

ADQUIRIR, IMPLEMENTAR Y CONFIGURAR SOLUCIONES DE SEGURIDAD DE LA INFORMACIÓN Y DE CONECTIVIDAD, PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DE LA CORPORACIÓN AUTÓNOMA REGIONAL DE LA ORINOQUIA – CORPORINOQUIA, EN EL MARCO DEL PROYECTO "FORTALECIMIENTO DE LA CAPACIDAD OPERATIVA DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA GESTIÓN AMBIENTAL DE CORPORINOQUIA 2024–2027"

FICHA TECNICA DEL BIEN No 1	
<b>Nombre</b>	Licenciamiento Software para equipo de seguridad perimetral (firewall) existente en la corporación.
<b>Cantidad</b>	1
<b>Clasificación UNSPSC</b>	Software de equipos de seguridad de red y de redes privadas virtuales vpn-43233204
<b>Unidad de medida</b>	Unidad
<b>Características- Especificaciones Técnicas</b>	<p>Suministro de licenciamiento de seguridad compatible con la infraestructura tecnológica de la entidad, que permita mantener habilitadas las funcionalidades de protección avanzada de red y acceso a los servicios de actualización del fabricante, con las siguientes características:</p> <ul style="list-style-type: none"> <li>• Compatibilidad con firewall Sophos XGS 3300.</li> <li>• Licenciamiento tipo Xstream Protection, que garantice la continuidad de los servicios de seguridad del equipo.</li> <li>• Firewall base: Funcionalidades esenciales del firewall de próxima generación (NGFW), Control de aplicaciones, inspección de tráfico y reglas avanzadas de filtrado.</li> <li>• Protección de redes: Inspección profunda de paquetes (DPI) para detectar amenazas, Prevención de intrusiones (IPS) para bloquear ataques en la red.</li> <li>• Protección Web: Filtro de contenido web para controlar el acceso a sitios peligrosos o no deseados, protección antivirus, anti spam, Ransomware., análisis en tiempo real para bloquear amenazas de sitios maliciosos.</li> <li>• Control de aplicaciones</li> <li>• Inspección de tráfico cifrado SSL/TLS.</li> <li>• Protección de Día Cero: Uso de inteligencia artificial y machine learning para detectar y mitigar amenazas desconocidas, defensa contra exploits y malware avanzado.</li> <li>• Orquestación en Central: Gestión centralizada de dispositivos y políticas desde Sophos Central, automatización de respuestas ante incidentes de seguridad.</li> <li>• DNS Protection: Protección contra ataques basados en DNS, evitando conexiones con servidores maliciosos, Bloqueo de dominios de phishing y filtrado de contenido en la capa DNS.</li> <li>• La vigencia del licenciamiento debe ser por treinta y seis (36) meses contados a partir de la activación de las licencias.</li> <li>• El software debe quedar instalado y el upgrade debe quedar actualizado en el firewall.</li> <li>•</li> </ul> <p>La solución deberá garantizar la protección de los equipos mediante acceso continuo a actualizaciones y soporte técnico especializado para optimizar la configuración del firewall durante la vigencia del licenciamiento adquirido</p>

