1. DESCRIPCIÓN SUSCINTA DE LA NECESIDAD QUE LA CVS PRETENDE SATISFACER CON LA CONTRATACIÓN.

Necesidad: La Corporación Autónoma Regional de los Valles del Sinú y del San Jorge (CVS), ente corporativo de carácter público creado mediante la Ley 13 de 1973 y regulado por la Ley 99 de 1993, tiene a su cargo la administración, protección y aprovechamiento sostenible de los recursos naturales renovables y del medio ambiente dentro de su jurisdicción. Para el cumplimiento de sus funciones misionales y administrativas, la entidad depende de una infraestructura tecnológica que soporta los procesos estratégicos, misionales, de apoyo y de gestión institucional, así como el almacenamiento, procesamiento y transmisión de información de carácter técnico, administrativo, financiero, contractual y ambiental.

En el desarrollo de sus actividades, la Corporación ha implementado durante los últimos años un esquema integral de seguridad informática basado en tecnologías Sophos, el cual comprende soluciones de protección para estaciones de trabajo, servidores, correo electrónico y seguridad perimetral. Estas herramientas han permitido mitigar riesgos asociados a amenazas cibernéticas, software malicioso, ransomware, ataques de ingeniería social, phishing, explotación de vulnerabilidades, accesos no autorizados y demás eventos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información institucional.

Actualmente, la CVS cuenta con licenciamiento de las soluciones **Sophos Endpoint Central XDR**, **Sophos Intercept X Advanced for Server con EDR**, **Sophos Central Email Advanced** y tecnologías de seguridad perimetral Sophos, las cuales se encuentran próximas a vencer o requieren actualización tecnológica para mantener los niveles adecuados de protección frente al panorama actual de ciberamenazas. La no renovación de estos servicios generaría una disminución significativa en la capacidad de detección, análisis y respuesta ante incidentes de seguridad informática, aumentando la exposición de la entidad a riesgos operativos, tecnológicos y de pérdida de información.

Adicionalmente, la Corporación dispone de un dispositivo de seguridad perimetral **Sophos XG135W**, equipo que, debido a su antigüedad tecnológica y a la finalización de su ciclo de soporte por parte del fabricante, no satisface las exigencias actuales de rendimiento, capacidad de procesamiento, inspección avanzada del tráfico y protección frente a amenazas sofisticadas. Esta situación hace necesaria la modernización de la infraestructura de seguridad perimetral mediante la adquisición de un equipo de nueva generación que garantice altos estándares de disponibilidad, rendimiento, escalabilidad y protección integral.

Desde el punto de vista técnico, la solución requerida debe permitir la implementación de un modelo de **seguridad sincronizada (Synchronized Security)**, característica exclusiva del ecosistema Sophos, mediante la cual los componentes de protección de usuarios, servidores, correo electrónico y firewall intercambian información de seguridad en tiempo real, permitiendo identificar, aislar y responder automáticamente ante amenazas detectadas dentro de la red corporativa. Esta capacidad reduce

significativamente los tiempos de respuesta frente a incidentes, mejora la visibilidad de los eventos de seguridad y fortalece la postura institucional de ciberseguridad.

Para garantizar la continuidad operativa y la protección integral de los activos tecnológicos de la entidad, se requiere la adquisición de:

• Ciento treinta y tres (133) licencias **Sophos XDR User**.
• Seis (6) licencias **Sophos XDR Server**.
• Cien (100) licencias **Sophos Central Email Advanced**.
• Un (1) equipo **Sophos Firewall XGS 138**.
• Una (1) licencia **Sophos Xstream Protection** para el firewall adquirido.

Las licencias **Sophos XDR User** proporcionan capacidades avanzadas de protección, detección y respuesta extendida frente a amenazas, incorporando mecanismos de inteligencia artificial, análisis de comportamiento, detección de ransomware, protección contra exploits y capacidades de investigación y respuesta ante incidentes. Por su parte, las licencias **Sophos XDR Server** permiten extender estas capacidades a los servidores corporativos, protegiendo los servicios críticos y la información institucional alojada en ellos.

Igualmente, la solución **Sophos Central Email Advanced** fortalece la seguridad del correo electrónico institucional mediante mecanismos de protección contra phishing, malware, ransomware, suplantación de identidad, archivos maliciosos y enlaces peligrosos, mitigando uno de los principales vectores de ataque utilizados actualmente por los ciberdelincuentes para comprometer infraestructuras tecnológicas.

De igual forma, la adquisición del **Sophos Firewall XGS 138** con licencia **Xstream Protection** permitirá incorporar funcionalidades avanzadas de firewall de nueva generación (NGFW), incluyendo inspección profunda de paquetes, sistema de prevención de intrusiones (IPS), protección web, control de aplicaciones, análisis de tráfico cifrado TLS/SSL, inteligencia contra amenazas, sandboxing en la nube y control granular del tráfico de red, garantizando una protección perimetral acorde con las necesidades actuales de la Corporación.

La integración de estos componentes dentro de una única plataforma de administración centralizada facilitará la gestión de la seguridad informática, optimizará los recursos tecnológicos y permitirá una administración más eficiente de los eventos, alertas y políticas de seguridad, generando mayor visibilidad y control sobre toda la infraestructura tecnológica institucional.

