ESTUDIOS PREVIOS

Fecha: noviembre de 2025.

1. **DESCRIPCIÓN DE LA NECESIDAD QUE LA ENTIDAD ESTATAL PRETENDE SATISFACER CON EL PROCESO DE CONTRATACIÓN**

La Empresa Férrea Regional S.A.S. – EFR S.A.S., fue creada el 15 de diciembre de 2010, mediante Escritura Pública No. 1280, como una sociedad por acciones simplificada, del orden departamental, de carácter comercial con aportes públicos, con domicilio en Bogotá, con autonomía administrativa, patrimonial y presupuestal tiene como objeto: "Corresponde a la EMPRESA FÉRREA REGIONAL S.A.S, en las condiciones que señalan las normas vigentes y las autoridades competentes: (i) El desarrollo, establecimiento, explotación y operación del sistema de transporte masivo y del sistema de transporte ferroviario, incluyendo las respectivas infraestructuras. (ii) la gestión, de otros sistemas alternativos de transporte, cuando así lo determinen las autoridades competentes, así como a facilitar y coadyuvar a la integración modal con otros sistemas de transporte de entes gestores y modos de transporte para la correcta prestación de servicio de transporte. (iii) La gestión, ejecución y administración de proyectos de infraestructura de transporte que atiendan las necesidades de movilidad, cuando dicha labor se asigne o delegue por la correspondiente autoridad de transporte a través convenio o contrato, labores que podrá desempeñar directamente o con terceros. (iv) Prestar servicios de asesoría, consultoría asistencia técnica y capacitación en servicios de transporte público en sus diferentes modalidades. (…)

Parágrafo: En desarrollo de este objeto, la sociedad podrá ejecutar todos los actos o contratos y solicitar las autorizaciones legales que fuesen necesarias y/o convenientes para el cabal cumplimiento de éste. (…)

En el desarrollo de sus actividades y para garantizar el cabal cumplimiento de su objeto social, la EFR SAS requiere la continua contratación de obras, bienes y servicios, aplicando las diferentes modalidades de contratación establecidas en el Estatuto de Contratación Estatal, particularmente en la Ley 80 de 1993, Ley 1150 de 2007, el Decreto 1082 de 2015 y demás decretos reglamentarios, al igual que en Regímenes Especiales de Contratación, normatividad que establece los procedimientos y parámetros en la contratación estatal de estricto cumplimiento, cuya desatención genera responsabilidad fiscal, disciplinaria y penal para los funcionarios.

Por otra parte en el año 2020 el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia –MinTIC, expidió la Resolución 1519 de 2020 "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.", dicha resolución establece los lineamientos que deben seguir los sujetos obligados para cumplir con la publicación y

divulgación de la información señalada en la Ley 1712 del 2014, definiendo para ello un conjunto de anexos técnicos que deben ser acogidos e implementados tanto en el sitio de transparencia y acceso a la información como en la página web de las Entidades públicas.

Mediante Acuerdo No. 03 del 16 de mayo de 2023 "Por el cual se establece la organización interna de la Empresa Férrea Regional S.A.S., se determinan las funciones de sus dependencias y se dictan otras disposiciones", se establece en el artículo décimo las funciones de la Dirección Administrativa y Financiera, señalando entre otras, las siguientes: "(…) 18. Liderar y coordinar estrategias enfocadas a la optimización de recursos con el fin de garantizar el adecuado funcionamiento de la EFR; (…); 20. Liderar y coordinar, los procesos administrativos y de apoyo con las diferentes áreas de la Empresa con el objeto de mantener el desarrollo de su actividad, unidad de propósito y eficiencia en la prestación de los servicios; 21. Identificar y priorizar las necesidades de tecnologías de la Información y las Comunicaciones para las áreas de la EFR; 22. Dirigir, coordinar y controlar la adquisición y almacenamiento de los elementos, materiales, y equipos bienes y servicios de la EFR. (…)"

En este sentido le corresponde a la Dirección Administrativa y Financiera garantizar la seguridad y privacidad de la información al interior de la Empresa identificando las acciones a implementar que le permitan dar cumplimiento a la normatividad vigente. Es por esto, que en desarrollo de su gestión se identificó la necesidad de adquirir una Solución de Seguridad Perimetral Firewall UTM.

La Solución de Seguridad Perimetral Firewall UTM., permite gestionar a nivel de hardware y software la seguridad de la red, durante la navegación de los usuarios para prevenir ataques, accesos no autorizados y otros riesgos cibernéticos que puedan vulnerar la información sensible que maneja la EFR, afectando la integridad y disponibilidad de los recursos tecnológicos.

A continuación, se detallan aspectos clave que justifican su adquisición:

- **Control de Acceso y Filtrado de Tráfico (Principio de Mínimo Privilegio):** Su función principal es filtrar y bloquear el tráfico entrante y saliente no autorizado, basándose en reglas predefinidas (direcciones IP, puertos, protocolos). Sin un Firewall, la red está expuesta a cualquier escaneo o conexión maliciosa desde Internet, facilitando ataques como el escaneo de puertos o la explotación de servicios vulnerables.
- **Prevención de Intrusiones y Malware:** Un Firewall de próxima generación (NGFW) permite detectar y bloquear activamente amenazas como virus, ransomware, y troyanos que intentan entrar o salir de la red, incluso a nivel de aplicación, deteniendo la amenaza antes de que llegue al endpoint o al servidor.
- **Segmentación de Red y Mitigación de Movimiento Latera**l: Un Firewall permite dividir la red interna en segmentos lógicos (ej. Red de Servidores, Red de Usuarios, Red de IoT). Esta segmentación aísla los recursos críticos. En caso de que un

atacante o malware comprometa un segmento (ej. un PC de usuario), el Firewall puede impedir el "movimiento lateral" hacia segmentos más sensibles (ej. la base de datos central), limitando drásticamente el impacto de la brecha.

- **Cumplimiento Normativo y Auditoría:** Prácticamente todos los marcos de cumplimiento (como PCI DSS, HIPAA, ISO 27001) exigen la implementación de un Firewall para proteger los datos sensibles. La adquisición y configuración de un Firewall proporciona un registro de auditoría detallado del tráfico de red, lo cual es esencial para el análisis forense post-incidente y para demostrar el cumplimiento ante reguladores.
- **Gestión y Optimización de Ancho de Banda (QoS):** Además de la seguridad, el Firewall permite priorizar el tráfico crítico del negocio mediante políticas de Calidad de Servicio (QoS) y bloquear el tráfico improductivo (ej. ciertas redes sociales o streaming), asegurando que los recursos de red se utilicen de manera eficiente.

Dado la EFR requiere tener un mayor detalle y control sobre todos los accesos correspondientes a Internet (Correo Electrónico, Redes Sociales, Navegación Web, etc.)., se hace necesario realizar la adquisición del licenciamiento y servicios de soporte de esta solución de seguridad perimetral.

2. VERIFICACIÓN DE QUE LA NECESIDAD SE ENCUENTRA PREVISTA EN EL PLAN ANUAL DE ADQUISICIONES

Este proceso se encuentra en la **línea No. 206** del Plan Anual de Adquisiciones 2025 de la Empresa Férrea Regional S.A.S.

3. OBJETO, ESPECIFICACIONES E IDENTIFICACIÓN DEL CONTRATO.

3.1. OBJETO:

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.

3.1.1. ALCANCE:

El alcance del presente contrato comprende la adquisición e implementación de una Solución Integral de Seguridad Perimetral de tipo Firewall UTM (Unified Threat Management), la cual deberá garantizar la protección de la infraestructura tecnológica de la Entidad contra amenazas cibernéticas, asegurando la confidencialidad, integridad y disponibilidad de la información y los servicios.

