ESTUDIOS PREVIOS

(De conformidad con el Manual de contratación aprobado mediante Acuerdo No 001 del 30 de marzo de 2026)

FECHA:	26 de junio de 2026
FECHA DE ACTUALIZACIÓN	01 de julio de 2026
OBJETO:	SERVICIO DE CIBERSEGURIDAD EN PREMISAS PARA LA OPERACIÓN TRANSITO RIONEGRO Y SEDES EN ADMINISTRACIÓN DE SOMOS RIONEGRO S.A.S.

1. DESCRIPCIÓN DE LA NECESIDAD

Desde la empresa SOMOS RIONEGRO S.A.S., se vienen desarrollando diversos programas orientados a apoyar al Municipio de Rionegro en la implementación de políticas, programas y proyectos relacionados con la movilidad y el transporte público de pasajeros. En este marco, se ejecuta el Contrato Marco Interadministrativo de Concesión No. 080-2011, cuyo objeto contempla la operación de registros municipales (RMA, RMI, RMC, RMT), el portal de información de infractores, y adecuaciones locativas para el fortalecimiento institucional.

Este contrato, cedido por UNE a SOMOS RIONEGRO S.A.S. mediante documento del 26 de junio de 2018, incluye en su Cláusula Cuarta – Especificaciones Técnicas, el Anexo Técnico "Solución para el Control de Movilidad, Seguridad Vial y Fortalecimiento de la Autoridad", que establece la implementación de servicios tecnológicos y operativos para la detección electrónica de infracciones, monitoreo vial, servicios digitales y apoyo a la gestión de cobro persuasivo.

En cumplimiento de dicho marco contractual, y ante los elevados índices de siniestralidad en el municipio, se han implementado dispositivos SAST (Sistemas Automáticos, Semiautomáticos y otros Medios Tecnológicos) autorizados por la Agencia Nacional de Seguridad Vial, con el fin de promover comportamientos seguros y preservar la vida de los actores viales.

Para garantizar la operación segura y confiable de estos dispositivos, así como el manejo adecuado del material probatorio generado, se requiere la implementación de oficinas de operación y centros de administración del sistema. En este contexto, se identifica la necesidad de contratar un servicio de ciberseguridad en premisas, que actúe como barrera perimetral para proteger los activos tecnológicos involucrados.

Justificación técnica y operativa de la necesidad

La operación del sistema SAST y los servicios digitales asociados al contrato involucran el procesamiento, almacenamiento y transmisión de información altamente sensible, como:

- Material probatorio generado por dispositivos de detección electrónica.
- Datos personales de ciudadanos vinculados a trámites de tránsito.
- Conexiones a bases de datos externas (RUNT, SIMIT).

- Aplicativos operativos para la gestión de comparendos, licencias, traspasos, y atención al ciudadano.

Ante este panorama, la implementación de dispositivos de seguridad en premisas es indispensable por las siguientes razones:

Protección de activos tecnológicos críticos: Cada sede alberga infraestructura que soporta la operación diaria. Sin una barrera perimetral robusta, estos activos quedan expuestos a accesos no autorizados, intrusiones, malware y pérdida de evidencia digital.

Cumplimiento normativo: El manejo de datos personales y material probatorio exige cumplir con la Ley 1581 de 2012, estándares de seguridad informática, y principios de cadena de custodia digital.

Segmentación operativa: Cada sede cumple funciones específicas. La instalación de dispositivos permite segmentar redes, aplicar políticas diferenciadas y monitorear eventos en tiempo real.

Continuidad operativa: Un incidente de seguridad puede interrumpir trámites ciudadanos, afectar registros y generar pérdida de información crítica.

Proyección tecnológica: La infraestructura está en constante crecimiento. Los dispositivos permiten escalabilidad, integración con sistemas de monitoreo y trazabilidad.

Características del servicio requerido

El servicio contempla la instalación y administración de equipos tipo firewall, cuya función principal es:

- Bloquear accesos no autorizados a la red institucional.
- Prevenir intrusiones y proteger datos confidenciales relacionados con la operación del sistema SAST.
- Aplicar políticas de seguridad que regulen el tráfico de red, permitiendo únicamente comunicaciones legítimas.
- Detectar y bloquear amenazas en tiempo real mediante tecnologías de análisis de patrones recurrentes (RPD).
- Filtrar contenido web inapropiado o no autorizado, reduciendo riesgos derivados de la navegación.

Ubicación estratégica de los equipos

Para garantizar una cobertura efectiva y segmentada de la operación, se requiere la instalación de equipos de seguridad perimetral en premisas, distribuidos de la siguiente manera:

Sede Administrativa SOMOS Rionegro

Abarca el área administrativa, programas institucionales como BiciRio, Semaforización, ZER y otros proyectos de movilidad. El equipo protegerá los activos tecnológicos asociados a la gestión documental, planificación operativa y servicios digitales transversales.

Sede Tránsito

Centro operativo de trámites como registro inicial, traspasos vehiculares, licencias de conducción, certificados de tradición, comparendos, acuerdos de pago, revisión de fotodetecciones y atención al ciudadano. Esta sede mantiene conexión directa con las cámaras de fotodetección, bases de datos externas y aplicativos operativos, lo que exige una infraestructura segura, resiliente y proyectada para el crecimiento tecnológico.

