Estudio Previo No: 17065

ORGANISMO: Secretaría de Talento Humano y Servicios Administrativos
DEPENDENCIA: Dirección de Tecnología e Información.

1. DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER CON EL PROCESO DE CONTRATACIÓN.

1.1. Datos Generales del proceso que se pretende adelantar

MODALIDAD CONTRACTUAL: Selección Abreviada - Subasta Inversa Electrónica

OBJETO: RENOVACIÓN Y SUSCRIPCIÓN DE PLATAFORMA DE PROTECCIÓN ENDPOINTS Y HERRAMIENTAS DE SEGURIDAD DIGITAL

PRESUPUESTO (VALOR): $826.098.989 OCHOCIENTOS VEINTISÉIS MILLONES NOVENTA Y OCHO MIL NOVECIENTOS OCHENTA Y NUEVE MIL PESOS MLC Incluido el IVA del 19%

Aportan recursos las siguientes secretarías:

- DIRECCIÓN DE TECNOLOGÍA E INFORMACIÓN: $640.683.000 Seiscientos cuarenta con seiscientos ochenta y tres mil pesos MLC.
- SECRETARIA SECCIONAL DE SALUD DE ANTIOQUIA: $171.200.000 Ciento setenta y un millones doscientos mil PESOS MLC.
- FÁBRICA DE LICORES Y ALCOHOLES DE ANTIOQUIA: $90.000.000 Noventa millones de PESOS MLC.

PLAZO: Por un periodo de 12 meses contados a partir de la firma del acta de inicio.

1.2. Descripción de la Necesidad

De conformidad con lo señalado en los numerales 7 y 12 (numeral modificado por el artículo 87 de la Ley 1474 de 2011) del Artículo 25 de la Ley 80 de 1993, en concordancia con el Artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, modificado por el artículo 1 del Decreto 399 del 13 de abril de 2021, las Entidades Estatales están obligadas a llevar a cabo estudios y documentos previos para comprobar la necesidad de contratar el bien o servicio, obra o labor, dejando constancia de su adecuación al Plan de Desarrollo, al Plan de Acción de la Entidad y al Plan Anual de Adquisiciones.

Así mismo, de acuerdo al Decreto N° D2024070003913 de 2024, el cual establece en su artículo 181 como una de las funciones de la Secretaría de Talento Humano y Servicios Administrativos la de "Coordinar, articular, promover y adoptar la gestión de las tecnologías de Información y las comunicaciones como apoyo al cumplimiento de las políticas, planes, programas y proyectos de la Gobernación de Antioquia.". Para cumplir con esta función, el artículo 189 del Decreto en mención

establece que la Subsecretaría de Servicios Administrativos se encarga de "Dirigir y articular la gestión de las tecnologías de información y las comunicaciones a nivel interno, como apoyo al cumplimiento de las políticas, planes, programas y proyectos de la Gobernación de Antioquia"; a su vez, el artículo 190 establece que la Dirección de Tecnología e Información se encarga de "Gestionar los requerimientos de soporte y servicio técnico de la plataforma tecnológica de la entidad, con el fin de garantizar su correcto funcionamiento".

En ese sentido, el Plan de Desarrollo 2024-2027 "Por Antioquia Firme" contempla dentro de la Línea Estratégica No. 5 "Autonomía desde la gobernanza", componente No. 2 "Eficiencia administrativa, transparencia y acceso a la información pública", el programa No. 4 de "Administración de la infraestructura física y equipamiento de la Gobernación de Antioquia", el cual incluye acciones tendientes a la modernización y actualización de los componentes de la infraestructura física y equipamiento del Centro Administrativo Departamental (CAD) y las sedes externas de la entidad.

En el marco de dicho programa, se formuló el proyecto denominado "Fortalecimiento de los sistemas de información e infraestructura de TIC de la Gobernación de Antioquia", el cual incluye dentro de sus actividades el fortalecimiento de la Infraestructura y Gobierno de TIC, dentro de las que se contempla la modernización o actualización de los componentes tecnológicos en materia de comunicaciones para la entidad.

Actualmente, la operación de los servicios de la plataforma de Tecnologías de la Información y las Comunicaciones (TIC) soporta de manera transversal los procesos misionales, estratégicos y de apoyo de la Gobernación de Antioquia. La prestación de los servicios a la ciudadanía se apoya de forma directa en la infraestructura tecnológica institucional, la cual es utilizada por las distintas dependencias que conforman la estructura organizacional vigente para el periodo 2024–2027, entre las que se encuentran el Despacho del Gobernador, los departamentos administrativos, las secretarías sectoriales, las gerencias, las oficinas asesoras y las demás dependencias adscritas a la Entidad.
La criticidad de las actividades que se desarrollan diariamente a través de los servicios TIC, así como la necesidad de almacenar, procesar, mantener y proteger la información institucional que circula por la red de datos de la Entidad, exigen garantizar adecuados niveles de confidencialidad, integridad, disponibilidad y privacidad de la información. En este contexto, se hace indispensable la implementación y fortalecimiento continuo de medidas de seguridad informática sobre la infraestructura tecnológica, con el fin de mitigar riesgos cibernéticos, asegurar la continuidad de los servicios y proteger los activos de información de la Gobernación de Antioquia.

El equipo de Seguridad de la Información de la Dirección de Tecnologías e Información en consideración al alto crecimiento de ataques cibernéticos, se están robusteciendo, evolucionan con diferentes características y vectores de ataque, decidió por mantener el servicio de soporte técnico de Antimalware (o de protección de EndPoint).

Por otro lado, es importante mencionar que la Gobernación de Antioquia cada mes recibe en promedio 1'764.388 eventos mensuales de ataques cibernéticos de inyección de código, denegación de servicios, cross site scripting, acceso ilegal a recursos, entre otros a los portales web de la entidad, malware, troyanos, secuestro de información (Ransomware), virus, herramientas maliciosas, toolbars, spyware, entre otros a la red corporativa de equipos de cómputo, servidores corporativos; lo que nos lleva a requerir un Antimalware EndPoint, solución de Inteligencia artificial que permita identificar ataques

sofisticados, herramienta especializada para identificar brechas de seguridad informática en la plataforma tecnológica, protección de Web Application Firewall en la nube como control esencial para mitigar este tipo de ataques cibernéticos a los portales web y herramientas de auditoría del directorio activo, auditoria de los File Server y auditoria del gestor de contraseñas.

La Dirección de Tecnologías de la Información ha venido realizando inversiones estratégicas para fortalecer la Seguridad Informática de la entidad, con el propósito de mitigar riesgos cibernéticos y afectaciones reputacionales para la Gobernación de Antioquia, en un contexto de crecimiento sostenido de los ataques cibernéticos a nivel mundial.

Como resultado del monitoreo permanente, se evidencia un incremento significativo en los eventos cibernéticos identificados en la entidad: 5’050.643 eventos en 2023, 12’108.325 eventos en 2024 y 21’172.658 eventos en 2025, lo que demuestra un aumento exponencial del riesgo y la necesidad de fortalecer las capacidades de prevención, detección y respuesta.

A la fecha, se han materializado dos (2) eventos de Ransomware (secuestro de información) en equipos de cómputo de la entidad. Gracias a la reacción oportuna del equipo de Seguridad de la Información, fue posible aislar de manera inmediata los equipos afectados de la red corporativa, evitando la propagación del incidente y el impacto sobre la plataforma tecnológica de la Gobernación de Antioquia.

Las siguientes son las cifras de ataques cibernéticos en la Gobernación de Antioquia contenidos y/o mitigados desde el año 2020 al 2025 (mes de febrero).

Consolidado						
Ataque	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**
Ataques Firewall.				4.672.065	11.123.691	20.772.566
Cross Site Scripting.	1.444	2.809	188.076	11.459	491.554	19.727
DDoS.				884	9.992	420
Desconocido.		305.658	80.549	133.093	121.839	84.405
Enlace Malicioso.		3.058	23.844	25.407	2.950	997
Herramienta maliciosa.		356	498	263	23	
Ilegal Resource Access.	42.891	46.468	289.800	159.536	331.969	259.395
Malware.		874	3.452	1.868	692	1.340
Otra aplicación.		403	993	664	98	
Programa empaquetado peligroso.			-			
Programa Espia.		1.807	180	294	82	
Remote File Inclusion.	400	171	78	621	1.465	1.222
Spam.		489.114	127.377	17.615	13.640	10.729
SQL Injection.	17.165	6.139	12.181	26.107	10.199	21.573
Troyano.		16				
Virus		68.642	7.031	767	131	284
Total	**61.900**	**925.515**	**734.059**	**5.050.643**	**12.108.325**	**21.172.658**

Tabla No.1 - histórico de Reporte de Ataques en la Gobernación de Antioquia.

Gracias a la implementación de herramientas de seguridad informáticas avanzadas como el WAF (Web Application Firewall), EndPoint, Antimalware avanzado, solución de Inteligencia artificial que permita identificar ataques sofisticados y las soluciones especializadas para identificar brechas de seguridad informática en la plataforma tecnológica.

En el año 2025, la Gobernación de Antioquia definió un Plan de Cultura y Sensibilización en Seguridad de la Información, el cual incluyó diversas estrategias para fortalecer la conciencia institucional frente a los riesgos digitales. Entre las acciones desarrolladas se destacan piezas gráficas e infografías para los Miércoles de Seguridad, cápsulas de conocimiento TIC, news informativos y boletines de ciberseguridad, conmemoración del día internacional de la seguridad de la información, elaboración de material de seguridad de la información para el proceso de inducción y reinducción a funcionarios y practicantes, charlas de sensibilización dirigidas a funcionarios, contratistas y practicantes, enfocadas en temas como: Ransomware (secuestro de la información), secuestro del WhatsApp, protección en las redes sociales, Fake News (noticias falsas), contraseñas seguras, Ingeniería Social, Phishing (suplantación de identidad), demás temas relacionado con las mejores prácticas internacionales de seguridad de la información.