En consecuencia, resulta necesario y conveniente para la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge (CVS) contratar el suministro de la solución integral de seguridad informática descrita, con el fin de garantizar la continuidad de los mecanismos de protección actualmente implementados, fortalecer la capacidad de prevención, detección y respuesta frente a amenazas cibernéticas, proteger la infraestructura tecnológica y salvaguardar la información institucional como uno de los activos estratégicos más importantes para el cumplimiento de los objetivos misionales

y el adecuado desarrollo de la gestión pública.

Competencia: De conformidad con el artículo 30 de la Ley 99 de 1993, las Corporaciones Autónomas Regionales tienen por objeto la ejecución de las políticas, planes, programas y proyectos relacionados con el medio ambiente y los recursos naturales renovables, así como la administración, manejo y protección de dichos recursos dentro de su jurisdicción, garantizando la aplicación de las disposiciones legales vigentes y las directrices impartidas por el Ministerio de Ambiente y Desarrollo Sostenible.

Para el adecuado cumplimiento de su misión institucional, la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge (CVS) requiere disponer de una infraestructura tecnológica segura, confiable y disponible, que soporte los procesos misionales, estratégicos, administrativos y financieros, así como la gestión y conservación de la información institucional. En tal sentido, la implementación y mantenimiento de mecanismos de seguridad informática constituye una actividad transversal e indispensable para garantizar la continuidad de los servicios tecnológicos, la protección de los activos de información y la mitigación de riesgos asociados a amenazas cibernéticas.

De acuerdo con el Manual Específico de Funciones y Competencias Laborales de la Corporación, corresponde a la Jefatura de la Oficina Administrativa y Financiera, entre otras funciones:

1. Fijar las políticas, normas y adoptar los planes y procedimientos para la administración de los recursos económicos, financieros, físicos y tecnológicos de la Corporación.
2. Orientar la aplicación del Sistema de Desarrollo Administrativo relacionado con las políticas, estrategias, metodologías, técnicas y mecanismos de carácter administrativo y organizacional para la gestión y manejo de los recursos humanos, técnicos, materiales, físicos y financieros de la entidad.
3. Dirigir, coordinar y controlar la ejecución de los programas y actividades relacionadas con los asuntos de carácter administrativo, logístico, operativo y tecnológico de conformidad con las disposiciones vigentes.

En desarrollo de las funciones anteriormente descritas, corresponde a la Oficina Administrativa y Financiera adelantar las acciones necesarias para garantizar la adecuada operación, administración, protección y actualización de la infraestructura tecnológica institucional, incluyendo la adquisición y renovación de soluciones de ciberseguridad que permitan proteger los equipos de usuario final, servidores, sistemas de correo electrónico y dispositivos de seguridad perimetral que soportan el funcionamiento de la Corporación.

Así mismo, la Ley 80 de 1993, en sus artículos 3, 13, 32 y 40, establece que las entidades estatales podrán celebrar los contratos necesarios para el cumplimiento de los fines estatales y la continua y eficiente prestación de los servicios a su cargo, en ejercicio del principio de autonomía de la voluntad y dentro del marco de la función administrativa. De igual manera, la Ley 1150 de 2007 y el Decreto 1082 de 2015 facultan a las entidades públicas para adelantar los procesos de selección requeridos para satisfacer sus necesidades y garantizar el cumplimiento de sus objetivos institucionales.

En consecuencia, la Oficina Administrativa y Financiera de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge (CVS) es la dependencia competente para promover y gestionar el presente proceso contractual, cuyo objeto consiste en el suministro de una solución integral de seguridad informática compuesta por licencias Sophos XDR para usuarios y servidores, licencias Sophos Central Email Advanced y la adquisición de un firewall Sophos XGS 138 con licenciamiento Xstream Protection, con el propósito de fortalecer la ciberseguridad institucional, garantizar la continuidad operativa de los servicios tecnológicos y proteger la información corporativa frente a amenazas informáticas internas y externas.

Pertinencia: La adquisición de licencias de software de protección, del firewall perimetral y correos electrónicos se encuentra amparada en el plan de compras y en el Plan Anual de Adquisición de la entidad, los cuales son necesarios para el funcionamiento de sus dependencias.

2. DESCRIPCIÓN DEL OBJETO IDENTIFICADO CON EL CUARTO NIVEL DEL CLASIFICADOR DE BIENES Y SERVICIOS.

ADQUIRIR CIENTO TREINTA Y TRES (133) LICENCIAS SOPHOS XDR USER, SEIS (6) LICENCIAS SOPHOS XDR SERVER, CIEN (100) LICENCIAS SOPHOS CENTRAL EMAIL ADVANCED, Y LA ADQUISICIÓN DE UN (1) FIREWALL SOPHOS XGS 138 CON UNA (1) LICENCIA XSTREAM PROTECTION, PARA FORTALECER LA SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CORPORACIÓN AUTÓNOMA REGIONAL DE LOS VALLES DEL SINÚ Y DEL SAN JORGE – CVS.

Código UNSPSC:

- **43222501** – Dispositivos de seguridad de red.
- **43233205** – Software de seguridad de red.
- **43233506** – Software de protección antivirus.
- **43232901** – Software para protección de correo electrónico.
- **81112208** – Servicios de soporte y mantenimiento de software

3. CONDICIONES TECNICAS EXIGIDAS

3.1. Especificaciones técnicas

El contratista deberá suministrar licencias y equipo nuevo, originales, no reacondicionados, debidamente licenciados por el fabricante Sophos, garantizando compatibilidad, soporte y administración centralizada desde la consola en la nube Sophos Central, La adquisición de las licencias debe ser **por 12 meses a partir del 01 de diciembre de 2026, fecha en la que expiran las actuales licencias** y se llevara a cabo teniendo en cuenta los siguientes parámetros y especificaciones.

