ANEXO ESPECIFICACIONES TÉCNICAS

Las especificaciones técnicas establecidas en el presente documento constituyen requisitos mínimos de obligatorio cumplimiento. En consecuencia, el oferente podrá proponer bienes, equipos, licencias o soluciones tecnológicas con características equivalentes o superiores a las aquí señaladas, siempre que demuestre de manera suficiente y verificable que cumplen, como mínimo, con las condiciones funcionales, técnicas, operativas, de desempeño, compatibilidad, seguridad y calidad exigidas por la entidad, sin que ello genere costos adicionales ni limitaciones para su implementación y operación.

El firewall ofertado deberá ser de categoría empresarial (Enterprise Firewall NGFW), orientado a entornos corporativos e institucionales, soportado directamente por el fabricante y diseñado para garantizar la protección integral de la infraestructura tecnológica de la entidad. La solución deberá proporcionar capacidades avanzadas de seguridad, alta disponibilidad, inspección de tráfico, prevención y detección de amenazas, administración centralizada, interoperabilidad con plataformas tecnológicas existentes, y continuidad operativa, permitiendo una adecuada gestión de riesgos y fortaleciendo la postura de ciberseguridad institucional.

Es importante señalar que el dispositivo de seguridad actualmente en operación cuenta con licencia vigente hasta el 15 de septiembre de 2026. En consecuencia, para dicha fecha la entidad deberá disponer del nuevo dispositivo debidamente configurado, instalado y sometido a las pruebas correspondientes, con el fin de garantizar la continuidad del servicio y evitar posibles afectaciones operativas o riesgos de seguridad.

1. OBJETO.

SUMINISTRAR, INSTALAR, CONFIGURAR Y PONER EN FUNCIONAMIENTO UNA SOLUCIÓN INTEGRAL DE SEGURIDAD PERIMETRAL TIPO FIREWALL DE NUEVA GENERACIÓN (NGFW), INCLUYENDO EL LICENCIAMIENTO, PARA DEL FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA – FONDECÚN

2. CODIFICACIÓN DE LA NECESIDAD DENTRO DE LA CODIFICACIÓN DE BIENES Y SERVICIOS DE NACIONES UNIDAS.

De conformidad con el objeto contractual, los bienes y servicios requeridos se encuentran clasificados dentro de los siguientes códigos del Clasificador de Bienes y Servicios de las Naciones Unidas – UNSPSC:

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	PRODUCTO
43232801	Difusión de Tecnologías de la Información y Telecomunicaciones	Software	Software de administración de redes	Software de monitoreo de red
43222501	Difusión de Tecnologías de la Información y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de Seguridad de red	Equipo de seguridad de redes cortafuegos (firewall)

43233200	Difusión de Tecnologías de la Información y Telecomunicaciones	Software	Software de seguridad y protección	Software de seguridad y protección

3. ESPECIFICACIONES TÉCNICAS.

Con el propósito de garantizar condiciones adecuadas de protección y desempeño, FONDECUN requiere actualizar su infraestructura de seguridad perimetral, considerando los cambios en el panorama de ciberseguridad, el aumento sostenido del tráfico institucional y la mayor utilización de servicios y aplicaciones que emplean mecanismos de cifrado.

En consecuencia, no se contempla la reposición del equipo en operación por una solución de iguales características. La necesidad institucional corresponde a una actualización tecnológica que permita incrementar la capacidad de procesamiento y de inspección de tráfico, así como fortalecer los mecanismos de protección y respuesta ante amenazas, asegurando niveles adecuados de desempeño, disponibilidad y continuidad de los servicios tecnológicos.

La solución de seguridad perimetral deberá operar bajo un enfoque integral de ciberseguridad, contemplando capacidades de:

- Prevención de amenazas avanzadas.
- Detección de comportamientos maliciosos y actividades anómalas.
- Respuesta oportuna ante incidentes de seguridad.
- Inspección profunda del tráfico de red, incluyendo tráfico cifrado.
- Control y visibilidad de aplicaciones, usuarios y contenidos.
- Protección frente a amenazas conocidas y emergentes.

Adicionalmente, la infraestructura tecnológica de la Entidad soporta servicios críticos para la operación institucional, los cuales demandan altos niveles de disponibilidad, rendimiento y protección, por lo que la solución propuesta deberá garantizar la continuidad de los servicios, la resiliencia operativa y la capacidad de crecimiento futuro de la plataforma tecnológica, alineándose con las mejores prácticas y estándares de seguridad de la información.

La solución ofertada deberá ser nueva, original de fábrica, no usada, no remanufacturada, no reacondicionada y provenir de canales autorizados por el fabricante. Asimismo, el equipo, componentes, software y licenciamiento suministrados no deberán encontrarse en estado de obsolescencia, fin de comercialización (End of Sale - EOS), fin de soporte (End of Support - EOS), fin de desarrollo (End of Engineering - EOE) o fin de vida útil (End of Life - EOL) durante la vigencia del contrato y del licenciamiento ofrecido.