Cronograma del Plan de Cultura y Sensibilización de Seguridad de la Información de la Gobernación de Antioquia año 2025						
Programación	**Total Actividad**	**Puntaje x Actividad**	**Puntaje General de Cronograma**	**Actividad Ejecutada**	**Puntaje Actividades Ejecutadas**	**Puntaje General Avanzado**
1. Miércoles de Seguridad.	26	3,85%	44,07%	26	100,00%	44,07%
2. Capsulas de Seguridad.	13	7,69%	22,03%	13	100,00%	22,03%
3. News Informativos.	6	16,67%	10,17%	2	33,33%	3,39%
4. Boletines.	6	16,67%	10,17%	6	100,00%	10,17%
5. Charlas Internas.	3	33,33%	5,08%	3	100,00%	5,08%
6. Día de Seguridad	1	100,00%	1,69%	1	100,00%	1,69%
7. Curso Virtual de Seguridad.	4	25,00%	6,78%	4	100,00%	6,78%
Total, actividades programadas año 2025	**59**		**100,00%**	**55**		**93,22%**

Tabla No.2 -Cronograma del Plan de Cultura 2025 para la Gobernación de Antioquia.

Actualmente la Gobernación de Antioquia y la Fábrica de Licores y Alcoholes de Antioquia, cuenta con la funcionalidad de filtrado de contenido de navegación a Internet y el control de aplicaciones por medio del Endpoint; la cual controla el consumo de recursos a Internet por categorías (pornografía, hacking, juegos, suplantación de identidad, anonimizadores, virus, malware, troyanos, phishing, ransomware (secuestro de la información, entre otros) además, establece control sobre posibles escenarios de fraude cibernético por acceso a sitios maliciosos.

El filtrado de contenido de navegación en Internet es una herramienta esencial en las grandes, medianas y pequeñas entidades, por la multiplicidad de opciones, configuración y administración que beneficia a las organizaciones en el área de TI (Tecnología de Información), dado que:

- Previene el acceso a sitios web generadores de software malicioso.
- Previene el acceso a sitios web fraudulentos, construidos por los delincuentes cibernéticos para robar información sensible de los visitantes.
- Previene el acceso a sitios web inapropiados para un ambiente organizacional (pornografía, terrorismos, hacking, juegos, malware, adware, phishing entre otros).
- Optimiza el uso de los canales de internet, evitando que se consuma en navegación inapropiada.
- Genera estadísticas de navegación a internet de la entidad.

Considerando lo anterior, la entidad requiere que la Plataforma de Protección de Endpoint incluya las funcionalidades de control de navegación por categorías, listas blancas y listas negras, con el fin de aplicar el control de contenido web en los equipos de cómputo donde se encuentre instalada la suscripción. Para cumplir con estos requerimientos de manera más eficiente, se sugiere integrar la solución XDR (Extended Detection and Response) de EndPoint, la cual no solo proporciona protección avanzada contra amenazas en los Endpoint, sino que también permite una visibilidad y control más exhaustivo sobre las actividades de navegación, contribuyendo a una mayor seguridad, optimización del control de contenido web y disminuir el consumo del canal de internet.

Adicionalmente, la entidad requiere la instalación de soluciones de auditoría para el Directorio Activo, gestor de contraseñas y los File Servers, con el fin de garantizar el monitoreo y control continuo de las actividades en estos sistemas críticos. También se solicita la implementación de una solución de inteligencia artificial para los servidores, destinada a mitigar ataques cibernéticos sofisticados y facilitar la identificación de posibles brechas de seguridad informática en la plataforma tecnológica, mejorando así la capacidad de detección y respuesta ante amenazas avanzadas.

Desde la pandemia, las organizaciones se han visto obligadas a proteger sus equipos desde el lugar donde estén, La entidad cuenta con servidores públicos y contratistas trabajando de manera remota, lo que obliga a contar con una solución de seguridad de Endpoint respondiendo a la necesidad mencionada. Por tanto, se requiere implementar una solución de Endpoint con una consola de gestión en la nube para 3200 funcionarios que hacen uso de los equipos de cómputo de la entidad, estos equipos se encuentran en movilidad (Entrada y Salida de la red corporativa). La solución debe ofrecer protección web, reputación de descargas, control de aplicaciones, control web / bloqueo de URL basado en categorías, control de periféricos, control de aplicaciones, detección de malware con Deep Learning, análisis de comportamiento, bloqueo de aplicaciones no deseadas, sistema de prevención de intrusiones, prevención pérdida de datos, análisis de comportamiento en tiempo de ejecución, interfaz de análisis antimalware, detección de tráfico malicioso, protección contra archivos ransomware (Secuestro de la Información), protección del registro de arranque y del disco, Protección contra Man-in-the-Browser (Navegación segura).

Además de las amenazas de seguridad derivadas del software malicioso y de la navegación no controlada. Existen otros riesgos que actualmente no cuentan con medidas de mitigación (o no estarán activas) y que tienen el potencial de afectar de forma crítica los activos de información y la operación normal de la entidad. Estos riesgos incluyen:

- Aprovechamiento de vulnerabilidades no identificadas en la infraestructura de tecnologías de Información de la Gobernación de Antioquia.

- Aprovechamiento de vulnerabilidades no identificadas en las aplicaciones y sitios web de la Gobernación de Antioquia.
- Acceso, copia, alteración o eliminación indebida de archivos de la entidad, sin tener la capacidad de establecer los responsables de dichas acciones.
- Escalamiento de privilegios por parte de atacantes externos e internos en los sistemas institucionales, principalmente en el sistema de Directorio Activo.
- Acceso indebido a los recursos de la red interna institucional por una inadecuada disposición de reglas en el firewall o por un deficiente mecanismo de control de cambios.
- Afectación de los sitios web críticos de la Gobernación de Antioquia, a nivel de disponibilidad e integridad.

Como se mencionó anteriormente, la Gobernación de Antioquia cuenta con herramientas de ciberseguridad para mitigar este tipo de riesgos; una posible materialización de ellos resultaría en una grave afectación de la confidencialidad, disponibilidad, integridad y privacidad de la información de la Gobernación de Antioquia. Por tal razón, la entidad requiere renovar las herramientas de seguridad informática: (Auditoria del Directorio Activo, Auditoria de los File Servers, Gestor de Contraseñas, Análisis de Vulnerabilidades y una solución de Inteligencia artificial que permita identificar ataques sofisticados) cuya suscripción vencen el próximo mes de mayo de 2026.

❖ **Servicio de Soporte técnico para identificar brechas de seguridad en la plataforma tecnológica.** una herramienta en Seguridad informática que cumpla las siguientes características: escaneo de vulnerabilidades en sistemas operativos (Windows, Linux y Unix), diagnóstico de bases de datos (SQL Server, Oracle y MySQL), análisis de aplicaciones web, y evaluación de dispositivos de red Cisco (routers, switches, core y firewalls). Esta solución permitirá una detección proactiva de riesgos y vulnerabilidades, optimizando la protección de la infraestructura tecnológica frente a amenazas cibernéticas.

❖ **Servicio de Soporte técnico al software de auditoría y control de cambios a los ficheros alojados en los servidores de archivos de la entidad.** con el fin de monitorear, rastrear y controlar accesos, eliminaciones y /o cambios no autorizados a los archivos institucionales.

❖ **Servicio de Soporte técnico al software de auditoría al Directorio Activo.** Con un alcance de 4 controladores de Dominio, con el fin de identificar cambios no autorizados en los registros del directorio, escalamientos y modificaciones de privilegios, usuarios sospechosos y prácticas indeseadas en la gestión del Directorio Activo.

❖ **Servicio de soporte en la nube** de una solución de Inteligencia artificial que permita identificar ataques sofisticados, sino que también adapten sus defensas para favorecer la mejora constante y prevenir ciberataques futuros. Al correlacionar de forma nativa los datos de redes de alta capacidad, los Endpoint y la nube, que utilice el aprendizaje automático y el análisis para mejorar todas las fases de las operaciones de seguridad, correlacionando de manera automática con la protección perimetral del Firewall de Nueva Generación Palo Alto Networks.

❖ **Servicio de gestión de contraseñas.** Se requiere optimizar la seguridad y eficiencia mediante la implementación de una solución de gestión de contraseñas para 3500 usuarios de la Gobernación de Antioquia en el directorio activo. El objetivo es fortalecer las contraseñas de todas las cuentas de

acceso, reducir la carga sobre la mesa de ayuda (MEGANT) y generar o bloquear una lista negra de contraseñas no permitidas (prohibidas y/o vulnerables), garantizando así un control más efectivo sobre las credenciales y mejorando la protección frente a posibles ataques cibernéticos.

Incorporar el componente de XDR (Detección y Respuesta Extendida) a la solución de EndPoint fortalece de manera sustancial la capacidad institucional para prevenir, detectar y responder de forma oportuna a ciberataques avanzados, reduciendo el riesgo de indisponibilidad de servicios, pérdida de información y afectación reputacional.

La solución de ingesta de Palo Alto Networks constituye en un componente crítico para el fortalecimiento continuo del Centro de Operaciones de Seguridad (SOC) de nueva generación de la Gobernación de Antioquia**.** Actualmente, la entidad cuenta con 250 suscripciones activas de Cortex Palo Alto, las cuales han demostrado ser una herramienta robusta, confiable y eficiente para la detección temprana, análisis y respuesta ante incidentes de seguridad informática.

Además, para proteger los sitios web críticos de la entidad, la Gobernación de Antioquia debe renovar la solución Web Application Firewall (WAF). Esta renovación incluye los siguientes ítems:

- **Protección avanzada contra ataques web**: Ofrece una defensa integral contra amenazas como inyecciones SQL, Cross-Site Scripting (XSS), y otros ataques de capa 7, garantizando la seguridad de las aplicaciones web frente a exploits conocidos y desconocidos.

- **Filtrado y mitigación de bots**: La solución bloquea de manera proactiva el tráfico malicioso generado por bots automatizados, protegiendo el sitio web de ataques de denegación de servicio (DDoS) y evitando el acceso no autorizado a través de técnicas de scraping o vulnerabilidades.