3.1.2 CLASIFICACIÓN EN EL SISTEMA UNSPSC

Los bienes y/o servicios requeridos se clasifican de la siguiente forma:

Clasificación UNSPSC	Segmento	Familia	Clase	Producto
43222501 - Equipo de seguridad de red cortafuegos (firewall)	43	22	25	01
43233204 - Software de equipos de seguridad de red y de redes privadas virtuales VPN	43	23	32	04
81111801 - Seguridad de los computadores, redes o internet	81	11	18	01
81112208 - Mantenimiento de software de protección y seguridad	81	11	22	08

Fuente: Clasificador de Bienes y Servicios CCE.

4. CONDICIONES TÉCNICAS EXIGIDAS.

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 tener funcionalidades de WAF y Email Protection 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.**
1.32	El firewall debe garantizar la posibilidad de habilitar e incorporar funcionalidades de acceso de red de confianza cero (ZTNA) en caso de requerirse a futuro, sin necesidad de adquirir ni desplegar un appliance adicional.
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, PPTP.
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 y PPTP.
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 2 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 DH 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 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 de Firewall debe proveer un segundo motor de detección de malware independiente para escaneo dual.
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

Garantía y Soporte

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.

5. FUNDAMENTOS JURÍDICOS

- Constitución Política de Colombia;
- Ley 57 de 1887 “Código Civil”
- Ley 80 de 1993 y Decretos Reglamentarios;

- Ley 1150 de 2007 "Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos".
- Ley 1437 de 2011 "Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo".
- Ley 1474 de 2011 “Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública”.
- Ley 1564 de 2012 “Código General del Proceso”.
- Ley 1437 de 2011 “Código de Procedimiento Administrativo y de lo Contencioso Administrativo”.
- Ley 1564 de 2012 “Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones”
- Ley 2294 de 2023 “Por la cual se expide el Plan Nacional de Desarrollo, 2022-2026”.
- Decreto 410 de 1971 “Código de Comercio”.
- Decreto 019 de 2012 “Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública”.
- Decreto 1082 de 2015 "Por medio del cual se expide el decreto único reglamentario del sector Administrativo de Planeación Nacional"
- Decreto 310 de 2021 "Por el cual se reglamenta el artículo 41 de la Ley 1955 de 2019, sobre las condiciones para implementar la obligatoriedad y aplicación de los Acuerdos Marco de Precios y se modifican los artículos 2.2.1.2.1.2.7. y 2.2.1.2.1.2.12. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional".
- Ley 1955 de 2019,
- Ley 2069 de 2020,
- Decreto 1860 de 2021,
- Decreto 142 de 2023,
- Decreto 1600 de 2024
- Las demás normas concordantes con la materia, que rijan o lleguen a regir los aspectos de este proceso de selección.

6. MODALIDAD DE SELECCIÓN DEL CONTRATISTA, INCLUYENDO LOS FUNDAMENTOS JURIDICOS QUE SOPORTAN SU SELECCIÓN

El numeral 2° del artículo 2 de la Ley 1150 de 2007 dispone lo siguiente: *“La Selección abreviada corresponde a la modalidad de selección objetiva prevista para aquellos casos en que, por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicio puedan adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual” /(…)/ Serán causales de selección abreviada las siguientes: / a) La adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades, que corresponden a aquellos que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos./ Para la adquisición de estos bienes y servicios las entidades deberán, siempre que el reglamento así lo señale, hacer uso de*

procedimientos de subasta inversa o de instrumentos de compra por catálogo derivados de la celebración de acuerdos marco de precios o de procedimientos de adquisición en bolsas de productos; (…).

La Empresa Férrea Regional SAS para la vigencia 2025, contempla la adquisición de Firewall de hardware o firewalls de red, los cuales son dispositivos electrónicos externos que se colocan entre la computadora o red y el modem que da acceso a Internet y su objetivo es controlar las comunicaciones y conexiones con el exterior, tanto entrantes como salientes. Los firewalls por hardware proporcionan una línea de defensa adicional contra ataques procedentes del exterior, por ser dispositivos separados con su propio sistema operativo.[1]

Conforme con lo expuesto, se encuentra que, los bienes y/o servicios que la entidad pretende adquirir, presentan características técnicas uniformes y de común utilización, de las que trata el artículo 2.2.1.1.1.3.1. del Decreto 1082 de 2015 *"**Definiciones.** (…) Bienes y servicios de común utilización con especificaciones técnicas y patrones de desempeño y calidad iguales o similares, que en consecuencia pueden ser agrupados como bienes y servicios homogéneos para su adquisición y a los que se refiere el literal (a) del numeral 2 del artículo 2 de la Ley 1150 de 2007.".*

De acuerdo con lo anterior el objeto a contratar la presente contratación se efectuará a través de la modalidad de selección abreviada, de acuerdo con el literal a) del Numeral 2 Articulo 2 Ley 1150 de 2007 y las demás normas concordantes y complementarias sobre la materia.

No obstante la Empresa Férrea Regional S.A.S. procedió a validar la existencia de un Acuerdo Marco de Precios (AMP), que satisfaga la necesidad existente y puesto a disposición de las Entidades estatales por parte de la Agencia Nacional de Contratación Publica – Colombia Compra Eficiente evidenciando:

El Acuerdo Marco de Servicios de Conectividad IV, CCE-SNG-AMP-003-2024 - Proceso # CCENEG-074-01-2024, incluye en su catálogo segmento 1 (cobertura nacional) los equipos de seguridad perimetral (Firewall) en modalidad de Servicio, es decir con pago mensualizado por el uso de los equipos.

El Acuerdo Marco para la adquisición de servicios de Nube Privada IV, CCE-308-AMP-2022 - Proceso: CCENEG-061-01-2022, el cual incluye en el catálogo (segmento 2), la seguridad perimetral (Firewall) en la modalidad de servicio de Infraestructura como Servicio (IaaS)

Para el caso específico del Acuerdo Marco de Nube Privada, estos equipos se ofrecen en modalidad de servicio con el fin de brindar la protección perimetral de aquellos que se dispongan en un centro de datos de nube privada, dicha modalidad actualmente no responde a la necesidad de la entidad, debido a que la EFR, no cuenta con centro de datos de nube privada.

[1] Firewall por hardware | Guías Prácticas (guiaspracticas.com)

De otra parte, el Acuerdo Marco de Conectividad IV, ofrece el producto FIREWALL en modalidad de servicio, pero cuando se revisa la ficha técnica indica que la ELASTICIDAD ofrecida es “ROL de Firewall” lo que permite únicamente servicios de:

- Control de tráfico entrante y saliente.
- Aplicación de reglas de seguridad estáticas.
- Control de acceso por IP, puerto y protocolo.
- Protección básica contra ataques

En este caso, no sería posible contar con los servicios requeridos por la EFR tales como: (I) filtrado WEB el cual permite controlar el acceso a páginas por categorías (Drogas, Pornografía, Violencia, etc.), (II) sistema de prevención de intrusos (IPS), (III) control de aplicaciones y (IV) control de ancho de banda por aplicaciones (traffic Shaping).

Es de anotar, que la modalidad de servicio o Infraestructura como Servicio (IaaS) no atiende a la realidad de la necesidad establecida por la EFR, que corresponde a equipos de seguridad perimetral (Firewall) físicos en alta disponibilidad, de tal manera que sean parametrizadas las políticas para la prevención del riesgo de pérdida de información y vulnerabilidad de esta.