Sede Morelia

Punto de operación tránsito, con funciones de validación de infracciones, atención ciudadana y soporte a la gestión de movilidad. El equipo garantizará la protección de los sistemas locales, la continuidad operativa y la integridad de la información procesada.

La contratación del servicio de ciberseguridad en premisas es una medida técnica, legal y operativa necesaria para proteger la infraestructura tecnológica, garantizar la validez del material probatorio, y asegurar la continuidad de los servicios prestados por SOMOS RIONEGRO S.A.S. en el marco del contrato interadministrativo.

2. OBJETIVO PARA CONTRATAR

SERVICIO DE CIBERSEGURIDAD EN PREMISAS PARA LA OPERACIÓN TRANSITO RIONEGRO Y SEDES EN ADMINISTRACIÓN DE SOMOS RIONEGRO S.A.S.

2.1. ALCANCE

El alcance del presente contrato tiene como objetivo brindar por un periodo de 06 meses un servicio Plan Premium administrado de ciberseguridad en premisas para la operación tránsito y sedes administrativas de SOMOS Rionegro S.A.S. como se detalla a continuación:

Sede SOMOS
Dirección: Calle 42 No. 69A-41
Municipio: Rionegro
Solución Ciberseguridad On-Premises
1 UTM Firewall 100F

Sede TRÁNSITO
Dirección: CR 47 CL 62 - 50
Municipio: Rionegro
Solución Ciberseguridad On-Premises
1 UTM Firewall 100F

Sede Morelia
Dirección: 6.126200969434721, -75.41715058678979
Municipio: Rionegro
Solución Ciberseguridad On-Premises
1 UTM Firewall 60F

3. ESPECIFICACIONES TÉCNICAS

En la siguiente tabla se describe las especificaciones mínimas requeridas para el dispositivo tecnológico CIBERSEGURIDAD

ITEM	DESCRIPCIÓN	CANTIDAD DE EQUIPOS	PLAZO (MESES)
1	Seguridad en Premisas, equipo Firewall 100F + Cambios en Políticas de Ciber Seguridad + Monitoreo e Informes de Ciber Seguridad + Reingeniería de Políticas de Ciber Seguridad	02	06
2	Seguridad en Premisas, equipo Firewall 60F + Cambios en Políticas de Ciber Seguridad + Monitoreo e Informes de Ciber Seguridad + Reingeniería de Políticas de Ciber Seguridad	01	06

Ficha Técnica Equipo 100F

	FORTIGATE 100F	FORTIGATE 101F
Especificaciones de hardware		
Puertos GE RJ45	12	
Puertos de administración GE RJ45/HA/DMZ	1/2/1	
Ranuras de GE SFP	4	
10 ranuras de GE SFP+	2	
Puertos GE RJ45 WAN	2	
Puertos GE RJ45 o SFP compartidos*	4	
Puerto USB	1	
Puerto de consola	1	
Almacenamiento interno	—	1x 480 GB SSD
Transceptores incluidos	0	
Rendimiento del sistema, mezcla empresarial de tráfico		
Rendimiento de IPS [2]	2.6 Gbps	
Rendimiento de NGFW [2,4]	1.6 Gbps	
Rendimiento de protección contra amenazas [2,5]	1 Gbps	
Rendimiento del sistema		
Rendimiento del firewall (paquetes de UDP de 1518/512/64 bytes)	20/18/10 Gbps	
Latencia de firewall (paquetes UDP de 64 bytes)	5 µs	
Rendimiento del firewall (paquetes por segundo)	15 Mpps	
Sesiones concurrentes (TCP)	1.5 millones	
Sesiones nuevas/Segundo (TCP)	56,000	
Políticas de Firewall	10,000	
Rendimiento de VPN IPsec (512 bytes) [1]	11.5 Gbps	
Túneles de VPN IPsec de puerta de enlace a puerta de enlace	2,500	
Túneles de VPN IPsec del cliente a la puerta de enlace	16,000	
Rendimiento SSL-VPN	750 Mbps	
Usuarios de SSL-VPN concurrente (máximo recomendado, modo de túnel)	500	
Rendimiento de inspección de SSL (IPS, HTTPS promedio) [3]	1 Gbps	
CPS de inspección de SSL (IPS, HTTPS promedio) [3]	1,800	
Sesión concurrente de inspección de SSL (IPS, HTTPS promedio) [3]	135,000	
Rendimiento de Application Control (HTTP 64K) [2]	2.2 Gbps	
Rendimiento de CAPWAP (HTTP 64K)	15 Gbps	
Dominios virtuales (Predeterminado/máximo)	10/10	
Número máximo de FortiSwitches admitidos	24	
Número máximo de FortiAP (modo túnel/total)	128/64	