- **Seguridad en tiempo real**: Proporciona análisis en tiempo real y una protección dinámica, adaptándose rápidamente a nuevas amenazas, lo que permite mitigar los riesgos sin afectar la experiencia del usuario.

- **Optimización del rendimiento**: Además de la protección, la solución WAF mejora la velocidad de carga y el rendimiento de las aplicaciones web mediante su red de distribución de contenido (CDN), reduciendo la latencia y asegurando una experiencia de usuario más eficiente.

- **Servicio de soporte en la nube de la suscripción de los portales web y ancho de banda** (50 Mbps) para los 21 sitios web pertenecientes a la Gobernación de Antioquia y la secretaria Seccional de Salud y Protección Social de Antioquia por un periodo de 12 meses.

Ítem	Página Web
1	www.antioquia.gov.co
2	www.dssa.gov.co
3	www.seduca.gov.co

4	www.antioquiadatos.gov.co
5	pedt.dssa.gov.co
6	www.antioquiatic.edu.co
7	isolucion.antioquia.gov.co
8	intranet.antioquia.gov.co
9	gina.antioquia.gov.co
10	gplus2.antioquia.gov.co
11	sislab.dssa.gov.co
12	gir.dssa.gov.co
13	aplicaciones.antioquia.gov.co
14	sismana.antioquia.gov.co
15	siinforma.dssa.gov.co
16	r3047.dssa.gov.co
17	afiliacionrs.dssa.gov.co
18	trazabilidadfactura.dssa.gov.co
19	crae.dssa.gov.co
20	interventoria.dssa.gov.co
21	Disponible para otro ambiente web critico

Tabla No.3 - Servicios de Soporte en Nube.

ANTECEDENTES DE CIBERSEGURIDAD.

1. CIBERATAQUES A NIVEL MUNDIAL.

En 2025–2026, el mundo experimenta un aumento sin precedentes en los ciberataques. Los ataques informáticos se consolidan como uno de los tres principales riesgos globales según el Foro Económico Mundial (Global Cybersecurity Outlook 2025). La creciente sofisticación impulsada por inteligencia artificial y la expansión de la superficie digital han generado una situación crítica a escala global, con organizaciones públicas y privadas en la mira de estructuras criminales transnacionales cada vez más profesionalizadas.

Según datos actualizados de Check Point Research (Q1 2025), cada organización enfrenta en promedio 1.925 intentos de intrusión semanales a nivel global, representando un incremento del 47 %

respecto al año anterior. Nueve de cada diez organizaciones sufrieron al menos un ataque cibernético durante el último año, evidenciando la magnitud del problema y la urgente necesidad de implementar medidas de protección más robustas.

Los costos asociados al cibercrimen continúan escalando de forma exponencial. Según Cybersecurity Ventures y el Global Cybercrime Report 2025, el costo global del cibercrimen alcanzó los USD $10,5 billones en 2025 y se proyecta que ascenderá a USD $11,9 billones en 2026, con una trayectoria hacia USD $19,7 billones para 2030. El FMI estima que para 2027 el cibercrimen le costará al mundo USD $23 billones, lo que representa un incremento del 175 % respecto a 2022.

Las tácticas empleadas por los ciberdelincuentes se han tornado cada vez más sofisticadas. La IA generativa permite crear correos de phishing convincentes en apenas 5 minutos (frente a las 16 horas que tomaba manualmente). El 80 % de las campañas de ransomware en 2025 incorporaron capacidades de IA para el desarrollo de malware e ingeniería social.

a. **Principales amenazas cibernéticas identificadas:**

- Ransomware: continúa liderando las amenazas con 4.701 incidentes registrados a nivel global entre enero y septiembre de 2025 (Cipher/Grupo Prosegur). Los modelos Ransomware-as-a-Service (RaaS) reducen las barreras de entrada para atacantes novatos. Para 2026 se proyecta un incremento adicional del 41 %.

- Phishing: con cerca de 3.400 millones de correos spam diarios, la IA generativa ha elevado la tasa de éxito mediante mensajes hiperpersonalizados. El phishing de QR (quishing) y el phishing polimórfico son tendencias crecientes en 2025.

- Ataques DDoS: los ataques de denegación de servicio crecen en frecuencia y escala, apoyados en botnets de dispositivos IoT.

- Ataques a la cadena de suministro: se duplicaron en 2025 respecto a 2024, con un costo medio de EUR 4,33 millones por incidente y representando el 22,5 % de todas las brechas de seguridad registradas ese año (Cipher/Grupo Prosegur).

b. **Impacto del Ciberdelito en Números (Actualizado 2025–2026):**

A continuación, se detallan los siguientes impactos.

Indicador	Cifra	Año de Referencia
Pérdidas de la industria financiera por filtración de datos.	USD $6,08 millones	2025
Costo estimado del criptodelito a nivel mundial.	USD $30.000 millones	2025
Costo estimado del Ransomware (sector manufacturero).	USD $18.000 millones*	2025 (ene–sep)
Ataques de cadena de suministro – costo global anual.	USD $53.200 millones	2025
Organizaciones que serán víctimas más de una vez.	75 %	2025–2026
Costo global proyectado del cibercrimen.	USD $11,9 billones	2026
Costo global del cibercrimen (comparativo).	USD $10,5 billones	2025
Crecimiento interanual de ataques semanales (global).	+47 %	Q1 2025
Intentos de ransomware a nivel mundial.	~289 millones	2025

Incremento proyectado del ransomware para 2026.	+41 %	Proyección 2026

Tabla No.4 - Impacto Cibernético. Fuentes: Cybersecurity Ventures / Global Cybercrime Report 2025 / Cipher-Prosegur / Check Point Research / VPNRanks / IBM Cost of a Data Breach 2025.

Nota: (*) Pérdidas potenciales en el sector manufacturero si los ataques de ransomware hubiesen tenido éxito durante los primeros tres trimestres de 2025 (VDC Research / Kaspersky).

El costo global de los ciberdelitos muestra un incremento sostenido: de USD $6 billones en 2023 a USD $10,5 billones en 2025 y una proyección de USD $11,9 billones para 2026, lo que evidencia una aceleración exponencial con impacto económico devastador a nivel mundial.

c. **Estructura del cibercrimen organizado:**
La operación de las bandas de ciberdelincuentes se caracteriza por ser transnacional y altamente especializada. En 2025 los grupos operan bajo modelos de plataforma (RaaS) con divisiones de rescates de hasta 90/10 a favor de los operadores. Grupos como SafePay, Scattered Spider y Blind Eagle demostraron en 2025 que la extorsión ya no solo busca cifrar datos, sino robar propiedad intelectual para chantajear a toda la cadena de valor. El uso de herramientas de IA ofensiva como FraudGPT y WormGPT permite automatizar campañas de ingeniería social a velocidades nunca antes vistas.

d. **Riesgos Globales clasificados por gravedad a corto y largo plazo:**
Según el Informe de Riesgos Globales 2026[1] del Foro Económico Mundial, la **inseguridad cibernética** se mantiene como un riesgo significativo tanto a corto plazo (2 años) como a largo plazo (10 años), aunque con un perfil diferente al señalado en el informe de 2025.

- A corto plazo, la **inseguridad Cibernética** ocupa un lugar destacado dentro de los diez principales riesgos, reflejando la creciente exposición de los sistemas críticos a ataques, espionaje digital y manipulación de información. La interconexión global y la dependencia de la infraestructura tecnológica continúan aumentando la vulnerabilidad de gobiernos, empresas y sectores estratégicos.

- A largo plazo, la **inseguridad Cibernética** sigue presente en la clasificación, pero se combina con otros riesgos tecnológicos como los **resultados adversos de la inteligencia artificial** y la **desinformación persistente**, lo que evidencia que la amenaza digital se proyecta más allá de los ataques inmediatos y se vincula con transformaciones estructurales en el ecosistema tecnológico.

En comparación con el informe de 2025, donde el **ciberespionaje** era señalado junto con la guerra como los principales riesgos, el informe de 2026 muestra que la **inseguridad Cibernética** se consolida como un riesgo transversal, tanto en el corto como en el largo plazo, y se reconoce como un factor crítico para la estabilidad global en un entorno de creciente digitalización.

[1] Fuente de consulta: https://es.weforum.org/stories/2026/01/riesgos-globales-2026-la-confrontacion-geoeconomica-lidera-las-amenazas-mundiales-en-la-era-de-la-competencia/