NO.	UNIDAD DE MEDIDA	DETALLE	CANTIDAD
1	PAQUETE	Licencia de protección Sophos XDR - User, por 12 meses	133
2	PAQUETE	Licencias sophos Central Email Advance, por 12 meses	100
3	PAQUETE	Licencia de protección Sophos XDR - Server, por 12 meses	6
4	EQUIPO	Firewall XGS 138 Appliance	1
5	PAQUETE	Licencia del Firewall Sophos XGS 138 Xstream Protection - 12 meses	1

ITEM 1
Sophos XDR User
Cantidad: 133 Licencias

Las licencias ofertadas deberán cumplir como mínimo con las siguientes características:

- Licenciamiento Sophos XDR User para estaciones de trabajo.
- Administración centralizada desde consola Sophos Central en la nube.
- Protección antimalware basada en inteligencia artificial y deep learning.
- Protección contra ransomware con capacidades de detección y recuperación.
- Protección contra exploits y ataques de día cero (Zero-Day).
- Detección y respuesta extendida (XDR).
- Capacidad para correlacionar eventos provenientes de endpoint, firewall, correo electrónico y otros productos integrados.
- Acceso a Sophos Data Lake para almacenamiento y análisis de telemetría de seguridad.
- Funcionalidad Live Discover para búsqueda e investigación avanzada de amenazas.
- Funcionalidad Live Response para respuesta remota ante incidentes de seguridad.
- Análisis mediante Threat Graph para visualización y reconstrucción de ataques.
- Capacidades de threat hunting e investigación forense.
- Detección de comportamientos anómalos y actividades sospechosas.
- Integración con Security Heartbeat para intercambio de información de seguridad con firewall Sophos.
- Compatibilidad con sistemas operativos Windows y macOS soportados por el fabricante.
- Actualización automática de firmas, motores de detección y políticas de seguridad.

ITEM 2
Sophos Central Email Advanced
Cantidad: 100 Licencias

Las licencias ofertadas deberán cumplir como mínimo con las siguientes características:

- Protección avanzada de correo electrónico administrada desde Sophos Central.
- Protección contra spam, malware y virus.
- Protección avanzada contra phishing y Business Email Compromise (BEC).
- Protección contra suplantación de identidad mediante análisis de dominios, remitentes y marcas.
- Validación SPF, DKIM y DMARC.
- Escaneo de enlaces maliciosos mediante tecnología Time-of-Click URL Protection.
- Reescritura y verificación dinámica de URL sospechosas.
- Sandboxing en la nube para análisis de archivos adjuntos sospechosos.
- Detección de archivos maliciosos mediante inteligencia artificial.
- Protección frente a ransomware distribuido por correo electrónico.
- Control de contenido y capacidades DLP (Data Loss Prevention).
- Escaneo de correos entrantes y salientes.
- Cuarentena centralizada para administradores.
- Integración con Microsoft 365.
- Integración con Sophos XDR y Sophos MDR para intercambio de eventos de seguridad.
- Protección de cuentas de usuario frente a intentos de compromiso.
- Reportes e informes de seguridad desde Sophos Central.

ITEM 3
Sophos XDR Server
Cantidad: 6 Licencias

Las licencias ofertadas deberán cumplir como mínimo con las siguientes características:

- Licenciamiento Sophos XDR para servidores físicos, virtuales o en la nube.
- Protección para sistemas operativos Windows Server y Linux soportados por el fabricante.
- Administración centralizada desde Sophos Central.
- Tecnología anti-malware basada en inteligencia artificial.
- Protección contra ransomware.

- Protección contra exploits y vulnerabilidades avanzadas.
- Detección y respuesta extendida (XDR).
- Capacidades de análisis de amenazas en tiempo real.
- Herramientas Live Discover y Live Response para investigación y mitigación remota.
- Integración con Sophos Firewall mediante Security Heartbeat.
- Visibilidad de eventos y telemetría en Sophos Data Lake.
- Protección para cargas de trabajo locales, virtualizadas y en ambientes cloud.
- Correlación de eventos de seguridad provenientes de endpoints, servidores, firewall y correo electrónico.
- Gestión unificada desde Sophos Central.
- Actualizaciones automáticas de protección y motores de análisis.

ITEM 4
Equipo Firewall Sophos XGS 138
Cantidad: 1 Equipo

El equipo ofertado deberá ser nuevo, original de fabricante Sophos y cumplir como mínimo con las siguientes características:

- Características de Hardware
- Appliance Sophos XGS 138 o superior.
- Arquitectura Xstream.
- Procesador dedicado para aceleración de tráfico.
- Almacenamiento interno para registros y cuarentena.
- Mínimo cuatro (4) puertos Gigabit Ethernet.
- Mínimo dos (2) puertos 2.5 Gigabit Ethernet.
- Mínimo dos (2) interfaces SFP+ de 10 Gigabit.
- Puerto USB para administración.
- Soporte para conectividad redundante y expansión conforme a especificaciones del fabricante.
- Equipo nuevo, sin uso y con garantía del fabricante.
- Desempeño mínimo
- Firewall Throughput: 19 Gbps o superior.
- IPS Throughput: 5.8 Gbps o superior.
- NGFW Throughput: 5.1 Gbps o superior.
- Threat Protection Throughput: 4.7 Gbps o superior.
- VPN IPsec Throughput: 6.6 Gbps o superior.
- Soporte para mínimo 6.500.000 conexiones concurrentes.