FICHA TECNICA DEL BIEN No 2	
<b>Nombre</b>	<b>Licenciamiento software para equipo de seguridad perimetral (firewall) existente en la corporación, Protección de Servidor Web</b>
<b>Cantidad</b>	1
<b>Clasificación UNSPSC .</b>	Software de equipos de seguridad de red y de redes privadas virtuales vpn-43233204
<b>Unidad de medida</b>	Unidad
<b>Características- Especificaciones Técnicas</b>	<p>Suministro de licencia software de protección, compatible con la infraestructura tecnológica de la entidad, que permita proteger aplicaciones y servicios web publicados frente a amenazas y ataques informáticos .El software debe contener las siguientes características:</p> <ul style="list-style-type: none"> <li>• Compatibilidad con firewall Sophos XGS 3300.</li> <li>• Defensa específica para servidores web contra ataques como inyección SQL y cross-site scripting (XSS).</li> <li>• Detección y mitigación de ataques de inyección SQL (SQL Injection).</li> <li>• Detección y mitigación de ataques de Cross-Site Scripting (XSS).</li> <li>• Protección frente a intentos de ejecución remota de código.</li> <li>• Protección contra explotación de vulnerabilidades de aplicaciones web.</li> <li>• Inspección y filtrado del tráfico HTTP y HTTPS.</li> <li>• Integración con herramientas de monitoreo y protección en la nube con detección de amenazas en archivos adjuntos y enlaces maliciosos.</li> <li>• La vigencia del licenciamiento debe ser por treinta y seis (36) meses contados a partir de la activación de las licencias.</li> <li>• El software debe quedar instalado y el upgrade debe quedar actualizado en el firewall.</li> </ul> <p>La solución deberá garantizar la protección de los equipos mediante acceso continuo a actualizaciones y soporte técnico especializado para optimizar la configuración del firewall durante la vigencia del licenciamiento adquirido.</p>

FICHA TECNICA DEL BIEN No 3	
<b>Nombre</b>	Licenciamiento software de seguridad perimetral firewall existente en la corporación.
<b>Cantidad</b>	3
<b>Clasificación UNSPSC</b>	Software de equipos de seguridad de red y de redes privadas virtuales vpn-43233204
<b>Unidad de medida</b>	Unidad
<b>Características-Especificaciones Técnicas</b>	<p>Licenciamiento compatible con los firewall existentes de propiedad de la entidad, con las siguientes características:</p> <ul style="list-style-type: none"> <li>• Compatibilidad con firewall Sophos XGS 116.</li> <li>• Firewall base: Funcionalidades esenciales del firewall de próxima generación (NGFW), Control de aplicaciones, inspección de tráfico y reglas avanzadas de filtrado.</li> <li>• Protección de redes: Inspección profunda de paquetes (DPI) para detectar amenazas, Prevención de intrusiones (IPS) para bloquear ataques en la red.</li> <li>• Protección Web: Filtro de contenido web para controlar el acceso a sitios peligrosos o no deseados, análisis en tiempo real para bloquear amenazas de sitios maliciosos.</li> <li>• Protección de Día Cero: Uso de inteligencia artificial y machine learning para detectar y mitigar amenazas desconocidas, defensa contra exploits y malware avanzado.</li> <li>• Orquestación en Central: Gestión centralizada de dispositivos y políticas desde Sophos Central, automatización de respuestas ante incidentes de seguridad.</li> <li>• DNS Protection: Protección contra ataques basados en DNS, evitando conexiones con servidores maliciosos, Bloqueo de dominios de phishing y filtrado de contenido en la capa DNS.</li> <li>• La vigencia del licenciamiento debe ser por treinta y seis (36) meses contados a partir de la activación de las licencias.</li> <li>• El software de upgrade debe quedar implementado en los equipos ubicado en las sub Vichada, Arauca y la unidad ambiental de Cárquez.</li> </ul> <p>La solución deberá garantizar la protección de los equipos mediante acceso continuo a actualizaciones y soporte técnico especializado para optimizar la configuración del firewall durante la vigencia del licenciamiento adquirido.</p>