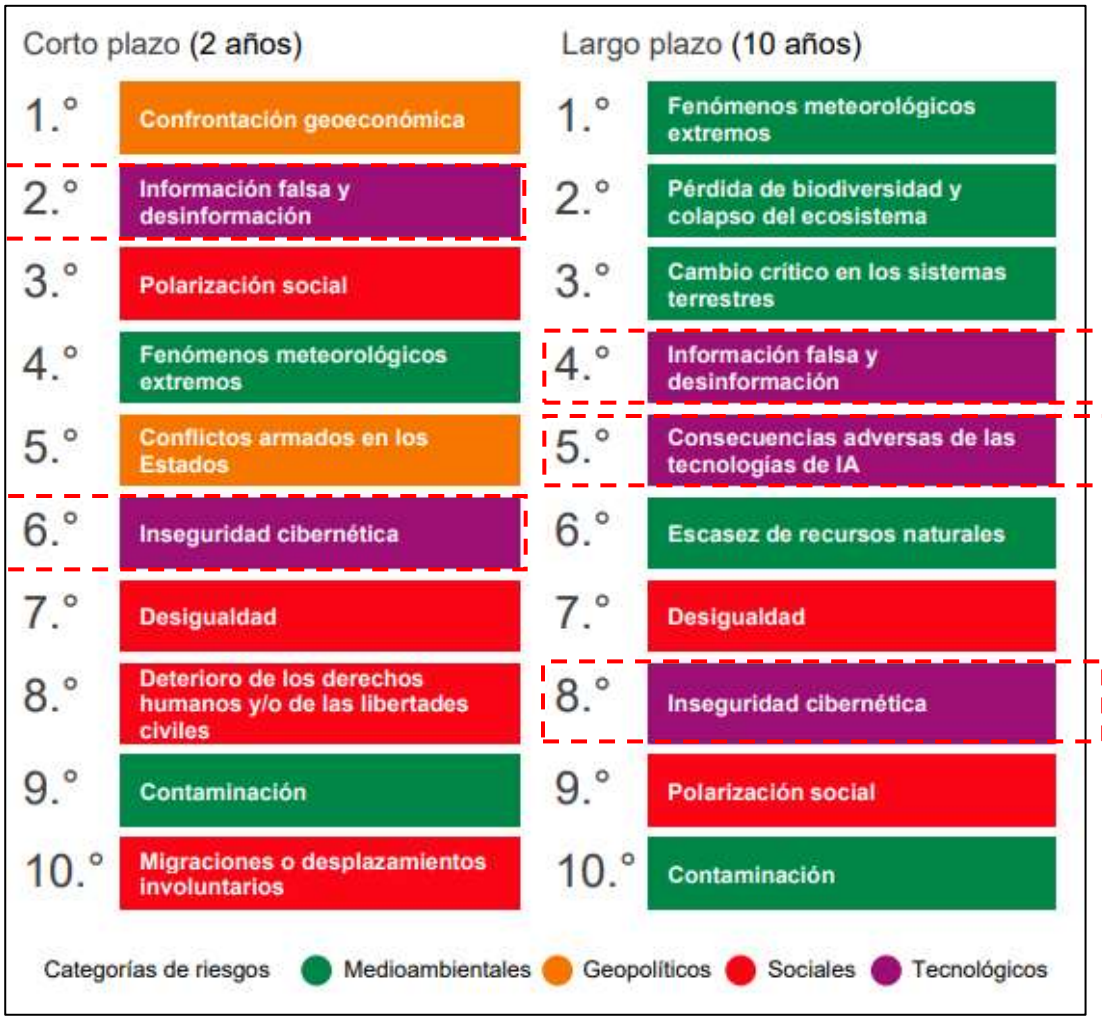


Imagen No.1 – Impacto probable de los riesgos durante un periodo de 2 y 10 años.

2. CIBERATAQUES EN AMÉRICA LATINA Y EL CARIBE.

América Latina se consolidó en 2025 como la región con el mayor crecimiento interanual de ciberataques a nivel mundial: un incremento del 108 % en ataques semanales por organización según Check Point Research, IBM y Kaspersky, alcanzando un promedio de 2.640–3.065 ataques semanales por entidad. Este nivel de actividad supera ampliamente a Asia-Pacífico (2.978), África (2.696), Europa (1.638) y Norteamérica (1.449).

Según la CEPAL, solo el 50 % de los controles de ciberseguridad recomendados son implementados por las empresas de la región. Los sectores más afectados han sido manufactura (+61 % interanual), gobierno, salud y servicios financieros. En el primer semestre de 2025, 1 de cada 5 sistemas de control industrial (ICS) de la región registró intentos de infección, con una tasa 1,8 veces mayor que la de Europa del Norte (Kaspersky ICS CERT).

El auge de las plataformas RaaS impulsadas por IA ha permitido a los grupos de cibercriminales escalar sus ataques. En el primer semestre de 2025 se registraron 1,1 millones de intentos de ransomware en la región, equivalentes a 3.000 ataques diarios (2 por minuto). La tendencia apunta a que el 90 % de las víctimas enfrenta amenazas de publicación de datos como parte de tácticas de doble extorsión.

a. **Países más afectados en América Latina y el Caribe en el 2025:**
Durante el año 2025, varios países de América Latina y el Caribe enfrentaron impactos significativos derivados de ciberataques, tensiones geoeconómicas y fenómenos ambientales extremos.

Las economías más expuestas fueron aquellas con alta dependencia tecnológica y con infraestructuras críticas vulnerables, lo que generó afectaciones en sectores financieros, energéticos y de servicios públicos. Al mismo tiempo, la desinformación digital y la polarización social intensificaron los riesgos en la región, evidenciando la necesidad de fortalecer la cooperación regional y las capacidades de resiliencia para mitigar los efectos de estas amenazas.

País	% Ataques Ransomware (1H 2025)	Ataques Semanales Prom./Org.	Var. Interanual
Brasil	33,85 %	3.348	+21 %
México	15,90 %	3.394	+16 %
Colombia	11,28 %	3.982	+36 %
Argentina	10,77 %	N/D	N/D
Chile	6,15 %	N/D	N/D

Tabla No.5 - Países más afectados a nivel regional 2025. Fuentes: SCILabs/Scitum (Ransomware LATAM 1H 2025); Check Point Research / Infobae (ataques semanales y variación).

Nota: Colombia ascendió al primer lugar en ataques semanales por organización en la región durante 2025, con 3.982 incidentes semanales y un crecimiento del 36 % interanual (Check Point Research / Infobae, diciembre 2025).

b. **Principales Incidentes en Nube en América latina en el 2025:**
Durante 2025, América Latina experimentó un aumento significativo en incidentes relacionados con servicios en la nube, afectando principalmente a sectores financieros, gubernamentales y de telecomunicaciones.

Los ataques más comunes incluyeron accesos no autorizados, filtraciones de datos sensibles y vulnerabilidades en la gestión de credenciales, lo que puso en evidencia la falta de prácticas robustas de seguridad digital en varias organizaciones. Asimismo, la dependencia creciente de soluciones en la nube expuso a las empresas a riesgos de disponibilidad y continuidad operativa, reforzando la necesidad de invertir en estrategias de ciberresiliencia y en marcos regulatorios que fortalezcan la protección de la información en la región.

Incidentes en Nube 2025	Participación
Brechas de Seguridad de Datos.	21%
Uso indebido de Servicios.	17%
Errores de Configuración y Administración.	12%
Incremento de Incidentes en Nube vs. 2023.	+61% (2024 vs. 2023)

Tabla No.6 - Principales Incidentes en Nube en América latina 2025.

3. **CIBERATAQUES EN COLOMBIA.**

Colombia enfrenta en 2025–2026 un escenario de ciberseguridad profundamente complejo. Durante 2024, el país registró 36.000–37.000 millones de intentos de ciberataques según Fortinet, con 77.866 denuncias por delitos informáticos, representando un aumento del 23 % respecto a 2023. En la primera mitad de 2025, Colombia fue víctima de 7,1 mil millones de intentos de ciberataques, ubicándose en tercer lugar en la región según FortiGuard Labs (Fortinet). Las pérdidas económicas por delitos cibernéticos superaron los USD $800 millones en 2024 (ANDI). El país ascendió al puesto 63 en el Índice Nacional de Ciberseguridad (NCSI) en 2024, mejorando seis posiciones, pero los desafíos persisten.

a. **Proyecciones de Ciberataques para Colombia 2025-2026:**

Con base en los datos del primer semestre de 2025 (7,1 mil millones de intentos) y las tendencias globales, se estima que Colombia enfrentará:

- Entre 14.000 y 16.000 millones de intentos de ciberataques durante 2025.
- Un promedio de 3.982 ataques semanales por organización (Check Point Research, dic. 2025).
- Para 2026: incremento proyectado del 36–50 % adicional en intensidad y sofisticación.
- Consolidación de Colombia como primer país de la región en ataques semanales por organización.

b. **Factores que Impulsan el Crecimiento:**

- Adopción Acelerada de Tecnologías Digitales: expansión de la transformación digital en el sector público; crecimiento del comercio electrónico; Estrategia Nacional de Seguridad Digital 2025-2027 del MinTIC; creación del Centro de Operaciones de Seguridad Nacional (SOC).
- Sofisticación de los Atacantes: uso masivo de IA generativa (FraudGPT, WormGPT); plataformas RaaS más accesibles; técnicas avanzadas de ClickFix, Tycoon 2FA, EvilProxy; deepfakes para fraude financiero y BEC.
- Grupos APT Locales y Regionales: el grupo Blind Eagle (APT-C-36) ejecutó en 2025 campañas de spear-phishing que afectaron a Avianca/LifeMiles (48.000 víctimas, USD $6,3M en pérdidas) y entidades estatales.

- Contexto Geopolítico Regional: aumento del ciberespionaje; ataques a infraestructura crítica.

c. **Sectores Claves en Colombia: Balance 2025 y Perspectiva 2026:**

Durante 2025, los sectores estratégicos de la economía colombiana enfrentaron un entorno marcado por la volatilidad internacional, la presión sobre las cadenas de suministro y el avance de riesgos tecnológicos como la ciberinseguridad. En 2026, las perspectivas apuntan a un escenario donde la resiliencia digital y la capacidad de adaptación frente a la desinformación y la polarización social serán determinantes para la competitividad nacional. Al mismo tiempo, los sectores productivos deberán responder a los desafíos ambientales y a la necesidad de fortalecer la cooperación público-privada, consolidando un balance que combine estabilidad económica con sostenibilidad y seguridad tecnológica.