ITEM 5

Licencia Xstream Protection para Firewall SOPHOS XGS138
Cantidad: 1 Licencia

La licencia deberá habilitar como mínimo:

- Sistema de Prevención de Intrusiones (IPS).
- Protección avanzada contra amenazas (ATP).
- Inspección profunda de paquetes (DPI).
- Xstream TLS Inspection para inspección de tráfico cifrado SSL/TLS.
- Antivirus de red.
- Filtrado web avanzado.
- Control de aplicaciones.
- Detección y bloqueo de malware.
- Protección frente a ransomware.
- Protección contra ataques DoS y DDoS.
- Inteligencia de amenazas proveniente de SophosLabs.
- SD-WAN integrado.
- VPN SSL e IPsec.
- Sincronización con Sophos Endpoint, Sophos XDR y Sophos Server Protection.
- Security Heartbeat.
- Gestión centralizada desde Sophos Central.
- Respuesta automática frente a equipos comprometidos mediante Synchronized Security.

Requisitos Generales, Servicios Conexos y Acuerdos de Nivel de Servicio (ANS)

Con el fin de garantizar la continuidad operativa, la correcta implementación de la solución integral de ciberseguridad, la protección permanente de los activos de información institucionales y la adecuada transferencia de conocimiento al personal de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge (CVS), el contratista deberá cumplir, como mínimo, con las siguientes condiciones:

1. Licenciamiento y Garantía

- Suministrar licencias nuevas, originales, vigentes y registradas oficialmente ante el fabricante SOPHOS.
- Garantizar que todos los productos suministrados correspondan a versiones comerciales activas y soportadas por el fabricante.
- Entregar certificados de licenciamiento y documentación que acredite la legalidad y vigencia de las suscripciones.

- Garantizar la cobertura de soporte y actualizaciones del fabricante durante toda la vigencia de las licencias suministradas.
- Garantizar que la solución conserve la interoperabilidad y administración centralizada mediante la plataforma Sophos Central.

2. Suministro, Configuración e Implementación del Firewall

- El contratista deberá entregar el equipo Sophos Firewall XGS 138 completamente configurado y parametrizado para su puesta en funcionamiento.
- La Corporación suministrará al contratista un archivo de respaldo (backup) de la configuración del firewall actualmente en operación, con el fin de facilitar la migración y continuidad de las políticas de seguridad existentes.
- El contratista deberá realizar el análisis técnico del respaldo suministrado, efectuar la migración de configuraciones compatibles y realizar los ajustes necesarios para optimizar el funcionamiento del nuevo equipo.
- La configuración deberá incluir, como mínimo:
    - Interfaces de red.
    - Segmentación de redes y VLAN.
    - Políticas de acceso.
    - Reglas de firewall.
    - NAT.
    - Publicación de servicios.
    - VPN existentes.
    - IPS.
    - Filtrado web.
    - Control de aplicaciones.
    - Inspección SSL/TLS.
    - Seguridad sincronizada con Sophos Central.
    - Configuración de alertamientos, bitácoras y monitoreo.
- El equipo deberá entregarse listo para instalación y entrada en operación con mínima afectación a la continuidad de los servicios tecnológicos institucionales.
- El contratista deberá brindar acompañamiento remoto y/o presencial durante el proceso de instalación, pruebas y puesta en producción.

3. Soporte Técnico Especializado

- El contratista deberá prestar soporte técnico especializado sobre la totalidad de la solución suministrada durante un período mínimo de doce (12) meses contados a partir de la activación de las licencias y puesta en funcionamiento del firewall.
- El soporte deberá cubrir:
    - Sophos XDR User.
    - Sophos XDR Server.

  - Sophos Central Email Advanced.
  - Sophos Firewall XGS 138.
  - Sophos Xstream Protection.
  - Plataforma Sophos Central.
- El soporte deberá ser proporcionado por personal certificado o acreditado en soluciones Sophos.
- Se deberá disponer de canales de atención mediante correo electrónico, mesa de ayuda, soporte remoto y línea telefónica.

4. Monitoreo y Acompañamiento Proactivo

El contratista deberá efectuar monitoreo especializado de la plataforma de seguridad suministrada durante toda la vigencia contractual, incluyendo:

- Revisión permanente de eventos de seguridad generados por las plataformas Sophos.
- Monitoreo de alertas críticas de malware, ransomware, phishing, explotación de vulnerabilidades, comportamientos anómalos y amenazas avanzadas.
- Verificación periódica del estado de salud de los agentes de protección instalados en equipos y servidores.
- Seguimiento al funcionamiento del firewall, servicios VPN, IPS, filtrado web y mecanismos de protección activa.
- Revisión de indicadores de seguridad y eventos relevantes reportados por Sophos Central.
- Emisión de recomendaciones para optimizar los niveles de protección de la infraestructura tecnológica institucional.

4. Atención y Respuesta ante Incidentes de Seguridad

El contratista deberá brindar acompañamiento especializado para la atención de incidentes de seguridad informática que se presenten durante la vigencia contractual.