	FORTIGATE 100F	FORTIGATE 101F
Número máximo de FortiToken	5,000	
Número máximo de FortiClient registrados	600	
Configuraciones de alta disponibilidad	Activo/activo, activo/pasivo, agrupamiento	
Dimensiones		
Altura x Ancho x Largo (pulgadas)	1.73 x 17 x 10	
Alto x Ancho x Largo (mm)	44 x 432 x 254	
Factor de forma	Montaje en rack, 1 RU	
Peso	7.25 lb (3.29 kg)	7.56 lb (3.43 lb)
Entorno		
Energía requerida	100-240 V CA, 50-60	
Corriente máxima	100 V/1 A, 240 V/0.5 A	
Consumo de energía (Promedio/máximo)	35.1 W/38.7 W	35.3 W/39.1 W
Disipación térmica	119.77 BTU/h	121.13 BTU/h
Entorno		
Temperatura de funcionamiento	32-104°F (0-40°C)	
Temperatura de almacenamiento	-31-158°F (-35-70°C)	
Altitud de funcionamiento	Hasta 7,400 pies (2,250 m)	
Humedad	10 a 90 % sin condensación	
Nivel de ruido	40.4 dBA	
Cumplimiento	FCC Parte 15B, Clase A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certificaciones	Laboratorio de ICSA: Firewall, IPsec, IPS, Antivirus, SSL-VPN; IPv6	

Ficha Técnica Equipo 60F

	FORTIGATE 60F	FORTIGATE 61F	FORTIWIFI 60F	FORTIWIFI 61F
Hardware Specifications				
GE RJ45 WAN / DMZ Ports	2 / 1	2 / 1	2 / 1	2 / 1
GE RJ45 Internal Ports	5	5	5	5
GE RJ45 FortiLink Ports (Default)	2	2	2	2
Wireless Interface	-	-	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2
USB Ports	1	1	1	1
Console (RJ45)	1	1	1	1
Internal Storage	-	1 × 128 GB SSD	-	1 × 128 GB SSD
System Performance — Enterprise Traffic Mix				
IPS Throughput [2]	1.4 Gbps			
NGFW Throughput [2, 4]	1 Gbps			
Threat Protection Throughput [2,5]	700 Mbps			
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10/10/6 Gbps			
Firewall Latency (64 byte UDP packets)	3.3 µs			
Firewall Throughput (Packets Per Second)	9 Mpps			
Concurrent Sessions (TCP)	700 000			
New Sessions/Second (TCP)	35 000			
Firewall Policies	5000			
IPsec VPN Throughput (512 byte) [1]	6.5 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels	200			
Client-to-Gateway IPsec VPN Tunnels	500			
SSL-VPN Throughput	900 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200			
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	630 Mbps			
SSL Inspection CPS (IPS, avg. HTTPS) [3]	400			
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000			
Application Control Throughput (HTTP 64K) [2]	1.8 Gbps			
CAPWAP Throughput (HTTP 64K)	6 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiSwitches Supported	24			
Maximum Number of FortiAPs (Total / Tunnel Mode)	64 / 32			
Maximum Number of FortiTokens	500			
High Availability Configurations	Active-Active, Active-Passive, Clustering			
Dimensions				
Height x Width x Length (inches)	1.5 × 8.5 × 6.3			
Height x Width x Length (mm)	38.5 × 216 × 160 mm			
Weight	2.23 lbs (1.01 kg)			
Form Factor	Desktop			
Radio Specifications				
Multiple User (MU) MIMO	-	-	3×3	
Maximum Wi-Fi Speeds	-	-	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz	
Maximum Tx Power	-	-	20 dBm	
Antenna Gain	-	-	3.5 dBi @ 5 GHz, 5 dBi @ 2.4 GHz	

Plan Premium

Dada la criticidad de la operación, el volumen de datos procesados, la sensibilidad del material probatorio y la necesidad de garantizar alta disponibilidad, trazabilidad y cumplimiento normativo, el servicio requerido debe ser de tipo Premium

Atributos	Estándar (Web filtering)	Avanzado (UTP)	Premium (UTP)
Filtrado de contenido basado en categorías	•	•	•
Filtrado web	•	•	•
VPN Site to Site ipsec	5 max	10 max	10 max

VPN client to Site ipsec	5 max	10 max	10 max
Firewall capa 3, 4	x	•	•
Control de aplicaciones	•	•	•
Enrutamiento basado en aplicaciones	x	•	•
Conectividad segura Cifrada	•	•	•
Balanceo Dinámico	•	•	•
Administración	Centralizada	Centralizada	Con posibilidad de Coadministración
DIA (direct internet access)	•	•	•
Optimización aplicaciones SaaS basado en SLA +	•	•	•
Reporteria	x	•	•
Firewall capa 7	x	•	•
Integración a Directorio Activo*	x	•	•
Antivirus perimetral	x	•	•
IPS/IDS	x	•	•
File filtering	x	•	•

Condiciones Especiales

Los Servicios Administrados de Ciberseguridad contemplan los siguientes componentes:

- Configuración de Políticas.
- Monitoreo.
- Informes.
- Reingeniería de Políticas

Cada uno de los anteriores con su alcance y ANS.