Por último, es importante indicar que la EFR pretende implementar servicios de VPN´s cliente, que permiten el acceso desde fuera de las instalaciones a los servidores públicos y colaboradores de la empresa.

Todo lo anterior la Empresa Férrea Regional requiere, por buenas prácticas, que el FIREWALL sea de propiedad de la entidad y no en modalidad de servicio o arrendamiento, de este modo se garantiza la autonomía en la operación y el desarrollo de un plan de continuidad de los servicios de seguridad y de red y todo lo que se encuentra ligado a estos.

En este orden de ideas, una vez consultados los Acuerdo Marco vigentes y suscritos por Colombia Compra Eficiente, se ha concluido que los mismos no satisfacen la necesidad en el entendido que no permitirán llevar a cabo la implementación de la solución teniendo en cuenta las especificaciones técnicas identificadas para satisfacer sus necesidades.

Por los motivos expuestos, la EFR considera beneficioso adelantar el presente proceso haciendo uso de la modalidad de selección de Selección Abreviada por Subasta Inversa, considerando que los bienes y servicios a adquirir corresponden a bienes de características técnicas uniformes y de común utilización.

7. VALOR ESTIMADO DEL CONTRATO Y SU JUSTIFICACIÓN:

El valor del contrato corresponderá al valor total de la oferta económica presentada por el proponente que cumpla con todos y cada uno de los requisitos habilitantes y que haya

presentado el menor precio en Lance, o el menor precio inicial, en caso de que no se presenten lances durante la Subasta, incluido IVA y demás impuestos, tasas, contribuciones de carácter nacional y distrital legales a que haya lugar; costos y demás conceptos fijos, variables, directos e indirectos en que pueda incurrir el futuro contratista para la ejecución del contrato desde la suscripción hasta la liquidación del mismo.

El presupuesto oficial estimado para el presente proceso es de **TRESCIENTOS OCHENTA Y SIETE MILLONES SEISCIENTOS OCHENTA MIL DOSCIENTOS DOCE PESOS ($387.680.212) M/CTE.**, incluido IVA y demás tributos nacionales, departamentales, municipales y distritales que se causen por el hecho de su celebración, ejecución y liquidación, así como todos aquellos gastos en que deba incurrir el contratista para perfeccionar y legalizar su relación con la entidad.

Para determinar el presupuesto del proceso se realizó el envío de solicitudes a empresas del sector vía correo electrónico, recibiendo tres (3) cotizaciones.

El siguiente cuadro resume las solicitudes enviadas, las recibidas y el tamaño de las empresas:

Empresas	Cotización Enviada	Cotización recibida	Tamaño Empresarial
IN TECH SAS	X	X	Mediana
CYBERIS S.A.S.	X	X	Microempresa
INGENIUM COLOMBIA SAS	X	X	Mediana

Para realizar el análisis de precios se hace un ejercicio estadístico el cual hace parte integral del presente documento, en el que inicialmente se calcula el promedio simple y desviación estándar de los valores unitarios cotizados, esto con la finalidad de aumentar y disminuir una desviación estándar al promedio obtenido y así se establece un rango de valores definido entre los límites inferior y superior frente al cual se calcula nuevamente el promedio de los valores unitarios (Valor unitario establecido por la EFR), que teniendo en cuenta las cantidades requeridas, permite determinar que el presupuesto oficial es la suma de **TRESCIENTOS OCHENTA Y SIETE MILLONES SEISCIENTOS OCHENTA MIL DOSCIENTOS DOCE PESOS ($387.680.212) M/CTE.,** incluido IVA y demás tributos nacionales y subnacionales que se causen por el hecho de su celebración, ejecución y liquidación.

A continuación, se muestra el análisis realizado a las cotizaciones recibidas:

Descripción del artículo	Cantidad	IN Tech SAS	Cyberis SAS	Ingenium Colombia	Promedio	Desviciación Estándar	Limite inferior	Límite Superior	Valor Unitario establecido por la EFR	Total
Solución de seguridad Perimetral Firewall (Hardware)	2	$ 40.537.526	$ 38.834.662	$ 40.571.877	$ 39.981.355,00	$ 993.213,79	$ 38.988.141,21	$ 40.974.568,79	$ 40.554.702	$ 81.109.404
Licenciamiento Firewall (Software)	2	$ 119.142.707	$ 112.381.903	$ 131.606.723	$ 121.043.777,67	$ 9.752.383,21	$ 111.291.394,46	$ 130.796.160,88	$ 115.762.305	$ 231.524.610
Implementación Firewall	1	$ 59.245.228	$ 60.919.830	$ 60.823.520	$ 60.329.526,00	$ 940.263,54	$ 59.389.262,46	$ 61.269.789,54	$ 60.871.675	$ 60.871.675
Garantía y Soporte	1	$ 14.811.306	$ 13.537.740	$ 22.808.820	$ 17.052.622,00	$ 5.025.520,29	$ 12.027.101,71	$ 22.078.142,29	$ 14.174.523	$ 14.174.523
									Valor Presupuesto	$ 387.680.212

De manera informativa a continuación, se relacionan gravámenes aplicables al presente proceso:

DESCRIPCIÓN	TARIFA
Estampilla Pro Desarrollo Departamental	2,0%
Estampilla Pro Electrificación Rural	0,2%
Estampilla Pro Hospitales Universitarios de Cundinamarca	2,0%
Estampilla Pro Cultura	1,0%
Estampilla Pro desarrollo de la Universidad de Cundinamarca (UDEC)	1,5%
Estampilla para el Bienestar del Adulto Mayor	2,0%
Tasa Pro Deporte y Recreación	2,5%
Total, porcentaje:	**11,2%**

NOTA: De acuerdo con el Decreto 175 de 2025 por el cual se modifica la tarifa del impuesto de timbre se informa que los cálculos presupuestales así como la responsabilidad que les asiste como sujeto pasivo de impuesto de timbre se hará efectiva si se cumplen los presupuestos de cuantía del contrato superior a 6,000 UVT ($298,794,000) e ingresos o patrimonio bruto al cierre de 2024 superiores a 30,000 UVT ($1,493,970,000); y para la aplicación del presente Decreto ambos criterios se evaluarán con la UVT de 2025 ($49,799),

El valor total del impuesto generado tendrá vigencia hasta la fecha establecida en el citado Decreto o la norma que lo modifique derogue o sustituya.

Teniendo en cuenta lo anterior y conforme al artículo 519 del Estatuto Tributario, el Impuesto de Timbre se causa cuando se cumplan los siguientes requisitos:

- La cuantía debe ser superior a 6.000 UVT (COP 298.794.000). Si el documento incorpora un valor inferior no se causa el impuesto.

- En tal sentido el contrato si se suscribe por debajo de las 6.000 UVT (COP 298.794.000), no genera impuesto de timbre.

8. APROPIACIÓN PRESUPUESTAL:

Las obligaciones que se contraen por parte de la Empresa Férrea Regional, para respaldar el presente proceso de selección y el contrato resultante de dicho proceso, cuenta con el siguiente certificado de disponibilidad presupuestal:

Número certificado disponibilidad presupuestal.	Fecha certificado disponibilidad presupuestal.
2025000467	21/10/2025

9. FORMA DE PAGO:

El valor del contrato se pagará así:

La Empresa Férrea Regional SAS pagara en Un único pago, previo recibo a satisfacción por parte del supervisor dónde conste la Implementación, Configuración y Puesta en Marcha de la Solución de Seguridad Perimetral Firewall UTM. Así como la entrega del certificado donde el contratista se obliga a prestar soporte proactivo o reactivo durante veinticuatro (24) meses contados a partir de la puesta en funcionamiento del Firewall.