Sector	Situación 2025	Perspectivas 2026
Sector Financiero	• Incremento sostenido de ataques de phishing, ransomware y fraude por deepfakes. • Las entidades financieras concentraron el 18,2 % de ataques con infostealers (Lumu Compromise Report 2025). • El IBM X-Force 2025 identifica el sector como el más atacado por phishing híbrido y compromisos de cadena de suministro. • Pérdidas promedio por brecha: USD $1,1 millones.	• Mayor adopción de IA defensiva, Zero Trust y autenticación biométrica. • El sector liderará la inversión en ciberseguridad (crecimiento estimado del 19 % en 2025). • La colaboración público-privada será clave para compartir inteligencia de amenazas. • Desafío: el ransomware concentra el 79 % de los incidentes en finanzas de LATAM.
Sector Salud	• Los hospitales y clínicas sufrieron ataques de ransomware y robo de historias clínicas. • El 51 % de las instituciones de salud carece de planes robustos de respaldo y recuperación. • El ataque al Ministerio de Salud subrayó la vulnerabilidad de las infraestructuras TIC. • A nivel global el sector salud es el más costoso en filtraciones por 12° año consecutivo (costo medio: USD $10,1 millones/brecha).	• Implementación del Plan Estratégico de Seguridad de la Información del Sector Salud. • Se espera avance en capacitación del personal y adopción de IA para detección proactiva. • Reto: la infraestructura insuficiente y escasez de talento especializado persisten. Necesidad urgente de planes de continuidad operativa ante incidentes.
Sector Gobierno	• Colpensiones registró 53 millones de intentos de intrusión en dos meses (abril–mayo 2025). • Dos entidades estatales sufrieron filtraciones publicadas en la dark web (actor Kazu). • Ataques de ransomware y ciberespionaje afectaron múltiples entidades. • El sector gubernamental concentró el 60 % de ataques anónimos y el 70 % de ransomware según Lumu Compromise Report 2025.	• Consolidación de la Estrategia Nacional de Seguridad Digital 2025-2027 (MinTIC). • Operación del SOC Nacional. Mayor inversión en tecnologías avanzadas de detección. • Reto: coordinación entre niveles de gobierno y fortalecimiento de la cadena de suministro tecnológico del Estado.

Sector Educativo	• Incidentes casi se duplicaron en 2024: 242 incidentes en 14 departamentos vs. 132 en 2023, afectando a más de 48.300 personas. • El sector concentró el 60 % de los ataques anónimos y el 50 % de ataques con droppers (Lumu 2025). • A nivel global, el educativo fue el sector más atacado con 4.349 incidentes semanales por organización (Check Point, dic. 2025).	• Necesidad urgente de modernización de infraestructura TIC. Adopción de plataformas educativas con seguridad integrada. • Capacitación en ciberseguridad para docentes y estudiantes. • Riesgo latente dado que la digitalización educativa post-pandemia amplió la superficie de ataque.

Tabla No.7 - Algunos sectores en Colombia 2025 y 20265.*Fuen*tes: Lumu Compromise Report 2025; IBM X-Force 2025; Fortinet FortiGuard Labs; MinTIC; Check Point Research; NSIT / e-dea.co.

d. **Riesgos en Internet en Colombia:**

El 78 % de los usuarios de internet en Colombia ha estado expuesto a algún tipo de riesgo en línea, superando el promedio global (informe Microsoft). Las PYMES representan el 70 % de las víctimas de ciberataques por limitaciones en inversión tecnológica. El 45 % de los usuarios colombianos recibió al menos un intento de phishing durante 2024.

Riesgos en Internet – Colombia	Incidencia
Desinformación.	59%
Contenidos violentos.	47%
Discurso de odio.	39%
Usuarios expuestos a riesgos digitales.	78%
PYMES víctimas de ciberataques.	70% de las víctimas.

Tabla No.8 – Riesgos en Internet en Colombia 2025. Fuentes: Microsoft / Prey Project / IDC.

e. **Lucha contra el Cibercrimen en Colombia – Resultados 2025:**

En 2024, el Centro Cibernético Policial reportó más de 70.000 incidentes cibernéticos, un aumento respecto a las 59.033 denuncias de 2023. Se evidenció un incremento del 23 % en denuncias por delitos informáticos comparado con 2023. El Centro Cibernético Policial en coordinación con la Fiscalía General de la Nación ejecutó durante 2024 los siguientes resultados operacionales:

- 16 operaciones que conllevaron a 48 capturas.
- Desarticulación de 9 estructuras de cibercrimen.
- 51 allanamientos y más de 535 elementos materiales incautados.
- Impacto a las finanzas criminales por $17.500 millones de pesos.
- Ocupación de 41 bienes.

- Suspensión del poder dispositivo de $5.554 millones en criptomonedas y rastreo de $38 millones de dólares en criptoactivos.

- Bloqueo de 30.165 páginas preventivamente (23.409 de material de abuso sexual infantil; 6.756 de juegos ilegales de azar).

- Atención de 11.866 incidentes informáticos vía plataforma CAI Virtual.

- 424 alertas y contenidos preventivos emitidos.

- 144 charlas de ciberseguridad impactando 13.451 personas

Las principales modalidades reportadas continúan siendo: hurto de cuentas de WhatsApp, suplantación de sitios web (phishing), estafa en compra/venta de productos en internet, gota a gota virtual y hurto de cuentas a redes sociales. La inversión en ciberseguridad en Colombia crecerá un 19 % proyectado hacia 2025–2026, reflejando mayor conciencia institucional y del sector privado.

4. **CIBERATAQUES EN EL DEPARTAMENTO DE ANTIOQUIA.**

El Departamento de Antioquia ha sido especialmente afectado por los ciberataques. Las organizaciones han reportado un aumento en intentos de intrusión y extorsión con impacto significativo en la continuidad operativa. Los dos incidentes más relevantes del período son detallados a continuación.

a. **Ciberataques en Antioquia 2024-2025:**

Durante el periodo 2024-2025, Antioquia registró un incremento sostenido en incidentes de ciberseguridad que afectaron tanto al sector público como al privado. Los ataques más frecuentes estuvieron relacionados con el robo de información, el acceso no autorizado a sistemas críticos y campañas de desinformación digital.

Este panorama evidenció la vulnerabilidad de la infraestructura tecnológica regional y la necesidad de fortalecer las capacidades de prevención, detección y respuesta. El balance refleja que la ciberinseguridad se ha consolidado como un riesgo transversal para la economía y la gobernanza local, lo que exige inversiones en resiliencia digital y cooperación interinstitucional para mitigar sus impactos.

2024 - Hackeo al 123: Emergencias de Medellín con papel y lápiz.	**2025 – EPM: Portal de Pagos Comprometidos / Colpensiones.**
El **11 de febrero de 2024**, el sistema de emergencias 123 de Medellín sufrió un ataque cibernético que obligó a la Central de Atención de Emergencias a suspender sus sistemas digitales y registrar las emergencias de forma manual. El incidente afectó también el funcionamiento de las 3.000 cámaras de la ciudad (dificultando enfoques y generando demoras). Evidenció la vulnerabilidad crítica de la infraestructura pública antioqueña.	El **23 de mayo de 2025**, usuarios reportaron que al ingresar al portal legítimo facturaweb.epm.com.co el sistema los redirigía hacia cuentas de terceros. Algunas víctimas perdieron montos cercanos a $500.000 COP. EPM suspendió sus canales digitales durante 36 horas. Adicionalmente, entre abril y mayo de 2025, Colpensiones (entidad nacional con fuerte presencia en Antioquia) enfrentó 53 millones de intentos de intrusión en dos meses, uno de los volúmenes más altos registrados en una entidad pública del país.

Tabla No.9 - Ataques cibernéticos Departamento de Antioquia 2024–2025. Fuentes: NSIT / e-dea.co / Infobae / medios locales.

b. **Tendencias por Sector en el Departamento de Antioquia 2025-2026:**
En el periodo 2025-2026, los sectores estratégicos de Antioquia muestran dinámicas diferenciadas que reflejan tanto los avances como los desafíos de la región. El sector tecnológico y financiero se enfrenta a un aumento en los riesgos de ciberinseguridad, lo que impulsa la necesidad de fortalecer la resiliencia digital y la protección de datos.

La industria energética y de infraestructura mantiene un papel clave en la competitividad regional, aunque debe adaptarse a presiones ambientales y regulatorias. Por su parte, el sector agroindustrial continúa siendo motor de crecimiento, pero enfrenta retos asociados a sostenibilidad y acceso a mercados internacionales. En conjunto, las tendencias evidencian que la innovación, la seguridad digital y la sostenibilidad serán factores determinantes para el desarrollo económico y social de Antioquia en los próximos años.

Sector	Tipo de Amenazas Principales 2025–2026
Salud	Ransomware, robo de historias clínicas, infostealers.
Servicios Públicos (EPM)	Phishing, APT, compromiso de backend, redirección de pagos.
Financiero	Fraude mediante deepfakes, BEC, infostealers, phishing.
Educativo	Ransomware, robo de información académica, droppers.
Gobierno Local	Ataques a bases de datos, ransomware, filtración en dark web.
PYMES	Ransomware, phishing, ingeniería social potenciada por IA

Tabla No.10 – Tendencias por Sector 2025–2026. Fuentes: Lumu / Check Point / Fortinet / NSIT / IBM X-Force.

c. **Vulnerabilidades Específicas Identificadas en el Departamento:**
- Infraestructura de Servicios Públicos: EPM como proveedor crítico de energía, agua y gas para municipios del Departamento presenta un objetivo de alto valor para grupos APT y ransomware.

- Hospitales y Clínicas: el 51 % de las instituciones de salud carece de planes robustos de respaldo y recuperación ante incidentes.

- Sector Empresarial: el 60 % de las empresas en Colombia no se siente preparada frente a ataques con IA (ESET Security Report 2025).

- Educación: los ataques a instituciones educativas casi se duplicaron en 2024.

5. **LA SEGURIDAD ENDPOINT SEGÚN GARTNER (2025 Y 2026).**
Según Gartner, las Plataformas de Protección de Endpoints (EPP) son cruciales para defender dispositivos gestionados contra amenazas conocidas y desconocidas. En 2025, Gartner reconoció

como líderes del mercado EPP a CrowdStrike, Microsoft, Sophos, SentinelOne y Palo Alto Networks, destacando sus capacidades avanzadas de EDR (Detección y Respuesta en Endpoints) y protección contra amenazas avanzadas.