<b>FICHA TECNICA DEL BIEN No 4</b>	
<b>Nombre</b>	<b>Licenciamiento de Antivirus y Protección de Endpoints</b>
<b>Cantidad</b>	150
<b>Clasificación UNSPSC</b>	Software de seguridad de transacciones y de protección contra virus- 43233205
<b>Unidad de medida</b>	Unidad
<b>Características- Especificaciones Técnicas</b>	<p>Licenciamiento para protección avanzada para 150 equipos de usuario final (endpoints), compatible e integrable con la infraestructura de seguridad informática existente de la entidad, permitiendo la administración centralizada, monitoreo de eventos de seguridad y operación coordinada con la plataforma de seguridad perimetral implementada.</p> <ul style="list-style-type: none"> <li>• Compatibilidad e integración con la infraestructura de seguridad existente de la entidad (firewall sophos).</li> <li>• Consola de administración centralizada en la nube.</li> <li>• Administración y monitoreo centralizado de los equipos protegidos.</li> <li>• Generación de reportes y alertas de seguridad.</li> <li>• Actualizaciones automáticas de firmas, motores de detección y componentes de seguridad durante la vigencia del licenciamiento.</li> <li>• Compatibilidad con sistemas operativos Windows y macOS soportados por el fabricante.</li> <li>• Detección y respuesta de puntos finales (EDR): Detecta y prioriza automáticamente las amenazas potenciales y vea rápidamente dónde centrar la atención y sepa qué máquinas pueden verse afectadas.</li> <li>• Anti-ransomware: Protección de archivos contra ransomware y análisis de comportamiento para detener ataques de ransomware y registro de arranque</li> <li>• Tecnología de aprendizaje profundo: Inteligencia artificial integrada en Intercept X que detecta malware conocido y desconocido sin depender de firmas.</li> <li>• Prevención de exploits: Bloqueo de exploits y las técnicas utilizadas para distribuir malware, robar credenciales y evadir la detección.</li> <li>• La vigencia del licenciamiento debe ser por treinta y seis (36) meses contados a partir de la activación de las licencias.</li> </ul> <p>El software debe quedar implementado en los equipos de la corporación</p>

<b>FICHA TECNICA DEL BIEN No 5</b>	
<b>Nombre</b>	<b>Licenciamiento de antivirus Protección Avanzada para Servidores</b>
<b>Cantidad</b>	17
<b>Clasificación UNSPSC</b>	Software de seguridad de transacciones y de protección contra virus - 43233205
<b>Unidad de medida</b>	Unidad
<b>Características- Especificaciones Técnicas</b>	<p>Licenciamiento para protección avanzada de servidores, compatible e integrable con la plataforma de seguridad Sophos actualmente implementada por la entidad, permitiendo la administración centralizada, correlación de eventos de seguridad y operación conjunta con la infraestructura de firewall existente:</p> <ul style="list-style-type: none"> <li>• Compatibilidad e integración con la infraestructura de seguridad existente de la entidad (firewall sophos).</li> </ul>



	<ul style="list-style-type: none"> <li>• Administración centralizada desde consola en la nube.</li> <li>• Manejo de IA con Deep Learning de Intercept X for</li> <li>• Bloqueo de ransomware: Intercept X for Server incluye funciones antiransomware avanzadas detectando y bloqueando procesos de cifrado malicioso utilizados en los ataques de ransomware.</li> <li>• Tecnología antiexploits que detiene las técnicas de explotación de las que se sirven los atacantes para infiltrarse en dispositivos, robar credenciales y distribuir malware.</li> <li>• Managed Threat Response (MTR): Servicio de búsqueda, detección y respuesta a amenazas 24/7/365 prestado por un equipo de expertos de Sophos</li> <li>• La vigencia del licenciamiento debe ser por treinta y seis (36) meses contados a partir de la activación de las licencias.</li> </ul> <p>El software debe quedar implementado en los servidores de la corporación</p>
--	---