Lo anterior, previa radicación de la factura o cuenta de cobro con los soportes respectivos y el correspondiente recibo a satisfacción por parte del supervisor.

La documentación requerida para proceder con el pago debe ser entregada por el contratista a la EFR en (los siguientes correos: Factura: efr@facturacion.efr-cundinamarca.gov.co Documentos Soporte: yanny.carrion@efr-cundinamarca.gov.co previo recibo a satisfacción por parte del supervisor designado por la EFR) a más tardar dentro de los (tres (3) días hábiles siguientes a la entrega de los bienes, productos o servicios sin que sobrepase el día veinticinco (25) de cada mes, fecha de cierre de recepción de facturación establecida por la EFR, para tramitar el pago el contratista deberá aportar los documentos descritos previamente y los que se mencionan a continuación:

Para el pago se deberán adjuntar:

1. Recibo a satisfacción de los bienes y/o servicios objeto del contrato.
2. Factura debidamente expedida de acuerdo con lo establecido en el Estatuto Tributario para los casos correspondientes.
3. Certificación de pago de aportes de seguridad social (salud, pensión, riesgos laborales) parafiscales (ICBF, caja de compensación, SENA), según artículo 50 de la ley 789 de 2002 y demás normas concordantes como demás documentos requeridos.

10. PLAZO DE EJECUCIÓN Y DE VIGENCIA:

El plazo de ejecución del contrato se contará desde la fecha de inicio en la plataforma SECOP II, previa aprobación de la garantía única por parte de la EFR y la expedición del registro presupuestal y hasta el 31 de diciembre de 2025.

Nota: La vigencia del licenciamiento, soporte, mantenimiento y derechos a actualizaciones será de veinticuatro (24) meses contados a partir de la implementación de la solución.

11. LUGAR DE ENTREGA:

El lugar de entrega para los elementos físicos será la calle 26 # 57 – 83 oficina piso 7 torre 8 en la ciudad de Bogotá D.C.

Debido a que las licencias son elementos intangibles, su entrega se realizará de manera digital realizando la correspondiente activación a nombre de la EFR, ya sea por medios telefónicos o a través de internet.

12. TIPO DE CONTRATO A CELEBRAR

Las partes suscribirán un contrato de Compraventa, el cual se regulará por las normas civiles y comerciales y en lo establecido en la Ley 80 de 1993, la Ley 1150 de 2007, decretos reglamentarios y demás normas aplicables o aquellas que los modifiquen, adicionen o sustituyan.

13. SUPERVISIÓN Y/ O INTERVENTORÍA:

La supervisión, será ejercida por la Directora Administrativa y Financiera o la persona que llegare a designar el Ordenador del Gasto, conforme a lo establecido en la Ley 80 de 1993, Ley 1474 de 2011 y demás normas que regulan la materia, y/o por quien este delegue.

14. OBLIGACIONES GENERALES DEL CONTRATISTA

Conforme a lo establecido en la Constitución Política de Colombia, el Estatuto General de la Contratación, el Reglamento de Contratación y el Manual de Supervisión de la EFR y demás normatividad aplicable, las obligaciones generales del contratista serán las siguientes:

1) Cumplir a cabalidad el objeto del contrato, de acuerdo con los términos y condiciones pactadas, las cuales sólo podrán ser modificadas previo acuerdo entre las partes;
2) Constituir una garantía de cumplimiento dentro de los tres (3) días siguientes a la comunicación de aceptación de la oferta.
3) Ejecutar el objeto del contrato con autonomía e independencia.
4) Actuar con suma diligencia, responsabilidad e idoneidad en la ejecución de las actividades contratadas
5) Atender los requerimientos y/o recomendaciones que durante el desarrollo del

contrato le imparta la EFR a través del supervisor para una correcta ejecución y cumplimiento de sus obligaciones contractuales;

6) Entregar los informes y productos requeridos de acuerdo con lo estipulado en el contrato, y los que le solicite el supervisor en el desarrollo y ejecución del contrato;
7) Cumplir con las obligaciones que como contratista le corresponden frente al Sistema de Seguridad Social Integral y parafiscales, y acreditar el pago oportuno de las mismas en debida forma; en concordancia con lo establecido en el Decreto 1072/15 y la Resolución 0312 de 2019 del Ministerio del Trabajo.
8) Realizar y responder por el pago de los tributos que se causen o llegaren a causar por la celebración, ejecución y liquidación del contrato (cuando a ésta hubiere lugar);
9) Presentar la respectiva factura, cuenta de cobro o su documento equivalente, de acuerdo con el régimen tributario aplicable al objeto contratado, junto con el informe de actividades realizadas en el respectivo periodo. Es obligación del Contratista conocer y presupuestar todos los gravámenes de los cuales es responsable al momento de celebrar el contrato;
10) Mantener a la EFR libre de cualquier daño o perjuicio originado en reclamaciones de terceros, que se deriven de sus actuaciones o de las de sus subcontratistas o dependientes (si fueren autorizados);
11) Responder ante las autoridades por los actos u omisiones que en el ejercicio de este contrato lleve a cabo, cuando con ellos cause perjuicio a la EFR o a terceros;
12) No ceder el presente contrato sin el consentimiento y aprobación previa, escrita y expresa de la EFR;
13) Mantener estricta reserva y confidencialidad sobre la información y documentos a que tenga acceso, maneje en desarrollo de su actividad o que llegue conocer en desarrollo del contrato;
14) Informar oportunamente de cualquier petición o amenaza, de quien actuando por fuera de la ley pretenda obligarlo a hacer u omitir algún acto o ocultar hechos que afecten los intereses de la EFR;
15) Informar oportunamente al supervisor de cualquier anomalía o dificultad que advierta en el desarrollo del contrato, y proponer alternativas de solución a las mismas;
16) Presentar con la última cuenta de cobro el pantallazo de la Declaraciones de bienes y rentas, conflictos de interés e impuesto sobre la renta y complementarios (Ley 2013 de 2019), donde se evidencie el “Retiro” en la columna “Tipo de Publicación de Información” y la "fecha de publicación”, la cual debe ser posterior a la terminación del contrato

15. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

1) Realizar todas aquellas actividades que se desprendan del objeto contractual y que sean indispensables para correcta su ejecución.
2) Participar en la reunión de inicio del proyecto, en donde el contratista deberá presentar a la supervisión del contrato de la EFR, el plan de instalación de los elementos de seguridad, además del cronograma de actividades a desarrollar, debe incluir riesgos y procedimiento de administración de cambios. Durante la fase de instalación, participar en las reuniones de seguimiento quincenales durante el

periodo de ejecución, en las cuales el contratista deberá entregar informes de ejecución y avances del proyecto.