Módulo/servicio	PLAN
Cambios en políticas de Ciberseguridad	06 cambios/mes. •Respuesta en 8 horas, 5x8
Monitoreo (Básico)	Disponibilidad de infraestructura. 7x24** •Monitoreo de dos (2) dispositivo UTM y un (1) equipo en respaldo*** •Alertas de Seguridad. 7x24
Informes de Ciberseguridad (Básico)	•De incidentes de disponibilidad. Mensual, entrega en los 5 primeros días hábiles del mes. Informes de Seguridad. Mensual, entrega los 10 primeros días hábiles del mes.
Reingeniería de políticas de Ciberseguridad	Análisis y rediseño. 1 al año

COMPONENTES IMPLICADOS PERÍMETRO DE SEGURIDAD DIGITAL

- **Firewall**: este servicio provee un primer nivel de seguridad que permite filtrar el tráfico de entrada y salida a la red de acuerdo con una lista de reglas definida. El Firewall es un servicio básico que suele complementarse con otros servicios de seguridad para ayudar a prevenir eventos que impacten la confidencialidad, integridad y disponibilidad de la información y servicios de la compañía. A través de esta funcionalidad se protege el acceso a segmentos de red de importancia para la compañía, así como a puertos TCP/UDP de servicios críticos para el negocio.

- **VPN**: las Redes Privadas Virtuales (VPN, por sus siglas en inglés) evita que terceros no autorizados puedan interceptar la información que está viajando de entre dos nodos de la red a través de una red insegura como Internet. El servicio VPN permite ingresar de manera segura a redes privadas y/o servicios del cliente hospedados en los Data Center Tigo. Las VPN ayudan a mantener la confidencialidad de la información que viaja entre diferentes puntos de la red.

- **Antivirus Gateway (Malware Protection):** Proporciona una protección de red contra una variedad de amenazas incluyendo códigos maliciosos conocidos y desconocidos (malware), Advanced Target Attacks (ATA) y Advanced Persistent Threats (APT). Este servicio proporciona una primera protección frente a ataques externos que pueden poner en riesgo la integridad o disponibilidad de la información y servicios críticos del negocio.

- **Application Control (Firewall Capa 7):** análisis de tráfico hasta la capa 7 de aplicaciones. Esta protección es usada para controlar aplicaciones riesgosas y no deseadas en la red, por ejemplo: juegos, vídeos, música, voz sobre IP, transferencia de archivos, Bases de Datos, deportes, entre otras, controlando aplicaciones evasivas o peer- to-peer, como por ejemplo BitTorrent o Skype. Así mismo permite tener control del tráfico dependiendo del sistema operativo del dispositivo (IOS, Android, Windows, OSX). Esta funcionalidad es un complemento que disminuye el riesgo de ataques que afecten la confidencialidad, integridad o disponibilidad de la información.

- **IDS/IPS:** Proporciona protección ante amenazas a nivel de red empleando una Base de Datos de firmas que periódicamente son actualizadas por el fabricante de acuerdo con las nuevas amenazas. El servicio IDS/IPS previene ataques que pongan en riesgo principalmente la integridad y disponibilidad de información y servicios críticos de la Compañía.

- **WCF (Filtrado de Contenidos):** El filtrado de contenido es un método que permite controlar la información que un usuario de Internet puede ver. A través de este servicio la Compañía puede lograr que la navegación a Internet sea más productiva y segura para sus colaboradores, evitando el acceso a páginas de contenidos no deseados como pornografía, drogas, juegos, entretenimiento, racismo, entre otros.

- **Full UTM (Unified Threat Management):** incluye los servicios de Firewall, VPN Client-to-Site (C2S), VPN Site-to-Site (S2S), WCF, IDS/IPS, Application Control, Antivirus Gateway.

SERVICIOS ADMINISTRADOS DE CIBERSEGURIDAD

Los Servicios Administrados de Ciber Seguridad están enfocados en administrar y soportar servicios de Ciber Seguridad, así como las plataformas que los soportan y o incidentes de Ciber Seguridad.

A través de los Servicios Administrados de Ciber Seguridad se realiza:

- Descubrimiento y protección de Amenazas.
- Respuesta a Incidentes.
- Gestión de Políticas.
- Cumplimiento -cuando se requiera- de requerimientos regulatorios (por ejemplo: PCI, HIPPA).
- Monitoreo de los Servicios de Ciber Seguridad, plataformas de red y sistemas de TI.

BENEFICIOS

Los beneficios más relevantes de los servicios administrados de Seguridad.

- Disminución de carga operativa delegando en especialistas y experiencia de la administración de la seguridad perimetral.
- Planeación predecible de costos de administración de Ciber Seguridad sin inversiones asociadas y que estén alineados con las expectativas del negocio.
- Visibilidad y control de las políticas de seguridad para facilitar la toma de decisiones en los gastos en infraestructura de TI.
- Flexibilidad para realizar cambios sobre políticas de seguridad a través de un equipo experto que realiza la gestión completa de los servicios de Ciber Seguridad
- Disminución de riesgos operativos con la notificación proactiva y correlación de eventos de Ciber seguridad.

Configuración de Políticas

La dinámica de cada negocio, así como las amenazas y vulnerabilidades que surgen cada día obliga a las empresas a actualizar las políticas de Ciberseguridad periódicamente de forma preventiva o ante un evento. Cada uno de los Planes de Oferta de Servicios Administrados de Ciberseguridad tiene definido un número máximo de cambios mensuales en los servicios de Ciberseguridad contratados.

Definición de Cambio: Los cambios comprenden aquellas actividades que conlleven a la creación, modificación y/o eliminación de políticas, usuarios y configuraciones de los servicios de Ciberseguridad contratados por el cliente y que se encuentran en operación. La contabilización de estos cambios se inicia después del periodo de Estabilización del Servicio de Ciberseguridad contratado.