FICHA TECNICA DEL BIEN No 6	
<b>Nombre</b>	<b>Software de copias de seguridad (Backups) de información corporativa</b>
<b>Cantidad</b>	1
<b>Clasificación UNSPSC</b>	Software de seguridad y protección - 43233200
<b>Unidad de medida</b>	Unidad
<b>Características</b>	<p>Debe contener las siguientes características:</p> <ul style="list-style-type: none"> <li>• Capacidad para replicar en la nube hasta <b>QUINCE (15)</b> servidores físicos o Virtuales, los cuales están alojados en el Datacenter de la Corporación.</li> <li>• La licencia permite realizar una copia total de la imagen (Snapshot) de los sistemas operativos Windows y/o Linux instalados en cada servidor del Datacenter, permite realizar las copias de seguridad tanto de estados del sistema, aplicaciones tales como bases de datos Microsoft SQL Sever, Exchange Server, Share Point, Active Directory, HyperV y Office 365.</li> <li>• <u>Almacenamiento local ilimitado según la capacidad de unidades de Almacenamiento NAS local con los que cuenta la corporación y 5 Terabytes de Almacenamiento remoto (en la nube), garantizando el almacenamiento de los backup diarios o mensuales.</u></li> <li>• compatibilidad, soporte de replicación y almacenamiento, para sistemas Windows Server, Linux, VMWare, Proxmox, Citrix, Virtuozzo, Nutanix, G Suite, Oracle y Android.</li> <li>• Debe permitir características de protección de pérdida de información (que tenga la posibilidad de encriptación de la información, que permita hacer copias diferenciales, incrementales y totales personalizadas y que permita personalizar cuanto tiempo se deben mantener y cada cuanto tiempo se deben hacer), a través del resguardo de copias de seguridad local y en la nube, ubicadas en Datacenters remotamente distantes.</li> <li>• Entregar 2 cuentas de administración con rol de administrador.</li> <li>• La licencia debe permitir hacer copias de seguridad con duplicación de archivos, para mejorar el ahorro de ancho de banda y almacenamiento.</li> <li>• La licencia debe ofrecer algoritmos de inteligencia artificial en tiempo real para la detección, bloqueo y prevención de aplicaciones maliciosas tipo ransomware, cryptomining.</li> <li>• Ofrecer encriptación SSL de todos los canales de transmisión local y hacia la Nube.</li> </ul>





	<ul style="list-style-type: none"> <li>• La licencia ofrece encriptación AES-256 para toda la información alojada Local y Cloud.</li> <li>• Permitir monitorización de replicación y automatización en tiempo real vía WEB.</li> <li>• La licencia debe permitir la monitorización del estado de la replicación de los datos a través de una consola Web, consultada a través de Internet.</li> <li>• Monitorización de alertas de error de replicación desde una consola Web a través de Internet, con envío automático de informes, a cuentas de correo electrónico.</li> <li>• Permitir una administración unificada y en tiempo real desde una consola Web a través de Internet.</li> <li>• En caso de falla o desastre (borrado de información, fallos en hardware o cualquier situación de pérdida de datos), la licencia debe incluir acompañamiento en sitio durante el proceso de estabilización y recuperación de los sistemas.</li> <li>• La vigencia del licenciamiento debe ser por treinta y seis (36) meses contados a partir de la activación de las licencias.</li> </ul> <p>La licencia debe incluir soporte técnico en sitio, cuando este lo amerite, en caso de ser requerido por la Corporación, durante el periodo de duración de la licencia. La licencia debe incluir actualizaciones inmediatas durante 36 meses.</p>
--	--

FICHA TECNICA DEL BIEN No 7	
<b>Nombre</b>	<b>Access Point</b>
<b>Cantidad</b>	<b>14</b>
<b>Clasificación UNSPSC</b>	Punto de acceso inalámbrico – 43222640
<b>Unidad de medida</b>	Unidad
<b>Características</b>	<ul style="list-style-type: none"> <li>• AP 5 GHz, 2.4 GHz Banda Doble para mas de 350 usuarios simultáneos.</li> <li>• Wifi 7 de largo alcance. ancho de banda de 4,3 gbps en la banda de 5 ghz y 688 mbps en la de 2,4 ghz</li> </ul> <p>Se deben entregar Instalados y Configurados en Sitio. Con el respectivo soporte técnico especializado para resolver incidencias y optimización la configuración.</p>

**Revisó: EDWIN FELIPE TORRES MEDINA**  
 Profesional Universitario Grado 10 Cod 2044

**Aprobó: LILIANA AGUDELO CIFUENTES**  
 Subdirectora de Planeación Ambiental

**Proyectó: BLADIMIR GONZALEZ HOYOS**  
 Profesional Contratada/SPA No. 120.12.13.25.793