3) Entregar los bienes objeto del contrato de acuerdo con las especificaciones técnicas, los bienes deben ser de alta calidad que cumplan con las normas y especificaciones técnicas de las regulaciones nacionales e internacionales.
4) El contratista deberá entregar todas las soluciones / equipos en los sitios/sedes indicadas por la entidad.
5) Todas las plataformas que entregue el contratista deberán ser de propósito específico, no se aceptan soluciones genéricas.
6) Asumir todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones.
7) Entregar las bandejas, tornillos, Pathc Cord de Cobre y fibra requeridos, que permita la instalación y funcionamiento de la totalidad de los elementos solicitados.
8) Los elementos no deberán ser remanufacturados, deberán ser nuevos y originales.
9) Entregar las declaraciones de importación para cada Producto entregado.
10) Entregar la garantía del producto y la identificación de originalidad.
11) Garantizar la calidad de los productos por defectos de fabricación, efectuando la reposición de los equipos sin ningún costo para la Entidad, realizando la reposición de los bienes dentro de las 48 horas siguientes al diagnóstico realizado.
12) Cambiar totalmente el equipo por uno nuevo y/o de iguales o superiores características técnicas, cuando éste presente fallas físicas no reparables, durante el tiempo de garantía objeto de este contrato, sin ningún tipo de costo adicional para la Entidad. Entendiéndose como falla, el desperfecto o no funcionamiento de cualquiera de las partes de hardware o software que conforman el equipo o sistema. Así mismo, en caso de requerirse el cambio del equipo, lo debe entregar nuevamente instalado, configurado, implementado y puesto en producción en un plazo no mayor a 24 horas en caso de pérdida total de servicio que controlan las máquinas.
13) Efectuar todas las pruebas necesarias para comprobar el correcto, perfecto y continuo funcionamiento de cada uno de los equipos entregados a plena satisfacción de acuerdo con la naturaleza de estas, estas pruebas serán coordinadas por el supervisor.
14) Tramitar ante el fabricante la suscripción y actualización del licenciamiento a nombre del EFR, con soporte técnico de la solución de seguridad (Firewall).
15) El contratista debe mantener actualizado el Firmware de todos los componentes ofertados durante el perdió de garantía y soporte, de acuerdo con las últimas versiones estables liberadas por el fabricante a solicitud del supervisor del contrato.
16) Proveer información sobre sus canales de comunicación y asignar a un ejecutivo de cuenta.
17) Prestar Soporte cuando la Entidad lo requiera. Lo anterior, para proveer mantenimiento correctivo o apoyo para cualquier cambio de configuración que se requiera durante el término de vigencia de la renovación y actualización del licenciamiento.
18) Prestar el soporte técnico y entregar informe sobre labores realizadas durante la ejecución de estas horas.

19) Los servicios deben estar orientados a apoyar presencialmente y/o remotamente en modalidad 5x8, durante 24 meses, con atención en sitio con un tiempo de respuesta máximo de cuatro (4) horas. El contratista atenderá los requerimientos de soporte a los equipos reportados y efectuará la asistencia técnica ante la presencia de fallas.
20) Entregar documento expedido por el Representante Legal donde se especifique el horario de atención 5x8, los teléfonos de contacto, la dirección de correo electrónico o mesa de ayuda para solicitud de soporte, atención de incidentes y seguimiento a los mismos. Así como el procedimiento para solicitar soporte técnico.
21) Entregar la certificación expedida por el fabricante dónde conste la garantía mínima de veinticuatro (24) meses para cada uno de los componentes de hardware, software y/o equipos o dispositivos que componen la solución de seguridad; debe incluir todos los costos de operación, en los que debe contemplar mano de obra, transporte y los repuestos.
22) Realizar la transferencia de conocimiento del servicio adquirido al personal designado por la EFR frente a las configuraciones realizadas de la solución de ciberseguridad de manera presencial o remota según las condiciones.
23) Prestar acompañamiento al personal de la EFR y gestión de requerimientos 5x8 por dos (2) años para la solución de ciberseguridad en los procesos de actualización de nuevas versiones y la gestión de casos que requieran el soporte de la herramienta durante la vigencia anual de las licencias. Las actualizaciones corresponden a todas las versiones oficiales presente oficialmente al mercado del producto adquirido.
24) Llevar a cabo la firma del acuerdo de confidencialidad de la EFR por el contratista y de su equipo de trabajo.
25) Las demás que se deriven de la naturaleza del contrato y que garanticen su cabal y oportuna ejecución.

16. OBLIGACIONES DE LA EFR S.A.S.

1) Designar al funcionario que ejercerá la supervisión y el control de ejecución del contrato, quien estará en permanente contacto con el contratista, para la coordinación de cualquier asunto que así se requiera.
2) Verificar, a través del supervisor del contrato, el cumplimiento del pago de aportes al Sistema General de Seguridad Social en Salud (EPS), Pensión (AFP) y Riesgos Laborales (ARL) y pagar los honorarios que cobre EL CONTRATISTA en la forma establecida en este documento, efectuando las retenciones legales a que haya lugar.
3) Suscribir, a través del supervisor del control de ejecución del contrato, los documentos y actas que sean necesarias durante el desarrollo del contrato.
4) Informar de manera inmediata, acerca de cualquier circunstancia que amenace vulnerar los derechos del contratista, al igual que cualquier perturbación que afecte el desarrollo normal del contrato.
5) Guardar la confidencialidad y velar por la protección de los productos y servicios propuestos por el contratista cuando a ello hubiere lugar.
6) Suministrar en forma oportuna la información solicitada por EL CONTRATISTA para una excelente ejecución del contrato y resolver las peticiones que le sean presentadas por EL CONTRATISTA en los términos consagrados en la Ley.
7) Pagar el valor del contrato en el tiempo y la forma pactada.

8) Adoptar las medidas necesarias para mantener durante el desarrollo y ejecución del contrato las condiciones técnicas y financieras existentes.
9) Cumplir y hacer cumplir las condiciones pactadas en el contrato y en los documentos que de este forman parte.

17. CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE.

De conformidad con el artículo 5 de la Ley 1150 de 2007 la selección objetivo es:

Es objetiva la selección en la cual la escogencia se haga al ofrecimiento más favorable a la entidad y a los fines que ella busca, sin tener en consideración factores de afecto o de interés y, en general, cualquier clase de motivación subjetiva. En consecuencia, los factores de escogencia y calificación que establezcan las entidades en los pliegos de condiciones o sus equivalentes tendrán en cuenta los siguientes criterios:

1. La capacidad jurídica y las condiciones de experiencia, capacidad financiera y de organización de los proponentes serán objeto de verificación de cumplimiento como requisitos habilitantes para la participación en el proceso de selección y no otorgarán puntaje, con excepción de lo previsto en el numeral 4 del presente artículo. La exigencia de tales condiciones debe ser adecuada y proporcional a la naturaleza del contrato a suscribir y a su valor.

17.1. REQUISITOS HABILITANTES Y CRITERIOS

17.1.1. REQUISITOS FINANCIEROS HABILITANTES

Los indicadores de capacidad financiera buscan establecer unas condiciones mínimas que reflejan la salud financiera de los proponentes a través de su liquidez y endeudamiento. Estas condiciones muestran la aptitud del proponente para cumplir oportuna y cabalmente el objeto del contrato.

La capacidad financiera del oferente, como requisito mínimo, se verificará con base en los factores financieros denominados: a) índice de liquidez; b) índice de endeudamiento; c) razón de cobertura de Intereses, que se revisarán con fundamento en la información reportada en el RUP frente a los estados financieros de la vigencia 2024.

En caso de que la Entidad no esté inscrita en el RUP, para la verificación de la capacidad financiera, las entidades deberán aportar una certificación suscrita por el Representante Legal, el Contador Público y/o el Revisor Fiscal, en la que señale los indicadores financieros aquí solicitados. Dichos indicadores serán los arrojados por el ejercicio contable con corte a 31 de diciembre de 2024. Esta certificación deberá acompañarse con los correspondientes estados financieros y los certificados vigentes expedidos por la Junta Central de Contadores, de vigencia de inscripción y antecedentes disciplinarios de estos profesionales (Contador Público y/o el Revisor Fiscal).