Comprenden aquellas se considerará una solicitud de cambio:

- Cada requerimiento que realice el cliente a través de los canales formales definidos.

- La aplicación a un servicio de Ciberseguridad contratado. Es decir que si un requerimiento solicitado contiene cambios para diferentes servicios (por ejemplo, Firewall y Filtrado de Contenidos), se considerará como dos solicitudes de cambio independientes.
- Los cambios que se aplican sobre servicios de Ciberseguridad en Premisas se contabilizan por toda la Organización del Cliente (no por dispositivo).
- Todos los cambios contemplados en el servicio se consideran realizarse de forma remota desde el SOC.
- Cambios que se encuentren dentro del alcance del servicio de Ciberseguridad contratado. Aquellas solicitudes de cambio que exceden el alcance de los servicios contratados implican modificación de la Oferta Comercial contratada y deberán canalizarse a través del Ejecutivo de Ventas ya que conllevan un cambio en el cargo mensual del servicio de Ciber Seguridad.

Monitoreo Proactivo

Los planes de Servicios Administrados de Ciberseguridad incluyen el seguimiento 7x24 a la disponibilidad y salud de la infraestructura, las alertas de seguridad y correlación de eventos.

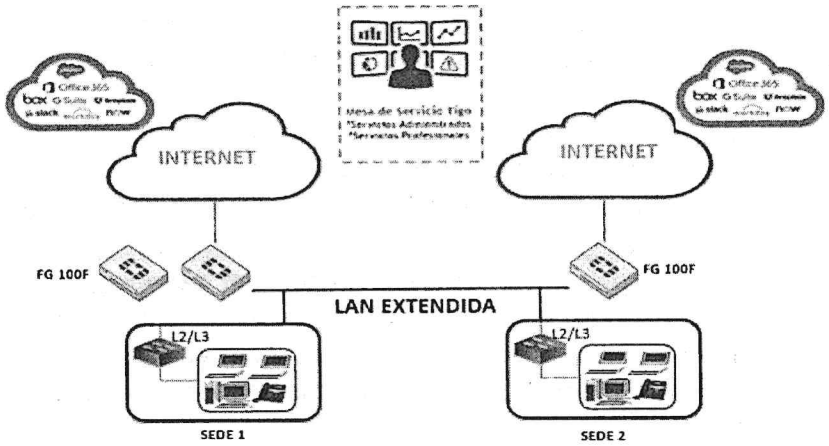
Definiciones:

- **Monitoreo de Disponibilidad Infraestructura**: consiste en el seguimiento de variables como consumo de CPU, memoria o ancho de banda en interfaces del (los) equipos que soportan los servicios de Ciber Seguridad. En los servicios VPN no se incluye el monitoreo de equipos remotos de terceros, ni de enlaces de comunicación de backbone, metro ni de último kilómetro.

- **Monitoreo de Alertas de Seguridad**: identificación de comportamientos anómalos en casos como:
  - Detección de firmas en servicios como IDS/IPS o Anti-Malware.
  - Direcciones IP o puertos TCP/UDP origen o destino asociados a reglas de servicio Firewall.
  - La cantidad de renegociaciones de las fases de la VPN.
  - Tráfico hacia URLs/aplicaciones permitidas o requerimientos realizados hacia URLs/aplicaciones no permitidas.

TOPOLOGIA DE LA SOLUCION

La siguiente topología incluye los ítems de seguridad en premisas para las sedes a través de los equipos Firewall y los servicios administrados de Ciberseguridad.



CONSIDERACIONES TÉCNICAS

- En sede Somos se destinará un (01) equipo Firewall 100F y en la sede Transito un (01) equipo Firewall 100F, los cuales recibirán el canal de Internet existente en cada sede y brindará protección perimetral, teniendo en cuenta que para cada sede incluye (full UTM).
- En la sede Morelia se destinará un (01) equipo Firewall 60F con un plan básico UTM

4. VALOR Y FORMA DE PAGO

4.1 VALOR

El valor total del contrato es de CINCUENTA MILLONES CIENTO VEINTIDOS MIL OCHOCIENTOS PESOS M/L ($ 50.122.800) retenciones a diera lugar.

SEDE	DESCRIPCIÓN	CANTIDAD MESES	VALOR MENSUAL (IVA INCLUIDO)	VALOR TOTAL (IVA INCLUIDO)
SOMOS	Seguridad en Premisas (1 equipo Firewall 100F) + Cambios en Políticas de Ciber Seguridad + Monitoreo e Informes de Ciber Seguridad + Reingeniería de Políticas de Ciber Seguridad	06	$ 3.903.200	$ 23.419.200
TRÁNSITO	Seguridad en Premisas (1 equipo Firewall 100F) + Cambios en Políticas de Ciber Seguridad + Monitoreo e Informes de Ciber Seguridad + Reingeniería de Políticas de Ciber Seguridad	06	$ 3.903.200	$ 23.419.200
MORELIA	Seguridad en Premisas (1 equipo Firewall 60F) + Cambios en Políticas de Ciber Seguridad + Monitoreo e Informes de Ciber Seguridad + Reingeniería de Políticas de Ciber Seguridad	06	$547.400	$ 3.284.400
TOTAL				**$50.122.800**

4.2 FORMA DE PAGO

La entidad pagara al contratista, mediante actas parciales de avance mes vencido por el servicio ciberseguridad premisas, acompañados de factura, informe de actividades por parte del contratista, informe de supervisión por parte de la entidad, pago por concepto de seguridad social, parafiscales, cedula y tarjeta de Contador Público o Revisor fiscal según sea el caso, cuenta bancaria y demás requisitos exigidos por el área financiera y Supervisora del contrato.

5. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de SEIS (06) MESES, contados a partir desde la suscripción del acta de inicio, sin exceder el 31 de diciembre de 2026.

6. LUGAR DE EJECUCIÓN

Municipio de Rionegro, en la sede principal de la empresa SOMOS RIONEGRO S.A.S.

7. INFORMACION PRESUPUESTAL

CDP	CÓDIGO	FONDO	DESCRIPCION	VALOR	FECHA
556	91.2.3.2.02.02.008	1	Servicios prestados a las empresas y servicios de producción	$50.122.800	30/06/2026

8. IMPUESTOS TASAS Y CONTRIBUCIONES

El proponente debe tener en cuenta todos los gastos e impuestos que puedan afectar sus precios y hayan de causarse por la ejecución del contrato, tales como: Impuesto a la Renta, Industria y Comercio, timbre y publicación, si son del caso; el valor que ocasione la constitución de garantías, así como las deducciones, retenciones y el impuesto al valor agregado IVA sobre la utilidades del contrato, y otras a que haya lugar de acuerdo con las normas vigentes (Reteica, Estampilla Pro-Cultura, Estampilla Pro-Hospitales, Pro-Adultos, Pro-Deporte) así:

IMPUESTO DE INDUSTRIA Y COMERCIO (RETEICA):	8/1000
ESTAMPILLA PRO-HOSPITAL:	1% del valor total del contrato
ESTAMPILLA PRO POLITÉCNICO	0.4 % del valor total del contrato
ESTAMPILLA PRO ADULTO MAYOR	3.0 % del valor total del contrato (En caso de que aplique)
ESTAMPILLA PRO- CULTURA	1.0%
ESTAMPILLA PRO-DEPORTE	2.5% De acuerdo con la condición de cada contratista y a la naturaleza del contrato.

NOTA: Se adjunta la certificación expedida por el área financiera de la entidad, en la que se establece el régimen de estampillas, impuestos y demás deducciones aplicables al presente proceso contractual.

9. ANALISIS DEL MERCADO

La entidad, vela para que se lleven a cabo los procedimientos y etapas estrictamente necesarios para seleccionar la propuesta que resulte más afín a los intereses de la entidad, así mismo, busca que toda actuación en la ejecución y cumplimiento de las obligaciones a cargo de los contratistas seleccionados se desarrolle optimizando costos y evitando dilaciones o perjuicios para una de las partes.

Con el propósito de identificar una oferta favorable, idónea y ajustada a las necesidades de la entidad para la adquisición del servicio de ciberseguridad para SOMOS RIONEGRO S.A.S., se realizó un sondeo de precios en el mercado mediante la solicitud de cotizaciones a tres (3) proveedores del sector, en cumplimiento de lo dispuesto en el numeral 9.1.2 del Manual de Contratación, relativo a los requisitos para la contratación directa, y en el artículo 9.1.2.1, referente a la etapa precontractual, específicamente al análisis del sector y al análisis del mercado. Este ejercicio permitió obtener información técnica, comercial y económica suficiente para determinar el presupuesto estimado del proceso y verificar las condiciones de oferta existentes en el mercado.

SOMOS moviendo futuro

Comparación de precios entre diferentes proveedores

GENERAL PROVISIONS GROUP S.A.S

Item	Descripcion	Meses	Valor Unitario	Valor Total
1.1	Seguridad en Premisas (1 FortiGate 60F) - Sede Morelia	6	$ 538.200,00	$ 3.229.200,00
1.2	Seguridad en Premisas (1 FortiGate 100F) - Sede SOMOS	6	$ 3.936.000,00	$ 23.616.000,00
1.3	Seguridad en Premisas (1 FortiGate 100F) - Sede Transito	6	$ 3.870.400,00	$ 23.222.400,00
			SUBTOTAL	$ 50.067.600,00
			IVA	$ 9.512.844
			TOTAL	$ 59.580.444

SERTECOPY

Item	Descripcion	Meses	Valor Unitario	Valor Total
1.1	Seguridad en Premisas (1 FortiGate 60F) - Sede Morelia	6	$ 533.600,00	$ 3.201.600,00
1.2	Seguridad en Premisas (1 FortiGate 100F) - Sede SOMOS	6	$ 3.804.800,00	$ 22.828.800,00
1.3	Seguridad en Premisas (1 FortiGate 100F) - Sede Transito	6	$ 3.804.800,00	$ 22.828.800,00
			SUBTOTAL	$ 48.859.200,00
			IVA	$ 9.283.248
			TOTAL	$ 58.142.448