Se entenderán como incidentes, entre otros:

- Infecciones por malware.
- Ataques de ransomware.
- Ataques de phishing.
- Compromiso de cuentas de usuario.
- Explotación de vulnerabilidades.
- Intrusiones no autorizadas.
- Eventos de seguridad detectados por Sophos XDR.
- Ataques contra servicios publicados.
- Eventos de compromiso de servidores.

- Alertas críticas emitidas por Sophos Central.

Para estos casos el contratista deberá:

- Realizar análisis técnico inicial del incidente.
- Apoyar las actividades de contención y mitigación.
- Brindar orientación para recuperación de servicios afectados.
- Apoyar los procesos de investigación y análisis forense disponibles a través de las herramientas Sophos.
- Emitir recomendaciones que eviten la recurrencia del incidente.

Acuerdos de Nivel de Servicio (ANS)

El contratista deberá atender los requerimientos realizados por la CVS conforme a los siguientes tiempos máximos:

Prioridad	Tipo de incidente	Tiempo máximo de respuesta
Crítica	Caída del firewall, incidente de ciberseguridad activo, ransomware, indisponibilidad de servicios críticos, compromiso de servidores o correo corporativo	Máximo 2 horas
Alta	Fallos de protección, alertas críticas, problemas de conectividad asociados a la solución de seguridad	Máximo 4 horas
Media	Incidentes operativos o solicitudes de configuración	Máximo 8 horas hábiles
Baja	Consultas, asesorías o requerimientos preventivos	Máximo 24 horas hábiles

La atención inicial podrá ser remota; sin embargo, cuando la complejidad del evento lo requiera, el contratista deberá escalar el caso hasta lograr su solución definitiva.

7. Capacitación y Transferencia de Conocimiento

El contratista deberá realizar capacitación técnica dirigida al personal designado por la Corporación respecto de:

- Administración de Sophos Central.
- Gestión de Sophos XDR.

- Administración del Firewall Sophos XGS 138.
- Interpretación de eventos y alertas de seguridad.
- Buenas prácticas de ciberseguridad.
- Gestión de incidentes de seguridad informática.
- Operación de VPN y políticas de acceso.
- Consultas e investigaciones básicas mediante las funciones XDR.

Las capacitaciones deberán incluir material de apoyo digital y podrán realizarse de manera presencial o virtual según las necesidades de la Corporación.

8. Asesoría Permanente

Durante la vigencia contractual, el contratista deberá brindar asesoría técnica especializada sobre:

- Buenas prácticas de ciberseguridad.
- Fortalecimiento de la postura de seguridad institucional.
- Recomendaciones de endurecimiento (hardening) de servidores y estaciones de trabajo.
- Revisión y optimización de políticas de firewall.
- Gestión de vulnerabilidades.
- Protección de correo electrónico.
- Arquitecturas seguras de acceso remoto.
- Implementación de lineamientos de seguridad digital aplicables al sector público.

9. Informes y Seguimiento

El contratista deberá presentar informes periódicos cuando sean requeridos por la supervisión del contrato, incluyendo como mínimo:

- Estado general de la plataforma de seguridad.
- Principales amenazas detectadas.
- Incidentes atendidos.
- Actividades realizadas.
- Recomendaciones de mejora.
- Estado del licenciamiento.
- Estado operativo del firewall.
- Estadísticas de protección de endpoints, servidores y correo electrónico.

10. Garantía de Operación y Continuidad

El contratista deberá garantizar que la solución suministrada funcione como un ecosistema integrado de seguridad sincronizada, permitiendo el intercambio de información en tiempo real entre Sophos XDR, Sophos Server Protection, Sophos Email Advanced y Sophos Firewall XGS 138, con el propósito de fortalecer las capacidades institucionales de prevención, detección, investigación, contención, respuesta y recuperación frente a amenazas cibernéticas, contribuyendo a la protección de la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional y a la continuidad de las operaciones tecnológicas de la CVS.

3.2 Localización del proyecto, servicio o bien:

El domicilio principal para la ejecución de los trabajos objeto del presente contrato será en las instalaciones de La Corporación Autónoma Regional de los Valles del Sinú y del San Jorge CVS, Edificio Onomá Sede principal Carrera 6 No 61-25 - Montería – Córdoba.

3.3 Obligaciones del contratista:

Generales

1. Cumplir con el objeto del contrato con plena autonomía técnica y administrativa y bajo su propia responsabilidad, por lo tanto, no existe ni existirá ningún tipo de subordinación, ni vínculo laboral alguno entre el CONTRATISTA y la CVS.
2. Constituir y allegar a la CVS las garantías requeridas dentro de los tres (3) días hábiles siguientes a la suscripción del contrato.
3. Participar y apoyar a la CVS en todas las reuniones a las que éste lo convoque relacionadas con la ejecución del contrato.
4. Disponer de los medios necesarios para el mantenimiento, cuidado y custodia de la documentación objeto del presente contrato.
5. Atender los requerimientos, instrucciones y/o recomendaciones que durante el desarrollo del Contrato le imparta la CVS a través del supervisor de este, para una correcta ejecución y cumplimiento de sus obligaciones.
6. Entregar al supervisor del Contrato los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos cuando así se requiera.
7. Presentar la cuenta de cobro de conformidad con la forma de pago estipulada en el contrato, junto con el informe de las actividades realizadas para cada pago.
8. Guardar estricta reserva sobre toda la información y documentos que tenga acceso, maneje en desarrollo de su actividad o que llegue a conocer en desarrollo del contrato y que no tenga carácter de pública. En consecuencia, se obliga a no divulgar por ningún medio dicha información o documentos a terceros, sin la previa autorización de la CVS.
9. Asumir un buen trato para con los demás colaboradores internos y externos de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, y actuar con responsabilidad, eficiencia y transparencia.
10. Devolver a la CVS, una vez finalizado la ejecución del contrato los documentos que en desarrollo del contrato se hayan producido, e igualmente todos los archivos que se hayan generado en cumplimiento de sus obligaciones y al almacén, los bienes devolutivos que le hayan sido asignados en custodia.
11. Colaborar con la CVS en el suministro y respuesta de la información correspondiente, a los requerimientos efectuados por los organismos de control del Estado Colombiano en