Para 2026, Gartner predice que la protección autónoma de Endpoints con IA —capaz de tomar decisiones sin intervención humana— será el diferenciador clave. Se espera que la gestión unificada de Endpoints (UEM) y la integración IT/OT sean prioridades estratégicas. Los avances en IA y automatización son elementos centrales para mejorar la capacidad de respuesta y reducir el tiempo medio de detección y contención.

a. **Servicios de Ciberseguridad más Utilizados por CISOs 2025-2026:**

Servicio de Ciberseguridad	Uso Mundial	Uso en Latinoamérica
Servicios Gestionados de Ciberseguridad (MSSP).	Alta demanda por complejidad de amenazas y limitaciones presupuestarias.	Popularidad creciente, especialmente entre PYMES.
Soluciones de Seguridad en la Nube.	Enfoque principal para protección de activos digitales.	Aumento significativo; incidentes en nube crecieron 61 % en 2024.
Consultoría en Ciberseguridad.	Necesidad constante ante escasez de talento especializado.	Clave para mejorar capacidades de respuesta ante amenazas.
Cumplimiento Normativo.	Adaptación a DORA, NIS2, CRA (UE) y regulaciones de IA.	Enfoque en normativas locales y CONPES de ciberseguridad.
Secure Access Service Edge (SASE).	Gana terreno integrando seguridad y red en la nube.	Aumento en adopción para garantizar resiliencia empresarial.
Inteligencia Artificial (IA) Defensiva.	IA utilizada por ambas partes; IA generativa en el 80 % de campañas ransomware.	Implementación en SOC; herramientas como FraudGPT ya operan regionalmente.
Endpoint Security (EPP/EDR/XDR).	Aumento en adopción; CrowdStrike, MS Defender, SentinelOne lideran.	Creciente demanda ante proliferación de dispositivos IoT y móviles.
Zero Trust Architecture.	Marco estratégico prioritario ante incremento de ataques a cadena de suministro.	Adopción acelerada en sector financiero y gobierno de la región.

Tabla No.11 – Servicios de Ciberseguridad más utilizados por CISOs 2025–2026. Fuentes: Gartner / IDC / Check Point / IBM / ESET Security Report 2025.

1.3 Ubicación del proceso en la estructura del Plan de Desarrollo Departamental

PLAN DE DESARROLLO: POR ANTIOQUIA FIRME 2024-2027
LÍNEA ESTRATÉGICA: 55-Autonomía desde la gobernanza
COMPONENTE: 5502-Fortalecimiento institucional y gobernanza
PROGRAMA: 550201-Consolidación de las Tecnologías de la Información y las Comunicaciones
BPIN/BPID: 2024003050159
PROYECTO: Fortalecimiento de los sistemas de información e infraestructura de TIC de la Gobernación de Antioquia
INDICADOR: Ciudadanos que participan por medios electrónicos

1.4 Competencia del organismo para adelantar el proceso

Conforme a lo establecido en el Decreto No. D2024070003913 del 05 de septiembre de 2024, " Por el cual se determina la Estructura Administrativa de la Administración departamental, se definen las funciones de sus organismos y dependencias y se dictan otras disposiciones", se define en el artículo 180 el propósito de la Secretaría de Talento Humano y Servicios Administrativos como: “Liderar la gestión integral del talento humano, el desarrollo organizacional, la formulación, implementación y cumplimiento de políticas, planes, programas y proyectos relacionados con tecnologías de la información y las comunicaciones en la entidad Departamento de Antioquia.

En virtud de este propósito, se define como una de las funciones de la Secretaría de Talento Humano y Servicios Administrativos “Coordinar, articular, promover y adoptar la gestión de las tecnologías de Información y las comunicaciones como apoyo al cumplimiento de las políticas, planes, programas y proyectos de la Gobernación de Antioquia”, a su vez, se define como función de la Subsecretaría de Servicios Administrativos “Dirigir y articular la gestión de las tecnologías de información y las comunicaciones a nivel interno, como apoyo al cumplimiento de las políticas, planes, programas y proyectos de la Gobernación de Antioquia” (artículos 181 y 189, respectivamente).

El artículo 12 de la Ley 80 de 1993 adicionado parcialmente por el artículo 21 de la Ley 1150 de 2007, y el artículo 37 del Decreto 2150 de 1995, facultan al Gobernador en su calidad de Representante Legal del ente territorial, para delegar total o parcialmente la competencia para expedir los actos inherentes a la actividad contractual, realizar los procesos de selección y celebrar los contratos, en los servidores públicos que desempeñen cargos del nivel directivo o ejecutivo o su equivalente.

Por otra parte, mediante Decreto Departamental No. D2025070000089 del 03 de enero de 2025, artículo primero, el señor gobernador del Departamento de Antioquia, en ejercicio de sus facultades constitucionales y legales, delegó en cada uno de los Secretarios de Despacho Misionales y de Apoyo Transversal, dentro de los que se encuentra la Secretaría de Talento Humano y Servicios Administrativos, la competencia para adelantar todas las actividades precontractuales, contractuales y pos - contractuales, con relación a su misión, objetivos y funciones establecidos en el Decreto con fuerza de Ordenanza N° 2024070003913 del 5 de septiembre de 2024 y las demás normas que lo modifiquen, reglamenten, adicionen o complementen.

Por lo anterior, la competencia para adelantar el presente proceso es de la Secretaría de Talento Humano y Servicios Administrativos.

1.5 La forma de satisfacer la necesidad

Para satisfacer la necesidad, se requiere adelantar un proceso de selección abreviada por subasta inversa, con el fin de seleccionar una persona jurídica o natural que posea la experiencia, la capacidad jurídica, técnica y financiera para brindar Servicio de renovación y suscripción de plataforma de protección Endpoint y herramientas en seguridad informática, con el fin de enfrentar las amenazas cibernéticas, así como de afrontar, visualizar y analizar las situaciones que implican riesgos de seguridad de la información para la Entidad.

Se puede satisfacer la necesidad con la contratación de las plataformas de protección de endpoint y herramientas de seguridad digital de acuerdo con las especificaciones técnicas detalladas en el numeral 2.2 Especificaciones técnicas.

2. EL ONTRATAR, CON SUS ESPECIFICACIONES Y LA IDENTIFICACIÓN DEL CONTRATO A CELEBRAR

2.1 Objeto.

RENOVACIÓN Y SUSCRIPCIÓN DE PLATAFORMA DE PROTECCIÓN ENDPOINTS Y HERRAMIENTAS DE SEGURIDAD DIGITAL.

2.1.1 Alcance del Objeto Contractual

Se requiere el Servicio de renovación y suscripción de plataforma de protección Endpoint y herramientas en seguridad digital para los equipos de cómputo de la Gobernación de Antioquia y la Fábrica de Licores y Alcoholes de Antioquia, adicionalmente se requiere adquirir y renovar las herramientas en seguridad informática, por un periodo de 12 meses, con el fin de evitar la materialización de ataques cibernéticos y tener una mejor visibilidad de los eventos maliciosos que están ocurriendo en la red corporativa de la entidad. En las sedes de la Administración Departamental, tales como: Gobernación de Antioquía, Fábrica de Licores y Alcoholes de Antioquia, Secretaría Seccional de Salud de Antioquia y el Programa Aéreo de Salud.

Las herramientas de seguridad informática constan de: auditoria del directorio activo, auditoria de los Servidores de almacenamiento (FileServers), Gestión de contraseñas, escaneo de vulnerabilidades de seguridad informática para la infraestructura tecnológica, solución de Inteligencia artificial que permita identificar ataques sofisticados y la solución Web Application Firewall para proteger los portales web de ataques cibernéticos, ingesta y la adquisición de una herramienta para gestionar las contraseñas de los usuarios del directorio activo de la entidad.

Las características técnicas específicas, el lugar de ejecución y las obligaciones contractuales se definen a continuación en el numeral 2.2 Especificaciones técnicas.

2.2. Especificaciones técnicas:

Ver anexo 1 Especificaciones Técnicas

2.2.1. Adquisición de bienes

No se adquirirán bienes en el presente proceso.

2.2.2. Requerimientos ambientales

Para la renovación del licenciamiento y suscripción de plataforma de protección Endpoint y herramientas en Seguridad Digital del Departamento de Antioquia no le aplican leyes relacionadas con el uso, aprovechamiento o afectación de los recursos naturales.

2.2.3. Requerimientos en materia de Seguridad y Salud en el Trabajo

El SST debe ser implementado por las personas jurídicas y por las personas naturales que tengan personal a cargo conforme a los requisitos señalados en la Resolución 0312 de 2019. Para ello deberá presentar la autoevaluación vigente debidamente firmada por el representante legal y el responsable del Sistema de Seguridad y Salud en el Trabajo, junto con su tarjeta profesional vigente.

El Departamento de Antioquia podrá en cualquier momento pedir información adicional que permita verificar los requisitos de la autoevaluación o el cumplimiento de la normatividad en estándares de Seguridad y Salud en el Trabajo.

2.2.4. Autorizaciones, permisos, licencias y documentos técnicos

EL PROPONENTE debe entregar una certificación expedida por el fabricante en la cual se avale como canal apto para la distribución y/o comercialización, puesta en operación, pruebas y entrega a satisfacción, de las plataformas de antimalware.

2.2.5. Codificación del bien, obra o servicio según las Naciones Unidas – UNSPSC

GRUPO:	E - Productos de Uso Final
SEGMENTO:	43000000 - Difusión de Tecnologías de Información y Telecomunicaciones
FAMILIA:	43230000 - Software
CLASE:	43233200 - Software de seguridad y protección
PRODUCTO:	43233200 - Software de seguridad y protección

CLASIFICACION:	E - Productos de uso final
SEGMENTO:	43000000 - Difusión de Tecnologías de Información y Telecomunicaciones
FAMILIA:	43220000 - Equipos o plataformas y accesorios de redes multimedia o de voz y datos
CLASE:	43222500 - Equipo de seguridad de red
PRODUCTO:	43222500 - Equipo de seguridad de red

2.3. Partes

- Organismo contratante: Departamento de Antioquia - Secretaría de Talento Humano y Servicios Administrativos
- Contratista: Adjudicatario del proceso de selección

2.4 Plazo

Por un periodo de 12 meses contados a partir de la firma del acta de inicio.

2.5 Lugar de ejecución y entrega

El lugar de ejecución será:

Gobernación de Antioquia.
- Centro Administrativo Departamental (CAD) José María Córdova.
- Dirección de Tecnología e Información piso 2 oficina 210
- Calle 42B 52-106, piso 6 Centro de Computo (Data Center)
- Medellín, Antioquia, Colombia.