TIGO UNE

Item	Descripcion	Meses	Valor Unitario	Valor Total
1.1	Seguridad en Premisas (1 FortiGate 60F) - Sede Morelia	6	$ 460.000,00	$ 2.760.000,00
	Seguridad en Premisas (1 FortiGate 100F) - Sede SOMOS	6	$ 3.280.000,00	$ 19.680.000,00
1.3	Seguridad en Premisas (1 FortiGate 100F) - Sede Transito	6	$ 3.280.000,00	$ 19.680.000,00
			SUBTOTAL	$ 42.120.000,00
			IVA	$ 8.002.800
			TOTAL	$ 50.122.800

SOMOS moviendo futuro

MEJOR OFERTA

PROVEEDOR	TIGO UNE	
OFERTA	$	50.122.800

10. MODALIDAD DE CONTRATACIÓN

MODALIDAD	CAUSAL DE MODALIDAD
CONTRATACIÓN DIRECTA.	Se configura una causal de contratación directa estipulada en el Manual de Contratación de SOMOS RIONEGRO S.A.S., artículo 9 contratos cuyo presupuesto oficial sea hasta 350 SMLMV, literal K) contratos de Servicios

11. OBLIGACIONES

11.1 OBLIGACIONES GENERALES DEL CONTRATISTA

1. Cumplir con el objeto del contrato y las especificaciones técnicas, las cuales para todos los efectos forman parte integral del mismo.
2. Obrar con lealtad y buena fe en todas las etapas contractuales, evitando dilaciones y entorpecimientos que puedan afectar la ejecución.
3. Presentar las pólizas del contrato dentro de los cinco (05) días hábiles siguientes a la suscripción del mismo
4. Suscribir el acta de liquidación del contrato y las modificaciones que se generen durante su ejecución.
5. Realizar los actos necesarios y tomar las medidas conducentes para el debido y oportuno cumplimiento de las obligaciones contractuales.
6. Asumir el pago de los impuestos, gravámenes, aportes parafiscales y servicios de cualquier género que establezcan las leyes colombianas.
7. Aportar certificación expedida por el revisor fiscal (cuando exista, según lo establecido por la ley) o por el representante legal, que acredite el cumplimiento de las obligaciones con el Sistema de Seguridad Social Integral (salud, pensiones y riesgos laborales), así como los aportes a las Cajas de Compensación Familiar, el Servicio Nacional de Aprendizaje (SENA) y el Instituto Colombiano de Bienestar Familiar (ICBF), cuando a ello hubiere lugar. Esta certificación deberá adjuntarse al informe del supervisor y será verificada por este.
8. Informar oportunamente al supervisor sobre cualquier variación en el régimen de imposición por IVA u otras cargas tributarias, ya sea por los bienes o servicios contratados o por cambios en el régimen tributario del contratista.
9. Cumplir con las demás obligaciones especiales que se deriven del objeto contractual.

11.2 OBLIGACIONES ESPECIFICAS DEL CONTRATISTA

1. Cumplir con el objeto contractual y las especificaciones técnicas descritas en los estudios previos.
2. Cumplir y garantizar las especificaciones técnicas del dispositivo **firewall**, incluyendo hardware, sistema operativo y desempeño.
3. Garantizar la actualización y monitoreo continuo (7x24) de los equipos.
4. Asegurar la compatibilidad del firewall con los dispositivos **SAST** a cargo de la empresa.

5. Garantizar el correcto funcionamiento del firewall durante toda la vigencia del contrato.
6. Brindar soporte técnico 24/7 para la resolución de incidencias y fallos en la operación del dispositivo.
7. Aplicar actualizaciones periódicas de software y firmware para mantener la seguridad y eficiencia del firewall.
8. Implementar medidas de seguridad avanzadas para proteger la red contra amenazas cibernéticas.
9. Proveer herramientas de monitoreo en tiempo real para la detección de vulnerabilidades y ataques.
10. Informar oportunamente a la empresa sobre cualquier intento de acceso no autorizado o amenaza detectada.
11. Realizar mantenimientos preventivos periódicos conforme a las mejores prácticas del fabricante.
12. Atender mantenimientos correctivos en caso de fallas, dentro de los tiempos de respuesta establecidos en el contrato.
13. Reemplazar el equipo en caso de fallas críticas o irreparables, sin generar costos adicionales para la empresa.
14. Cumplir con todas las demás obligaciones que se deriven de las especificaciones técnicas, la propuesta técnica presentada y la ejecución del objeto contractual.

12. MATRIZ DE RIESGOS

No	Riesgo Previsible	Asignación	Probabilidad	Impacto	Tratamiento
1	Incumplimiento en la implementación de la solución de ciberseguridad dentro de los plazos establecidos.	Contratista	Media	Alto	Establecer cronograma detallado, seguimiento por el supervisor, aplicación de multas y cláusula penal en caso de incumplimiento.
2	Fallas en la configuración de los equipos o herramientas de seguridad que generen vulnerabilidades en la infraestructura tecnológica.	Contratista	Media	Alto	Implementar procedimientos de configuración segura, validación técnica, pruebas de funcionamiento y aceptación por parte de la supervisión.
3	Interrupción parcial del servicio durante actividades de instalación, actualización o mantenimiento.	Contratista	Media	Alto	Programar ventanas de mantenimiento autorizadas, implementar planes de contingencia y mecanismos de reversión (rollback).
4	Ataques cibernéticos sofisticados o de fuerza mayor que superen las capacidades razonables de mitigación de la solución implementada.	Compartido	Baja	Alto	Mantener políticas de actualización permanente, monitoreo continuo, respuesta a incidentes y coordinación entre las partes.