relación con la ejecución, desarrollo o implementación del contrato objeto del presente documento.
12. Realizar los pagos al SISS (salud, pensión y riesgos laborales), aportando los soportes de pago correspondientes, según cada caso, y de acuerdo con la normatividad vigente.

Especificas

Además de las obligaciones legales inherentes a la naturaleza del contrato, el CONTRATISTA se obliga a:

1. Suministrar, activar, implementar y dejar en correcto funcionamiento **ciento treinta y tres (133) licencias Sophos XDR User, seis (6) licencias Sophos XDR Server, cien (100) licencias Sophos Central Email Advanced, un (1) Firewall Sophos XGS 138 y una (1) licencia Sophos Xstream Protection**, por un período de doce (12) meses, contados a partide del 01 de diciembre de 2026 fecha en la que expiran las actuales licencias.
2. Garantizar que todas las licencias suministradas sean nuevas, originales, registradas ante el fabricante y con pleno derecho de uso durante la vigencia contratada.
3. Entregar el equipo Sophos Firewall XGS 138 nuevo, debidamente configurado, parametrizado y listo para su instalación y puesta en producción.
4. Recibir, analizar y restaurar el archivo de respaldo (backup) suministrado por la Corporación correspondiente al firewall actualmente en operación, realizando las conversiones, ajustes y optimizaciones necesarias para asegurar la migración de las configuraciones al nuevo equipo.
5. Migrar y configurar las reglas de seguridad, objetos, políticas, NAT, VPN, filtros, segmentación de red, controles de acceso, servicios publicados y demás parámetros requeridos para garantizar la continuidad operativa de la plataforma tecnológica institucional.
6. Configurar la consola Sophos Central y todos los componentes de la solución de seguridad informática suministrada, garantizando su integración y administración unificada.
7. Instalar, configurar, actualizar y poner en funcionamiento los agentes de protección en las estaciones de trabajo, equipos portátiles y servidores definidos por la Corporación.
8. Configurar e integrar la solución de protección de correo electrónico Sophos Central Email Advanced con el servicio de correo institucional, habilitando las políticas de seguridad, protección contra phishing, malware, ransomware, spam y demás funcionalidades disponibles.
9. Configurar la seguridad sincronizada (Synchronized Security) entre el Firewall Sophos XGS 138, Sophos XDR User, Sophos XDR Server y Sophos Email Advanced, garantizando la interoperabilidad de toda la plataforma.
10. Configurar el Active Directory del servidor de dominio en el firewall con la finalidad de ver los equipos de la red y la conectividad de los usuarios para una correcta identificación y monitoreo.

11. Realizar pruebas funcionales y operativas de todos los componentes implementados y presentar al supervisor evidencia de su correcto funcionamiento.
12. Brindar soporte técnico especializado durante los doce (12) meses de vigencia del licenciamiento, para todos los componentes de la solución suministrada.
13. Disponer de personal técnico con experiencia y conocimientos certificados o acreditables en tecnologías Sophos para la atención de requerimientos e incidentes.
14. Prestar asistencia técnica remota y, cuando las circunstancias lo requieran, asistencia presencial para la solución de fallas o incidentes asociados a la solución contratada.
15. Atender y gestionar oportunamente las solicitudes, requerimientos e instrucciones impartidas por el supervisor del contrato relacionadas con la administración, operación, configuración y optimización de la solución implementada.
16. Realizar ajustes, modificaciones y afinamiento (tuning) de las políticas de seguridad cuando se presenten bloqueos indebidos, falsos positivos o nuevas necesidades operativas de la Corporación.
17. Revisar periódicamente las políticas de seguridad configuradas en los endpoints, servidores, sistema de correo electrónico y firewall, proponiendo e implementando mejoras orientadas al fortalecimiento de la postura de ciberseguridad institucional.
18. Crear, modificar o actualizar políticas de seguridad, filtrado, control de aplicaciones, acceso remoto, navegación web y demás configuraciones que la Corporación requiera durante la ejecución contractual.
19. Monitorear permanentemente el estado de funcionamiento de la consola Sophos Central, las licencias, los agentes de protección, los servidores protegidos, la seguridad de correo electrónico y el firewall perimetral.
20. Realizar seguimiento continuo a los eventos, alertas e incidentes generados por las plataformas de seguridad implementadas.
21. Informar de manera inmediata al supervisor del contrato sobre alertas críticas, incidentes de seguridad, intentos de intrusión, ataques de ransomware, campañas de phishing, infecciones por malware o cualquier evento que represente riesgo para la infraestructura tecnológica de la Corporación.
22. Brindar apoyo técnico especializado para la atención, análisis, contención, mitigación y recuperación frente a incidentes de seguridad informática que se presenten durante la vigencia contractual.
23. Apoyar las actividades de investigación y análisis de eventos de seguridad mediante las herramientas Sophos XDR y demás funcionalidades disponibles en la solución implementada.
24. Configurar y verificar el correcto funcionamiento de los mecanismos de generación y envío automático de copias de respaldo (backup) del firewall, así como atender cualquier novedad relacionada con su ejecución o recepción.
25. Verificar periódicamente la correcta ejecución de las tareas de respaldo y recuperación de configuraciones relacionadas con el firewall y la consola de administración.
26. Brindar asesoría técnica especializada a la Corporación en materia de ciberseguridad, protección de infraestructura tecnológica, gestión de vulnerabilidades, protección del correo electrónico y fortalecimiento de controles de seguridad.