El proponente deberá acreditar los siguientes indicadores financieros, que verifican la capacidad financiera mínima requerida para un contrato como el que se pretende contratar:

Indicador	Fórmula	Valor óptimo
Índice de Liquidez	Activo Corriente / Pasivo Corriente	Mayor o igual a 1
Índice de Endeudamiento	Pasivo Total / Activo Total	Menor o igual a 0,75
Razón Cobertura de Intereses	Utilidad Operacional / Gastos de Intereses	Mayor o igual a 1,50

Nota: El oferente que presente en su RUP el indicador de cobertura de Intereses como INDETERMINADO se considerará como HABILITADO en este indicador.

Los Indicadores de Capacidad Organizacional solicitados para este proceso son:

Indicador	Fórmula	Valor óptimo
Rentabilidad del Patrimonio	Utilidad Operacional / Patrimonio	Mayor o igual a 0,08
Rentabilidad del Activo	Utilidad Operacional / Activo Total	Mayor o igual a 0,03

17.1.1.1. Ponderación de los componentes de los indicadores para proponentes plurales

A continuación, se muestra la fórmula de cómo se deberá realizar el cálculo de los Indicadores Financieros para Uniones Temporales o Consorcios, el criterio de revisión será:

a) De acuerdo con la sumatoria de las partidas individuales ponderado por su porcentaje de participación como el siguiente ejemplo*:*

Liquidez = AC 1*(%P) + AC2*(%P) / PC1*(%P) + PC 2*(%P)

En esta opción cada uno de los integrantes del oferente aporta al valor total de cada componente del indicador de acuerdo con su participación en la figura del oferente plural (unión temporal, consorcio o promesa de sociedad futura). La siguiente es la fórmula aplicable para los indicadores que son índices en la opción 1:

$$(ii)\ Indicador = \frac{\left(\sum_{i=1}^{n} Componente\ 1\ del\ indicador_i \times porcentaje\ de\ participación_i\right)}{\left(\sum_{i=1}^{n} Componente\ 2\ del\ indicador_i \times porcentaje\ de\ participación_i\right)}$$

Donde: n: es el número de integrantes del oferente plural (unión temporal, consorcio o promesa de sociedad futura).

Esta opción incentiva que el integrante del proponente plural con los mejores indicadores tenga una mayor participación en dicho proponente plural.

17.1.2. Capacidad Técnica y de Experiencia

La verificación de experiencia y de los aspectos técnicos estará a cargo del Comité Técnico, constituido al interior de la Empresa Férrea Regional. Este aspecto no otorga puntaje, pero Habilita o No Habilita la propuesta para continuar evaluando los criterios de la calificación. Se evaluará con HABILITADO o NO HABILITADO.

17.1.2.1. Aceptación de Especificaciones Técnicas

Los proponentes a través de la suscripción de la carta de presentación de la oferta manifiesta que conoce plenamente las especificaciones técnicas del proceso y en caso de ser adjudicatario se compromete a cumplirlas en su integridad.

17.1.2.2. Certificación de proveedor autorizado expedida por el fabricante

Los proponentes deberán presentar una certificación oficial emitida por el o los fabricantes, que lo acredite como proveedor autorizado del portafolio de soluciones ofertadas, indicando el nivel de membresía. Dicha certificación deberá contar con una vigencia no menor a treinta (30) días calendario a la fecha de cierre del proceso.

17.1.2.3. Experiencia Acreditada del Proponente

La experiencia acreditada del proponente será verificada de la siguiente manera, conforme se encuentra vigente la inscripción en el RUP.

Los proponentes deberán estar inscritos bajo las condiciones del Decreto Nacional 1082 de 2015, y su información de contratos ejecutados debe estar certificada en el Registro Único de Proponentes, se verificará de acuerdo con el Clasificador de Bienes y Servicios hasta el tercer nivel en al menos dos (2) de las siguientes clasificaciones:

CODIGO	DESCRIPCION
43222500	Equipo de seguridad de red
43233200	Software de seguridad y protección
81111800	Servicios de sistemas y administración de componentes de sistemas
81112200	Mantenimiento y soporte de software

Los proponentes deben presentar máximo tres (3) contratos con entidades públicas o privadas ejecutados y terminados que se encuentren inscritos en el RUP en al menos dos (2) de los anteriores códigos cuyo objeto se encuentre relacionado con el objeto a contratar, su fecha de inicio no sea mayor a los últimos tres (3) años anteriores a la fecha de cierre del presente proceso y que su sumatoria sea mayor o igual al cien por ciento (100%) del presupuesto expresado en SMMLV. (las certificaciones deberán corresponder con las mismas aportadas para acreditar la experiencia en el RUP y relacionadas en el formato establecido por la EFR para tal fin).

Estas certificaciones deberán reunir los siguientes requisitos:

1) Nombre o razón social del contratante.
2) Nombre o razón social del contratista.
3) Objeto del contrato.
4) Fecha de iniciación del contrato
5) Fecha de terminación del contrato
6) Valor del contrato.
7) Nombre y cargo de la persona competente para expedirla.
8) En caso de que la certificación sea expedida a un consorcio o unión temporal, en la misma debe identificarse el porcentaje de participación de cada uno de sus integrantes.

Nota 1. Cada certificación de contrato u orden se analizará por separado; en caso de presentar certificaciones que incluyan contratos u órdenes adicionales al principal, el tiempo y/o el valor adicional se sumará la del contrato principal, quedando esta como una sola certificación.

Nota 2. No se tendrán en cuenta contratos en ejecución.

Nota 3. Para los contratos ejecutados originalmente por consorcios o uniones temporales de los cuales haya hecho parte un integrante del proponente plural en este proceso, se validará la experiencia afectando el valor certificado por el correspondiente porcentaje de participación.

Nota 4. La experiencia de los consorcios o uniones temporales será la sumatoria de las experiencias de los integrantes que la tengan de conformidad con su porcentaje de participación.

Nota 5. Las auto certificaciones solo serán tenidas en cuenta cuando vengan acompañadas de minutas de contratos u ordenes de servicio y del acta de liquidación, actas de recibo final, y/o un documento que certifique el cumplimiento a satisfacción.

Nota 6. En caso de que no cumpla con las exigencias aquí señaladas, la experiencia certificada de esta forma no será tenida en cuenta como experiencia mínima del proponente.

Nota 7. Cuando el oferente presente contratos en los cuales conste que participó en la ejecución bajo la modalidad de consorcio o unión temporal, deberán allegarse las respectivas certificaciones en donde se exprese su porcentaje de participación en dicho consorcio o unión temporal, el cual será tenido en cuenta para la determinación de la experiencia en este proceso de contratación.

Nota 8. En caso de que la experiencia requerida se encuentre englobada en un contrato general con un objeto más amplio, se deberá discriminar el objeto específico de la experiencia acreditada y los servicios objeto de la contratación. Se aceptará que se allegue de manera adicional, la certificación de este contrato, siempre y cuando en ella se discriminen los servicios por parte de la entidad o persona que los contrató y el monto que corresponde al servicio objeto del presente proceso.

Nota 9. Cuando las certificaciones sean expedidas por particulares (personas naturales), consorcios o uniones temporales, o por parte de empresas privadas o entidades ya liquidadas, se deberá anexar además de la certificación, copia del respectivo contrato, certificación de cumplimento a satisfacción o documento que pruebe la correcta ejecución de los trabajos.

Nota 10. En caso de que algún proponente no esté inscrito en el RUP, excepción legal demostrada, este deberá acreditar experiencia con la presentación de certificaciones de máximo Tres (3) contratos debidamente ejecutados con entidades públicas y/o privadas, cuyo objeto haya sido relacionado con el objeto a contratar y que su sumatoria sea mayor o igual al cien por ciento (100%) del presupuesto del proceso expresado en SMMLV.