5	Demoras en la atención de incidentes de seguridad conforme a los niveles de servicio (SLA).	Contratista	Media	Alto	Establecer ANS/SLA, tiempos máximos de respuesta y solución, con seguimiento permanente por parte del supervisor.
6	Divulgación, pérdida o acceso no autorizado a información institucional durante la ejecución del contrato.	Contratista	Baja	Alto	Suscripción de acuerdos de confidencialidad, controles de acceso, cifrado de información y cumplimiento de políticas de seguridad de la información.
7	Incompatibilidad de la solución con la infraestructura tecnológica existente de SOMOS RIONEGRO S.A.S.	Contratista	Baja	Alto	Realizar diagnóstico previo, validaciones técnicas y pruebas de interoperabilidad antes de la implementación definitiva.
8	Desactualización de firmas, licencias o componentes de seguridad durante la vigencia contractual.	Contratista	Media	Alto	Mantener vigentes las licencias, actualizaciones automáticas y soporte del fabricante durante toda la ejecución contractual.
9	Cambios tecnológicos o de arquitectura definidos por la entidad que requieran ajustes no previstos inicialmente.	Contratante	Baja	Medio	Gestionar modificaciones contractuales cuando técnicamente procedan y exista disponibilidad presupuestal.
10	Daños ocasionados a equipos institucionales por manipulación inadecuada durante la prestación del servicio.	Contratista	Baja	Alto	Personal certificado, protocolos técnicos de intervención y obligación de reparar o responder por los daños ocasionados.
11	Falta de disponibilidad del personal técnico especializado ofrecido por el contratista.	Contratista	Media	Medio	Exigir reemplazos con igual o superior perfil, sin afectar la continuidad del servicio.
12	Incumplimiento de las obligaciones laborales, parafiscales o de seguridad social del personal del contratista.	Contratista	Baja	Alto	Verificación periódica de aportes, requisito para pagos y aplicación de las sanciones contractuales correspondientes.
13	Modificaciones normativas en materia de ciberseguridad, protección de datos o seguridad digital durante la ejecución del contrato.	Compartido	Baja	Medio	Ajustar procedimientos y obligaciones conforme a la normativa vigente mediante acuerdos entre las partes.
14	Suspensión o indisponibilidad de servicios institucionales por causas atribuibles a la entidad (mantenimiento de infraestructura, cortes eléctricos, cambios internos, etc.).	Contratante	Baja	Medio	Coordinar las intervenciones con el contratista y reprogramar actividades cuando sea necesario.

15	Incumplimiento de los niveles mínimos de disponibilidad y operación de la solución de ciberseguridad.	Contratista	Media	Alto	Establecer indicadores de disponibilidad, monitoreo permanente, reportes periódicos y aplicación de descuentos o sanciones por incumplimiento.

13. GARANTÍAS

El contratista otorgará a favor de SOMOS RIONEGRO S.A.S garantía única que avalará el cumplimiento de las obligaciones derivadas del contrato, mediante la cual se garantizarán los riesgos, por los valores y vigencias, que se señalan en el contrato, y se obliga a constituirlas dentro de los cinco (5) días hábiles siguientes a la fecha de suscripción del contrato; de no hacerlo en este término, sin causa justificada, se hará acreedor a una multa equivalente al medio por ciento (0.5 %) del valor del contrato por cada día de mora.

La garantía se mantendrá vigente durante la vigencia y liquidación del contrato y se ajustará a los límites, existencia y extensión del riesgo amparado. La garantía se entenderá vigente hasta la liquidación del contrato garantizado y la prolongación de sus efectos y, tratándose de pólizas, no expirará por falta de pago de la prima o por revocatoria unilateral.

La garantía consistirá en una póliza expedida por una compañía de seguros legalmente autorizada para funcionar en Colombia, constituida a partir de la fecha de suscripción del contrato y que contenga los siguientes amparos.

GARANTÍA	MONTO	VIGENCIA
Cumplimiento	10% del valor total del contrato	Igual al plazo del mismo y por doce (12) meses más
Calidad del servicio	10% del valor total del contrato	Igual al plazo contractual.

14. SUPERVISIÓN

Con el fin de proteger la moralidad, prevenir actos de corrupción y tutelar la transparencia de la actividad contractual, la supervisión de este contrato estará a cargo del **INGENIERO LIDER DE SISTEMAS,** quien deberá controlar su correcta ejecución y cumplimiento.

SEBASTIAN VERA MUÑOZ
INGENIERO LIDER DE SISTEMAS

Elaboró: Sebastián Vera / Líder de Sistemas
Marcela Orjuela / Ingeniera de Sistemas
Revisó: Alejandra Vásquez / Abogada
Diego Alejandro Gallego Tobón / Secretario General / Componente Jurídico
Aprobó: Julián Castro / Subgerente Técnico (E) / Componente Técnico
Wilfredy Castaño Castaño / Subgerente Administrativo y Financiero / Componente Financiero