Fábrica de Licores de Antioquia.
- Carrera 50 # 12 Sur 149.
- Itagüí, Colombia.
- CONMUTADOR +57 604 383 7000.

2.6. Identificación del contrato que se pretende celebrar

Para la ejecución del presente contrato se requiere la **renovación y suscripción de la plataforma de protección de ENDPOINTS y herramientas de seguridad digital**, lo cual corresponde a un contrato de licenciamiento a través de una contratación con modalidad de selección abreviada, causal Subasta Inversa, el cual corresponde a servicios.

2.7. Obligaciones de las Partes
Son las responsabilidades a cargo de las partes y que serán esenciales para el adecuado desarrollo y ejecución del objeto contractual.

2.7.1. Obligaciones Generales de las partes

1. Perfeccionar conjuntamente la minuta del contrato en los términos previstos, suscripción del acta de inicio, suspensiones o prórrogas, modificaciones y en general las actas que se produzcan en el desarrollo del contrato incluyendo acta de liquidación.
2. Suministrar la información disponible que se requiera para la ejecución del contrato.
3. Apoyar técnicamente el desarrollo del contrato.
4. Asistir a las reuniones programadas y brindar la información que se requiera.
5. Coordinar conjuntamente, la realización de visitas técnicas de campo y demás eventos que se consideren necesarios en cumplimiento del objeto.
6. Propender por el logro de los productos pactados.
7. Mantener un flujo constante de la información necesaria durante ejecución y liquidación del contrato; entre otras.
8. Mantener el SECOP II actualizado en cuanto respecta a sus obligaciones

2.7.2 Obligaciones del Contratista

El contratista Seleccionado deberá cumplir el contrato de conformidad con los requerimientos técnicos dados por el Departamento de Antioquia y acordes con las necesidades de la administración. La propuesta presentada debe contemplar los requerimientos que en virtud del contrato le haga el supervisor, ejecutando las demás actividades que se encaminen al cabal cumplimiento y ejecución de sus obligaciones contractuales, tales como:

2.7.2.1. Obligaciones Técnicas

El proponente deberá cumplir con la totalidad de los ítems exigidos en el documento técnico anexo a estos estudios y documentos previos, los requerimientos mencionados en el literal 2.1.1 Alcance del Objeto Contractual, 2.2. Especificaciones técnicas, 2.2.5. Codificación del bien, obra o servicio según las Naciones Unidas – UNS
PSC y las respectivas certificaciones de estos estudios y documentos previos, además de los requerimientos de los diferentes documentos de perfeccionamiento de este proceso contractual.

2.7.2.2. Obligaciones Administrativas, Legales y Financieras

1. Presentar mensualmente un informe que dé cuenta del avance físico, administrativo, financiero y ambiental de la ejecución del contrato.
2. Suministrar todos los equipos y herramientas, personal e instrumentos de trabajo que requiera para la ejecución adecuada de las labores contratadas dentro del plazo contractualmente establecido.
3. Mantener en el sitio de los trabajos el personal requerido para cumplir el objeto del contrato.
4. Disponer de los medios necesarios para la ejecución del contrato, conforme a lo estipulado en los pliegos.
5. Allegar la Garantía con la cual se amparen los riesgos previstos del proyecto para el inicio del plazo contractual, así como las requeridas de acuerdo al inicio del contrato, las prórrogas, las adiciones, modificaciones o restablecimiento de las mismas de conformidad con el plazo establecido;
6. Presentar de manera oportuna los documentos necesarios para el pago de conformidad con la forma de pago establecida en el presente documento.
7. Previo a la suscripción del Acta de Inicio, y durante el plazo contractual, estará a cargo del contratista el pago mensual de salarios, prestaciones sociales, parafiscales, riesgos laborales, y cumplir con sus obligaciones frente al sistema de seguridad social integral, parafiscales (Cajas de Compensación Familiar, SENA e ICBF). Para el efecto el Contratista debe presentar al supervisor del contrato, dentro del término establecido, la documentación que acredite el cumplimiento del pago de estas obligaciones.
8. Facilitar la labor de la supervisión dando respuesta oportuna a las observaciones y/o requerimientos que se realicen, de la cual se dejará constancia escrita.
9. Informar a la Interventoría/supervisión oportunamente sobre cualquier anomalía, inconveniente o dificultad durante la ejecución de las actividades objeto del contrato, y las posibles soluciones para la resolución de los mismos**.**
10. Los informes, recolección de información, resultado y demás actividades asociadas a la ejecución del presente contrato, son de uso exclusivo y propiedad al 100% del Departamento de Antioquia, razón por la cual el contratista debe facilitar todos los documentos, estudios, bases de datos, resultados y demás relacionados al objeto del presente contrato o bien para reportes y análisis propios del Departamento o bien para patente de registro a nombre del Departamento, en los formatos solicitados y sin perjuicio de los derechos de autor que para el caso correspondan.
11. Presentar los informes de cumplimiento ambiental con la periodicidad mensual, de seguridad y salud en el trabajo del proyecto.
12. Garantizar la implementación de las medidas necesarias para prevenir la ocurrencia de posibles accidentes no solo para trabajadores sino para la comunidad en general.
13. Cumplir con los requisitos para la prevención de accidentes y enfermedades laborales del personal propio y/o el de los proveedores de acuerdo con lo establecido en el Código Sustantivo del Trabajo

y demás normas que rijan la materia, dando aplicación en lo que corresponda al Manual de Seguridad y Salud en el Trabajo dirigido a Contratistas del Departamento de Antioquia.

14. La información entregada durante la ejecución del contrato, goza de confidencialidad. El contratista manifiesta que es jurídicamente capaz de salvaguardar la información recolectada y suministrada, obligándose a: 1: Guardar confidencialidad sobre los mecanismos y sistemas de información que se le brinda. 2. Reconocer y dar manejo adecuado a la información recolectada en desarrollo del objeto contractual; 3. Responsabilizarse por la información suministrada; 4. Suministrar información veraz, completa y correcta, en desarrollo de las diferentes actuaciones.
15. Presentar en debida forma la factura correspondiente a la licencia. Si el contratista está obligado a facturar electrónicamente, deberá presentar al Departamento la factura electrónica validada previamente por la DIAN, como requisito necesario para el pago de los bienes y/o servicios contratados, de acuerdo con las instrucciones y directrices de la DIAN.
16. Estarán a cargo del Contratista y de acuerdo al régimen tributario los IMPUESTOS, TASAS Y CONTRIBUCIONES, establecidos por las diferentes autoridades nacionales, departamentales o municipales.
17. El Contratista, bajo la gravedad de juramento, manifiesta que ni él ni sus representantes legales, apoderados, revisor fiscal o quien haga sus veces: i). Están incluidos en la lista ONU emitida por el Consejo de Seguridad de las Naciones Unidas o la lista emitida por la oficina de control de activos extranjeros de las Naciones Unidas (OFAC) también conocida como lista Clinton, ni en ninguna otra lista restrictiva emitida por organismos nacionales o internacionales, policiales, judiciales o de investigación con igual fin; ii). Han participado en actividades de lavado de activos o financiación del terrorismo; iii). Declaración bajo la gravedad de juramento declaración de inasistencia alimentaria.
18. Asumir el pago de salarios, prestaciones e indemnizaciones de carácter laboral del personal que contrate para la ejecución del contrato, lo mismo que el pago de honorarios, los impuestos, gravámenes, aportes y servicios de cualquier género que establezcan las leyes colombianas y demás erogaciones necesarias para la ejecución del contrato.
19. Los precios de los bienes y servicios referenciados por el contratista en la propuesta de precio se entenderán fijos durante la vigencia del contrato.
20. Suministrar al Departamento y/o al supervisor del contrato toda la información que se requiera con el fin de que estos puedan verificar tanto el cumplimiento de los requisitos y compromisos contractuales como los legales a que haya lugar en razón del contrato.
21. De acuerdo al régimen tributario aplicable al caso concreto, el contratista debe inscribirse en la Oficina de Industria y Comercio de los municipios donde se presta el servicio (en caso de que aplique).
22. Las demás que sean inherentes y derivadas de la ejecución del objeto contractual.

2.7.3. Obligaciones del Contratante

1. Realizar el pago del contrato según la forma establecida para ello.
2. Poner a disposición del contratista la información necesaria que se requiera para el desarrollo de las actividades a ejecutar.
3. Asignar un supervisor por parte de la entidad contratante Departamento de Antioquia, para que ejerza las respectivas funciones de seguimiento y control.

4. Verificar la efectiva **renovación y suscripción de la plataforma de protección de endpoints y herramientas de seguridad digital** y el cumplimiento de todos los compromisos adquiridos por parte del Contratista, entre otras.
5. Efectuar por escrito todas las comunicaciones que se refieran a solicitud de servicios, quejas o reclamos al contratista.
6. Velar porque el contratista cumpla con los requisitos normativos de Seguridad y Salud en el Trabajo.
7. Verificar el cumplimiento del pago de salarios / honorarios y demás obligaciones laborales, así como los aportes al Sistema de Seguridad Social Integral, conforme a lo señalado en el Artículo 50 de la Ley 789 de 2002 y normas reglamentarias.
8. Elaborar informes mensuales que dé cuenta del seguimiento del contrato y el cumplimiento del mismo, evidenciándolo según cada necesidad.
9. Mantener al día el SECOP II con el fin de cumplir con la normatividad vigente.
10. Informar por escrito, de manera oportuna e inmediata al CONTRATISTA las posibles irregularidades encontradas durante el desarrollo del contrato.
11. Otras que sean necesarias para coadyuvar a la supervisión del Contrato y para la correcta ejecución contractual.