El fabricante deberá certificar la disponibilidad de actualizaciones de software, firmware, firmas de seguridad, parches y soporte técnico durante todo el período contratado, mediante documento o certificación del fabricante, que el modelo ofertado se encuentra vigente en el portafolio comercial y cuenta con soporte oficial para todo el período requerido y una vida útil de mínimo 5 años

Las siguientes especificaciones corresponden a los requisitos mínimos de capacidad y funcionalidad exigidos para la solución. Estas se encuentran definidas con base en criterios de desempeño, características técnicas y requerimientos operativos de acuerdo con el análisis de los requerimientos tecnológicos de la entidad.

Categoría	Requisito Técnico Mínimo
Tipo de solución	Appliance de seguridad tipo Firewall de Nueva Generación (NGFW), de propósito específico, equipo físico.
Arquitectura	Soporte de alta disponibilidade.
Rendimiento Firewall	>=8 Gbps
Rendimiento IPS	>=5 Gbps
Rendimiento NGFW	>=3 Gbps
Rendimiento Protección de Amenazas	>=2.5 Gbps
Rendimiento de VPN Ipsec	>=5 Gbps
Rendimiento del control de aplicaciones	>=6.7 Gbps
Rendimiento de SSL-VPN	>=1.5 Gbps
Rendimiento de inspección SSL	>=1.8 Gbps
Sesiones Concurrentes	>=3.000.000
CPS de inspección SSL	>=2100
Nuevas sesiones por segundo	=> 50000
Interfaces de red	Interfaces suficientes para la operación, incluyendo al menos: • Puertos GE RJ45 >=16 • Puertos 10GE SFP =>3 • 1 puerto de consola RJ45
Control de aplicaciones	Identificación y control de aplicaciones independiente de puerto/protocolo Control de aplicaciones basado en firmas y comportamiento Protección contra aplicaciones evasivas.
IPS	Sistema de prevención de intrusiones integrado con actualización de firmas respaldadas por el fabricante.
Antimalware	Protección contra malware en tiempo real con soporte de múltiples protocolos, integración con servicios avanzados de detección.
Filtrado web	Clasificación por categorías y control de navegación
Inspección SSL/TLS	Inspección de tráfico cifrado con políticas configurables
VPN	Soporte IPsec y SSL VPN
Autenticación	Integración con LDAP, RADIUS, TACACS+ y Active Directory
Routing	Soporte de ruteo estático y dinámico (OSPF, BGP, RIP)
SD-WAN	Soporte de balanceo inteligente basado en SLA (latencia, jitter, pérdida)
Alta disponibilidad	Sincronización de sesiones y conmutación automática
Logs y monitoreo	Registro de eventos, exportación a SIEM Dashboards en tiempo real
Gestión	Consola centralizada (local o cloud)
Virtualización	Soporte de instancias virtuales (mínimo 5 instancias independientes)
QoS	Control de ancho de banda y traffic shaping
Autenticación	Autenticación multifactor (MFA). Single Sign-On (SSO).
Protección avanzada contra amenazas	Detección y bloqueo de botnets. Protección DNS Security. Integración con servicios de inteligencia de amenazas
Conectividad	Soporte IPv4 e IPv6. NAT, PAT y NAT64.
Licenciamiento	Deberá incluir el licenciamiento necesario para habilitar todas las funcionalidades de seguridad ofertadas: IPS, control de aplicaciones, antivirus, antispam, antimalware, anti ransomware, cntra botnets, filtrado web, protección DNS, análisis avanzado de amenazas, soporte técnico 24x7 y actualizaciones del fabricante por mínimo tres (3) años

Soporte y garantía	3 años con actualizaciones y soporte técnico, se deberá entregar soporte de la garantía oficial del fabricante
Servicios incluidos	Instalación, configuración, afinamiento, monitoreo, mantenimiento y soporte

4. Servicios incluidos

El contratista deberá incluir sin costo adicional los siguientes servicios profesionales:

- Instalación física y lógica de la solución en la infraestructura de la entidad.
- Configuración inicial de la plataforma, incluyendo parametrización, ajuste y optimización de políticas de seguridad.
- Migración de configuraciones existentes, cuando aplique.
- Acompañamiento y soporte durante las pruebas funcionales, de rendimiento, aceptación, estabilización y puesta en producción

5. Capacitaciones y documentación

El contratista deberá realizar capacitación técnica de mínimo 4 horas, al personal designado por la entidad en los siguientes temas:

- Administración básica
- Gestión de políticas
- Monitoreo
- Gestión de incidentes
- Buenas prácticas de seguridad
- Actualizaciones

6. Entregables

- Manuales de operación, manual técnico del equipo.
- Informe que contenga el detalle de las actividades realizadas durante la ejecución del contrato. El informe debe contener información de la instalación, configuración y puesta en operación del equipo y su licencia, con sus soportes como log, configuración, registro fotográfico, y demás información relevante del proceso de instalación.
- Garantía del fabricante.
- Soporte del licenciamiento por el tiempo solicitado