debe ser realizado por personal certificado por fabricante. Se debe entregar un reporte con las actividades realizadas y recomendaciones de mejora continua.

FIRMA: _____

NOMBRE DEL REPRESENTANTE LEGAL: _____

NOMBRE O RAZÓN SOCIAL: _____

NIT: _____

DOCUMENTO DE IDENTIDAD: _____