Nota 11. En el caso donde la información contenida en las certificaciones no sea suficiente para validar el objeto y el valor solicitado para acreditar experiencia, se deberá allegar adicional, copias de facturas, actas de liquidación y/o contratos.

Experiencia acreditada del proponente extranjero

En cuanto a personas jurídicas extranjeras con sucursal en el país: Deberán acreditar este requerimiento como lo haría una persona jurídica de origen nacional.

A. En cuanto a personas jurídicas extranjeras no inscritas en el RUP por no tener domicilio o sucursal en el país: La experiencia se contará a partir de la fecha de constitución de la empresa (esta información será tomada del documento que acredite la existencia y representación legal de la empresa o del documento que permita corroborar información, expedido por el organismo y/o autoridad competente del país de origen de esta.

B. Cuando el valor del contrato esté dado en dólares americanos (USD) se convertirá a pesos colombianos utilizando para esa conversión, la tasa representativa del mercado (TRM) vigente para la fecha de cierre del proceso. En caso de que el valor del contrato esté dado en moneda extranjera

diferente al dólar americano, se realizará su conversión a dólares americanos de acuerdo con las tasas de cambio estadísticas publicadas por el Banco de la República, teniendo en cuenta la fecha de cierre del proceso y, posteriormente, se procederá a su conversión a pesos colombianos de conformidad con la TMR vigente para la fecha de recibo final o de su terminación, según corresponda. Cuando se encuentren contratos con prestación de servicios simultáneos en la misma u otras entidades o empresas o en un mismo período de tiempo, la Empresa Férrea Regional tendrá en cuenta para efectos de la evaluación de la experiencia todo el valor acreditado, sin importar que se superpongan los períodos de tiempo. La Entidad, se reserva el derecho de verificar la información suministrada por el proponente y de solicitar las aclaraciones que considere convenientes

Nota 1: Cuando el proponente sea una persona natural o jurídica extranjera que tenga domicilio o sucursal en Colombia, relacionará la información que acredite su experiencia, en igualdad de condiciones que los nacionales. Las personas jurídicas extranjeras que no tengan establecida sucursal en Colombia acreditarán el cumplimiento de este requisito mediante la presentación de máximo tres (3) certificaciones de contratos suscritos y ejecutados por el proponente y que contengan, como mínimo:

1. Nombre o razón social del contratante.
2. Nombre o razón social del contratista.
3. Objeto del contrato (objeto esté relacionado con la venta y/o soporte de soluciones de almacenamiento SAN).
4. Fecha de iniciación del contrato
5. Fecha de terminación del contrato
6. Valor del contrato.
7. Nombre y cargo de la persona competente para expedirla.
8. En caso de que la certificación sea expedida a un consorcio o unión temporal, en la misma debe identificarse el porcentaje de participación de cada uno de sus integrantes.

El valor de cada uno de los contratos certificados, sumados o de manera individual, debe ser igual o superior al presupuesto del presente proceso expresado en salarios mínimos legales mensuales vigentes. En caso de que el proponente (personas jurídicas extranjeras que no tengan establecida sucursal en Colombia) presente más de tres (3) certificaciones de contratos, deberá indicar en la propuesta, las certificaciones que deben ser tenidas en cuenta por la entidad con el fin de ser habilitado. En caso de que el proponente no precise tal información, la entidad tomará las tres (3) primeras presentadas que cumplan las condiciones requeridas, con el propósito de habilitar al proponente. Si una de las certificaciones no cumple con lo solicitado, se tendrá en cuenta la certificación siguiente, hasta completar las mínimas solicitadas. Esta misma regla se aplicará en caso de que el proponente (personas jurídicas extranjeras que no tengan establecida sucursal en Colombia) presente copia de (los) contrato (s) acompañada del acta de liquidación.

17.1.2.4. Personal Mínimo Requerido

El proponente deberá entregar diligenciado el formato adjunto "**Carta Compromiso de equipo de Trabajo**" mediante el cual se compromete a proporcionar el personal requerido en el documento denominado "Anexo de especificaciones técnicas mínimas" a la firma del acta de inicio.

18. CRITERIOS DIFERENCIALES PARA MIPYMES

De conformidad con lo establecido en el Decreto 1860 de 2021 y con el fin de incentivar la participación de las MiPymes domiciliadas en Colombia. La entidad define que las empresas MiPymes que cumplan con lo establecido en el artículo 2.2.1.2.4.2.18 del Decreto 1860 de 2021, deben presentar máximo cinco (5) contratos con entidades públicas o privadas ejecutados y terminados que se encuentren inscritos en el RUP en al menos dos (2) de los anteriores códigos cuyo objeto se encuentre relacionado con el objeto a contratar y que su sumatoria sea mayor o igual al cien por ciento (100%) del presupuesto expresado en SMMLV.

Estas certificaciones deberán reunir los siguientes requisitos:

1) Nombre o razón social del contratante.
2) Nombre o razón social del contratista.
3) Objeto del contrato.
4) Fecha de iniciación del contrato
5) Fecha de terminación del contrato
6) Valor del contrato.
7) Nombre y cargo de la persona competente para expedirla.
8) En caso de que la certificación sea expedida a un consorcio o unión temporal, en la misma debe identificarse el porcentaje de participación de cada uno de sus integrantes.

De conformidad con el artículo 2.2.1.2.4.2.2. del Decreto 1860 de 2021 "Por el cual se modifica y adiciona el Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional, con el fin reglamentar los artículos 30, 31, 32, 34 y 35 de la Ley 2069 de 2020, en lo relativo al sistema de compras públicas y se dictan otras disposiciones",

La condición de MiPymes será verificada de acuerdo con los siguientes documentos, los cuales deberán ser presentados con la oferta.

1. Cuando la oferta es presentada por personas naturales, el proponente deberá adjuntar certificación expedida por ellos y un contador público, adjuntando copia del registro mercantil.
2. Cuando la oferta es presentada por personas jurídicas, el proponente deberá adjuntar certificación expedida por el representante legal y el contador o revisor fiscal, si están obligados a tenerlo, adjuntando copia del certificado de existencia y representación legal expedido por la Cámara de Comercio o por la autoridad competente para expedir dicha certificación.
3. En caso de proponentes plurales, deberán acreditar por lo menos uno de los integrantes la calidad de MiPymes y tiene una participación igual o superior al diez por ciento (10%) en el consorcio o la unión temporal.

Para la acreditación deberán observarse los rangos de clasificación empresarial establecidos de conformidad con la Ley 590 de 2000 y el Decreto 1074 de 2015, o las normas que lo modifiquen, sustituyan o complementen.

De acuerdo con el Articulo 2.2.1.2.4.2.18 del Decreto 1082 de 2015 adicionado por el Artículo 3 del Decreto 1860 de 2021, únicamente el proponente MIPYME NACIONAL deberá presentar para acreditar su experiencia especifica hasta cinco (5) contratos ejecutados y terminados, cuya sumatoria de los valores tomados en SMMLV del RUP sea mayor o igual al ciento (100%) valor del presupuesto asignado para este proceso.

En ambos casos los contratos que acrediten la experiencia de los proponentes deben ser mayor o igual al ciento (100%) valor del presupuesto asignado para este proceso, en la ejecución del objeto específico del presente proceso. Las certificaciones de contratos suscritos y ejecutados deberán estar 100% al cierre del presente proceso de selección y la misma deberá estar debidamente inscrita en el RUP de acuerdo con los códigos anteriormente mencionados.

19. REQUISITOS JURÍDICOS HABILITANTES:

Estos requisitos se detallarán en el pliego de condiciones correspondiente.