27. Suministrar recomendaciones técnicas para mejorar continuamente los niveles de protección, disponibilidad e integridad de la información institucional.
28. Realizar las capacitaciones que requiera la Corporación sobre administración, operación, monitoreo, análisis de alertas, gestión de incidentes y mejores prácticas de ciberseguridad relacionadas con la solución contratada.
29. Efectuar jornadas de transferencia de conocimiento al personal designado por la Corporación durante la ejecución contractual, cuando estas sean solicitadas por el supervisor.
30. Presentar informes periódicos de gestión, incluyendo como mínimo:

- Estado de las licencias.
- Estado del firewall.
- Estado de los endpoints y servidores protegidos.
- Eventos de seguridad detectados.
- Incidentes atendidos.
- Acciones correctivas implementadas.
- Recomendaciones técnicas.
- Indicadores de funcionamiento de la solución.

31. Remitir al supervisor del contrato un informe semanal de monitoreo, en el que se relacionen las alertas relevantes, actividades realizadas, incidentes gestionados y recomendaciones de mejora.
32. Garantizar la confidencialidad, integridad y reserva de toda la información a la que tenga acceso con ocasión de la ejecución del contrato.
33. Garantizar la continuidad operativa de la solución integral de seguridad informática durante toda la vigencia contractual, procurando minimizar riesgos de indisponibilidad, pérdida de información o afectación de los servicios tecnológicos institucionales.
34. Mantener comunicación permanente con el supervisor del contrato y responder oportunamente los requerimientos técnicos, administrativos y operativos relacionados con el objeto contractual.
35. Cumplir con los acuerdos de nivel de servicio (ANS) definidos por la Corporación para la atención de incidentes críticos, altos, medios y bajos relacionados con la solución contratada.
36. Entregar al finalizar el contrato toda la documentación técnica actualizada de la solución implementada, incluyendo configuraciones relevantes, inventario de licencias, procedimientos de administración y recomendaciones para la continuidad operativa de la plataforma de seguridad

En caso de que apliquen:

- **Para el Eje de Calidad**

1. Asegurar que el personal requerido para la ejecución del contrato/convenio cuente con la educación, formación y experiencia para garantizar el óptimo desarrollo del objeto contractual.

2. Realizar un (1) ejercicio muestral para evaluar la percepción de satisfacción de los beneficiarios con respecto a la prestación del servicio y entregar a la CVS los resultados obtenidos.
3. Asegurar que los equipos de medición utilizados para el cumplimiento del objeto contractual o convenio cuentan con certificaciones iniciales de calibración y sus verificaciones intermedias y entregar copia de estas certificaciones a la CVS.

- **Para el Eje de Seguridad y Salud en el Trabajo.**

1. Designar por escrito un representante de seguridad y salud en el trabajo responsable del tema durante toda la vigencia del contrato/convenio, para que garantice el cumplimiento de obligaciones establecidas en el marco de su ejecución y la normatividad vigente.
2. Presentar a la CVS la matriz de identificación de peligros, valoración de riesgos y determinación de controles, documentados, en el marco de la Seguridad y Salud en el Trabajo durante la ejecución del contrato o convenio.
3. Suministrar a los colaboradores vinculados para la ejecución del contrato o convenio los elementos de protección personal requeridos para la realización de sus actividades y garantizar el uso correcto de éstos.
4. Garantizar que todo el personal vinculado para la ejecución del contrato o convenio se encuentre afiliado al Sistema de Seguridad Social y que disponga del concepto médico ocupacional favorable.

- **Para el Eje Ambiental.**

1. Identificar los aspectos e impactos ambientales de cada una de las actividades a ejecutar y establecer las acciones tendientes a reducir, mitigar y corregir los impactos ambientales significativos.
2. Adoptar las medidas necesarias para el ahorro y uso eficiente de agua, energía, papel, y para el manejo adecuado y la disposición final de los residuos especiales y/o peligrosos que se generen durante la ejecución del contrato o convenio.
3. Adoptar las medidas necesarias para el almacenamiento y manejo adecuado de los productos químicos utilizados durante la ejecución del contrato o convenio; de acuerdo con la normatividad vigente.
4. Formular e implementar plan de saneamiento que incluya como mínimo los programas de limpieza y desinfección, manejo de residuos, control de plagas y abastecimiento o suministro de agua potable, de acuerdo con la normatividad vigente.