A esta verificación NO se le asignará puntaje, su resultado será HABILITADO o NO HABILITADO.

La evaluación de los aspectos jurídicos será realizada por el Comité Evaluador de la Empresa Férrea Regional SAS, la cual verificará los documentos que deben ser presentados de acuerdo con las disposiciones legales vigentes, y las exigencias de la invitación pública.

20. EVALUACIÓN DE LA OFERTA ECONÓMICA

Conforme lo previsto en el numeral 3° del artículo 5 de la Ley 1150 de 2007 y el articulo 2.2.1.1.2.2.2. del Decreto 1082 de 2015, en los procesos para la selección de contratistas cuyo objeto sea la adquisición o suministro de bienes y servicios de características técnicas uniformes y común utilización, se tendrá como único factor de evaluación el menor precio ofrecido de las ofertas presentadas. Es decir, la EMPRESA FERREA REGIONAL adjudicará el proceso de selección al oferente que cumpla con todas las condiciones exigidas por la entidad en el estudio previo y el pliego de condiciones, y que ofrezca el menor valor resultado de la sumatoria de los ítems.

Descripción del artículo	Cantidad	Valor Máximo Unitario establecido por la EFR
Solución de seguridad Perimetral Firewall (Hardware)	2	$ 40.554.702,00
Licenciamiento Firewall (Software)	2	$ 115.762.305,00

Implementación Firewall	1	$	60.871.675,00
Garantía y Soporte	1	$	14.174.523,00

21. SOPORTE QUE PERMITA LA IDENTIFICACIÓN, CLASIFICACIÓN, EVALUACIÓN, CALIFICACIÓN, ASIGNACIÓN, TRATAMIENTO Y MONITOREO DE LOS RIESGOS PREVISIBLES

De conformidad con lo estipulado en el artículo 2.2.1.1.1.6.3 del decreto 1082 de 2015, que cita "Evaluación del Riesgo. La Entidad Estatal debe evaluar el Riesgo que el Proceso de Contratación representa para el cumplimiento de sus metas y objetos, de acuerdo con los manuales y guías que para el efecto expida Colombia Compra Eficiente" y según lo establecido en el Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación (M-ICR-01) expedido por Colombia Compra Eficiente, donde se establecen los parámetros y los elementos a tener en cuenta a la hora de hacer el análisis del Riesgo, se efectuó el presente documento con base en la matriz de evaluación del riesgo como aparece en el respectivo anexo. (Ver documento anexo: Matriz de Riesgo).

22. ANÁLISIS QUE SUSTENTA DE LA EXIGENCIA DE LAS GARANTIAS

De conformidad con lo dispuesto en la Ley 80 de 1993, Ley 1150 de 2007 y el Decreto 1082 de 2015, el contratista se obligará a garantizar el cumplimiento de las obligaciones surgidas a favor de la EFR S.A.S., con ocasión de la ejecución del contrato y de su liquidación a través de cualquiera de los mecanismos de cobertura del riesgo señalados en el Artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015 (Contrato de seguro contenido en una póliza, patrimonio autónomo y garantía bancaria).

En este sentir se efectuó el análisis que sustenta la exigencia de mecanismos de cobertura que garantizan las obligaciones surgidas del proceso de selección y del contrato a celebrar, concluyéndose que el contratista seleccionado, se obliga a constituir a favor de la EFR S.A.S., el mecanismo de cobertura del riesgo para amparar los perjuicios que se deriven del incumplimiento del ofrecimiento o del incumplimiento del contrato, según sea el caso.

Este mecanismo deberá ser expedido por una compañía de Seguros legalmente autorizada para funcionar en Colombia o podrá consistir en una Garantía Bancaria.

La garantía cubrirá los riesgos derivados de las obligaciones legales o contractuales, para lo cual, los oferentes y el contratista seleccionado deberá constituir GARANTÍA ÚNICA a favor de la Empresa Férrea Regional S.A.S. con NIT 900.403.616-1, que ampare los siguientes riesgos:

Garantía única de Cumplimiento

Cumplimiento	Equivalente al diez por ciento (10%) del valor del contrato, con una vigencia igual al plazo de ejecución del contrato y seis (6) meses más.
Calidad y correcto funcionamiento de los bienes y equipos suministrados	Equivalente al diez por ciento (10%) del valor del contrato, con una vigencia igual al plazo de ejecución del contrato y seis (6) meses más.
Calidad del Servicio	Equivalente al diez por ciento (10%) del valor del contrato, con una vigencia igual al plazo de ejecución del contrato y seis (6) meses más.
Pago de Salarios y Prestaciones Sociales	Equivalente al cinco por ciento (5%) del valor del contrato, con una vigencia igual al plazo de ejecución del contrato. y tres (3) años más.

23. MANIFESTACIÓN DE LA CONTRATACIÓN COBIJADA POR UN ACUERDO INTERNACIONAL O UN TRATADO DE LIBRE COMERCIO VIGENTE PARA EL ESTADO COLOMBIANO

Según lo señalado en el artículo 2.2.1.2.4.1.3 del Decreto 1082 de 2015, se procedió verificar los tratados y acuerdos internacionales suscritos por Colombia, apoyando el análisis en el Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación vigencia 2024, así:

Acuerdo Comercial		¿Vigente?	Entidad Estatal incluida	Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
Alianza Pacífico	Chile	SI	NO			NO
	México	SI	NO			NO
	Perú	SI	NO			NO
Canadá		SI	NO			NO
Chile		SI	SI	SI	SI (2)	NO
Corea		SI	NO			NO
Costa Rica		SI	NO			NO
Estados Unidos		SI	NO			NO
Estados AELC		SI	NO			NO
México		SI	NO			NO
Triángulo Norte	El Salvador	SI	SI	N/A	SI (2)	NO
	Guatemala	SI	SI	N/A	SI (2)	NO
	Honduras	SI	NO			NO
Unión Europea		SI	NO			NO
Israel		SI	NO			NO

Acuerdo Comercial	¿Vigente?	Entidad Estatal incluida	Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
Reino Unido e Irlanda del Norte	SI	SI	NO		NO
Comunidad Andina	SI	N/A	N/A	NO	SI

En conclusión, el Acuerdo Comercial vigente entre Colombia y la Comunidad Andina es aplicable al presente Proceso de Contratación. (La Decisión 439 de 1998 de la Comisión de la CAN es aplicable a todos los Procesos de Contratación de las Entidades Estatales del nivel nacional, independientemente del valor del Proceso de Contratación).

24. MANIFESTACIÓN DE LA CONTRATACIÓN COBIJADA POR ACUERDOS MARCO DE PRECIOS VIGENTE

El presente documento en el numeral "6. MODALIDAD DE SELECCIÓN DEL CONTRATISTA, INCLUYENDO LOS FUNDAMENTOS JURIDICOS QUE SOPORTAN SU SELECCIÓN" menciona que, una vez consultados los Acuerdo Marco vigentes y suscritos por Colombia Compra Eficiente, se ha concluido que los mismos no satisfacen la necesidad en el entendido que no permitirán llevar a cabo la implementación de la solución teniendo en cuenta las especificaciones técnicas identificadas para satisfacer sus necesidades.

25. ANEXOS

Se adjunta Certificado de Disponibilidad Presupuestal

YANNY LUGDY CARRIÓN PEDRAZA
Directora Administrativa y Financiera
Empresa Férrea Regional S.A.S.

Elaboraron: Aspectos económicos: Darío Sotelo – DAF
Aspectos técnicos: Darío Muñetón – Contratista – DAF