- **Para el Eje de Seguridad de la Información.**

1. Garantizar los procesos adecuados para la protección y confidencialidad de la información que se maneje dentro de la ejecución del contrato o convenio, conforme a las políticas internas de la CVS.
2. Suscribir un documento de compromiso de confidencialidad el cual deberá ser entregado al supervisor una vez se suscriba el contrato o convenio.
3. Informar al supervisor, en el momento que ocurran incidentes de seguridad o se materialice un riesgo de seguridad de la información que afecten la disponibilidad, integridad y/o confidencialidad de la información de la CVS en el marco de la ejecución del contrato o convenio.

3.4 Obligaciones de la CVS:

1. Designar un supervisor para ejercer el control y vigilancia de la ejecución de la orden.
2. Prestar el apoyo logístico al contratista para el logro de los objetivos trazados.
3. Realizar el pago oportuno.
4. Garantizar autonomía dentro de los términos contractuales.
5. Administrar correctamente el software instalado para la realización de las tareas de protección de la plataforma informática de la Corporación

4. VALOR ESTIMADO DEL CONTRATO Y SU JUSTIFICACIÓN

Para la adquisición de CIENTO TREINTA Y TRES (133) LICENCIAS SOPHOS XDR USER, SEIS (6) LICENCIAS SOPHOS XDR SERVER, CIEN (100) LICENCIAS SOPHOS CENTRAL EMAIL ADVANCED, Y LA ADQUISICIÓN DE UN (1) FIREWALL SOPHOS XGS 138 CON UNA (1) LICENCIA XSTREAM PROTECTION, se realizó la consulta de precios de mercado, con dos (2) cotizaciones, realizando un cuadro comparativo de las mismas obteniendo el promedio del costo de la licencia, para hacer parte del presente estudio previo.

No.	unidad de medida	DETALLE	CANTIDAD	MAESTRE CORPORACIÓN		CREAR SISTEMAS		PROMEDIO VALOR UNITARIO
				VALOR UNITARIO	VALOR TOTAL	VALOR UNITARIO	VALOR TOTAL	

1	PAQUETE	Licencia de protección Sophos XDR - User, por 12 meses	133	68,168	9,066,344	69,500	9,243,500	9,154,922
2	PAQUETE	licencias sophos Central Email Advance, por 12 meses	100	30,742	3,074,200	29,200	2,920,000	2,997,100
3	PAQUETE	Licencia de protección Sophos XDR - Server, por 12 meses	6	102,252	613,512	103,500	621,000	617,256
SUB TOTAL								12,769,278
IVA								N.A
TOTAL								12,769,278

No.	unidad de medida	DETALLE	CANTIDAD	MAESTRE CORPORACIÓN		CREAR SISTEMAS		PROMEDIO VALOR UNITARIO
				VALOR UNITARIO	VALOR TOTAL	VALOR UNITARIO	VALOR TOTAL	
4	EQUIPO	Firewall XGS 138 Appliance	1	4,662,463	4,662,463	4,646,000	4,646,000	4,654,232
5	PAQUETE	Licencia del Firewall Sophos XGS 138 Xstream Protection - 12 meses	1	3,638,652	3,638,652	3,645,000	3,645,000	3,641,826
SUB TOTAL								8,296,058
IVA								1,576,251
TOTAL								9,872,308

TOTAL ESTUDIO DE MERCADO	**22,641,586**

LA CORPORACIÓN considera que el valor del objeto de la presente contratación asciende hasta la suma de **VEINTIDÓS MILLONES SEISCIENTOS CUARENTA Y UN MIL QUINIENTOS OCHENTA Y SEIS PESOS MONEDA LEGAL COLOMBIANA ($22,641,586)**

4.1 FORMA DE PAGO

El valor del contrato se cancelará con un único pago total, previa presentación de la factura o cuenta de cobro por parte del contratista, la cual debe llevar visto bueno del supervisor, acompañada de certificación en la que conste la prestación del servicio a entera satisfacción suscrita igualmente por el supervisor del contrato.

5. PLAZO DE EJECUCION DEL CONTRATO

Treinta (30) días

6. CERTIFICADO DE DISPONIBILIDAD QUE RESPALDA LA CONTRATACION

El valor del presente proceso se encuentra respaldado por el Certificado de Disponibilidad Presupuestal No. 200 expedido el día 05 del mes de agosto de 2026.

7. GARANTIAS

GARANTÍA	%	VIGENCIA
Cumplimiento	10% del valor del contrato	Durante el plazo del contrato y 6 meses más
Calidad y correcto funcionamiento del bien	10% del valor del contrato	Durante el plazo del contrato y 6 meses más
Calidad del Servicio	10% del valor del contrato	Durante el plazo del contrato y 6 meses más

8. ANEXOS

DOCUMENTO	SI	NO APLICA
Análisis del Sector	X	
Formato perfil – CDP	X	
Presupuesto		
Análisis de precios unitarios		
Estudio de mercado y cotizaciones		
Certificación del área contable de los impuestos aplicables		
Proyecto con fichas		
Estudios - Diseños – Prediseño, planos		
Permisos – licencias – autorizaciones		
Justificación Técnica cuando el plazo supere vigencia fiscal		
Observaciones		

Fecha de Elaboración: 10 de agosto de 2026

ALVARO SEGUNDO DIAZ BANDA
Profesional Universitario

VoBo. ADRIANA NEGRETE CANTILLO
Jefe Administrativa y Financiera