3. LA MODALIDAD DE SELECCIÓN DEL CONTRATISTA Y SU JUSTIFICACIÓN, INCLUYENDO LOS FUNDAMENTOS JURÍDICOS QUE SOPORTAN SU ELECCIÓN

De conformidad con lo establecido en el Decreto 4170 de 2011, "Por el cual se crea la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente-, se determinan sus objetivos y estructura", ente rector, que tiene como objetivo "desarrollar e impulsar políticas públicas y herramientas, orientadas a la organización y articulación, de los partícipes en los procesos de compras y contratación pública con el fin de lograr una mayor eficiencia, transparencia y optimización de los recursos del Estado", y como una de sus funciones, señalada en el artículo 3 numeral 7, la de "Diseñar, organizar y celebrar los acuerdos marco de precios y demás mecanismos de agregación de demanda de que trata el artículo 2o de la Ley 1150 de 2007, de acuerdo con los procedimientos que se establezcan para el efecto", y en concordancia con lo señalado en el artículo 2.2..1.2.1.2.7 del Decreto 1082 de 2015, modificado por el artículo 1° del Decreto 310 de 2021, el cual quedó de la siguiente manera:

"ARTÍCULO 2.2.1.2.1.2.7. Procedencia del Acuerdo Marco de Precios. Las Entidades Estatales sometidas al Estatuto General de Contratación de la Administración Pública, están obligadas a adquirir Bienes y Servicios de Características Técnicas Uniformes de Común Utilización a través de los Acuerdos Marco de Precios previamente justificados, diseñados, organizados y celebrados por la Agencia Nacional de Contratación Pública –Colombia Compra Eficiente".

La Entidad procedió a verificar si existía Acuerdo Marco de Precios que ofreciera el Servicio de Soporte Técnico y Renovación de las Suscripciones para la Protección Endpoint y Herramientas en Seguridad Informática y comprobó que NO existe dicho acuerdo. Por consiguiente, determinó que la modalidad de contratación para ser aplicada dentro del presente proceso de selección será la señalada en el artículo 2° Numeral 2°, literal a) de la Ley 1150 de 2007 que a la letra dice:

"Selección abreviada. La Selección abreviada corresponde a la modalidad de selección objetiva prevista para aquellos casos en que, por las características del objeto a contratar, las circunstancias de

la contratación o la cuantía o destinación del bien, obra o servicio, puedan adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual.

El Gobierno Nacional reglamentará la materia. Serán causales de selección abreviada las siguientes:

a) La adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades, que corresponden a aquellos que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos.

Para la adquisición de estos bienes y servicios las entidades deberán, siempre que el reglamento así lo señale, hacer uso de procedimientos de subasta inversa o de instrumentos de compra por catálogo derivados de la celebración de acuerdos marco de precios o de procedimientos de adquisición en bolsas de productos".

Lo anterior en concordancia con los artículos 2.2.1.2.1.2.1 y siguientes del Decreto 1082 de 2015, norma que establece el procedimiento de la modalidad de subasta inversa para la adquisición de suministro de bienes y servicios de características técnicas uniformes y de común utilización.

De conformidad a lo anterior y teniendo en cuenta que el objeto del proceso de selección, corresponde a aquellos de características técnicas uniformes, por ser de común utilización y cumplir factores de desempeño similares, la modalidad de selección que corresponde para este proceso de contratación es el de subasta inversa. Adicionalmente, se llevará a cabo mediante subasta inversa electrónica en consideración a que la Secretaría de Suministros y Servicios cuenta con las herramientas informáticas necesarias para adelantarla en forma electrónica. (Se realizará a través de la plataforma de Secop II)

El presente proceso de selección se desarrollará con arreglo a los principios de transparencia, economía, responsabilidad, y de conformidad con los postulados que rigen la función administrativa, señalados en los artículos 209 la Constitución Política de Colombia, en las Leyes 80 de 1993 y 1150 de 2007.

Para satisfacer la necesidad de la entidad se realiza consulta en la Tienda Virtual del Estado Colombiano www.colombiacompra.gov.co, categoría: Tecnología, productos: Software Empresarial, acuerdo marco CCENEG-027-1-2020. Se hace una búsqueda en el catálogo: Antivirus, Escaneo de vulnerabilidades, Software de gestión de PQRS, software de gestión documental, Herramientas ITSM y software de videoconferencia por medio fabricantes y proveedores internacionales a través de sus partners en Colombia. Tener cobertura total para la adquisición de sus soluciones de software a lo largo y ancho del país. Adquirir servicios de soporte, migración, parametrización y capacitación relacionados con los servicios de software descritos anteriormente.

En el acuerdo marco referenciado solo se ofrecen la protección del EndPoint y la herramienta para análisis de vulnerabilidades en Seguridad informática, de acuerdo a lo anterior se evidencia que en esta subcategoría no se encuentran componentes asociados a los servicios de Protección de Ambientes web en la nube, software de auditoria para el directorio activo, software auditoria a los servidores de archivos, protección de análisis de comportamiento de última generación a servidores,

por lo cual no cubre la totalidad de lo descrito en el numeral 2.2 que satisface las necesidades de la entidad.

De acuerdo a lo anterior en la categoría de “Tecnología” y las subcategorías “Software Empresarial” se evidencia que en esta subcategoría no se encuentran componentes asociados a los servicios de Protección de Ambientes web en la nube, software de auditoria para el directorio activo, software de auditoría a los servidores de archivos, protección de análisis de comportamiento de última generación a servidores, tal y como se evidencia a continuación:

Acuerdos Marcos de Precios (AMP) vigentes para TI:

- Conectividad.
- Centro de datos y nube privada.
- Nube pública.
- Centro de contacto.
- Microsoft.
- Google.
- Suministro de Servicios de Impresión II.
- Consumibles de Impresión II.
- Servicios de BPO II.
- Software Empresarial
- Contratación de Mesa de Servicio.
- Compra o alquiler de Equipos Tecnológicos y Periféricos II.

4. EL VALOR ESTIMADO DEL CONTRATO Y LA JUSTIFICACIÓN DEL MISMO, INDICANDO LAS VARIABLES UTILIZADAS PARA CALCULAR EL PRESUPUESTO DE LA CONTRATACIÓN Y LOS RUBROS QUE LO COMPONEN

4.1 Análisis del sector

Ver anexo 2 análisis del sector

4.2. Presupuesto oficial

Anexo 3 presupuesto oficial.

Se estima el presupuesto oficial en $826.098.989 OCHOCIENTOS VEINTISÉIS MILLONES NOVENTA Y OCHO MIL NOVECIENTOS OCHENTA Y NUEVE MIL PESOS MLC Incluido el IVA del 19%

Aportan recursos las siguientes secretarías:

- DIRECCIÓN DE TECNOLOGÍA E INFORMACIÓN: $640.683.000 Seiscientos cuarenta con seiscientos ochenta y tres mil pesos MLC
- SECRETARIA SECCIONAL DE SALUD DE ANTIOQUIA: $171.200.000 Ciento setenta y un millones doscientos mil PESOS MLC.

- FÁBRICA DE LICORES Y ALCOHOLES DE ANTIOQUIA: $90.000.000 Noventa millones de PESOS MLC.

4.3 Forma de pago de los recursos

La Gobernación de Antioquia, en virtud de este contrato se compromete a pagar el valor del contrato en un (1) único pago cuando se cumplan las siguientes condiciones: con la suscripción de los productos a nombre del Departamento de Antioquia, entrega del certificado de los servicios de ENDPOINT y herramientas de seguridad informática; El valor que le corresponde pagar a la FLA el proponente favorecido debe generar factura directamente a nombre de la Fábrica de Licores y Alcoholes de Antioquia.

El pago se realizará dentro de los 30 días hábiles siguientes a la presentación de la factura, bajo los parámetros establecidos en la Circular K2020090000025 del 10 de enero de 2020 de la Secretaría de Hacienda, Dirección de Contabilidad.

Se pagará bajo los parámetros establecidos en la Circular K2024090000009 del 09 de enero de 2024, de la Secretaría de Hacienda, Dirección de Contabilidad, previo recibo a satisfacción por parte del Supervisor del contrato, donde se visualice el período pagado acorde con la fecha de la factura de pagos de parafiscales y sistema general de seguridad social, de conformidad con el Artículo 50 de la Ley 789 de 2002.
Es de aclarar, que en todo pago la Gobernación de Antioquia efectúa la retención de las siguientes estampillas:

Estampilla Pro-Desarrollo	0.6%
Estampilla Pro-Hospitales Públicos	1.0%
Estampilla Bienestar del Adulto Mayor	2.0%
Estampilla Politécnico Jaime Isaza Cadavid	0.4%
Estampilla Pro-Universidad de Envigado	0.4%
Estampilla Pro-Universidad Digital	0.4%
Tasa Pro-Deporte	2.5%
Total, de Estampillas	**7.3%**

Tabla No.12 – Retención de Estampillas.

Adicionalmente y en cumplimiento de las circulares 131 de 2013, 848 de 2014 y 538 de 2015 expedidas por la Secretaría de Hacienda del Departamento el contratista deberá acreditar con anterioridad a la suscripción del acta de inicio su registro en la Oficina de Industria y comercio de los Municipios en los que se ejecutarán las actividades contractuales.

Parágrafo 1. En caso de que el contratista esté obligado a facturar electrónicamente estará obligado a presentar la factura electrónica validada previamente por la DIAN, como requisito necesario para el pago, conforme a las disposiciones señaladas en el Decreto 358 del 5 de marzo de 2020, en concordancia con lo dispuesto en la Resolución 0042 del 5 de mayo de 2020 y demás normas que los modifiquen, complementen o sustituyan.

Parágrafo 2. La Entidad no se hace responsable por las demoras presentadas en el trámite para el pago al contratista cuando ellas fueren ocasionadas por encontrarse incompleta la documentación de soporte o no ajustarse a cualquiera de las condiciones establecidas en el presente Contrato.

Parágrafo 3. La Entidad hará las retenciones a que haya lugar sobre cada pago, de acuerdo con las disposiciones legales vigentes sobre la materia.

Parágrafo 4. Para el pago el contratista deberá allegar paz y salvo de seguridad social y aportes parafiscales.

4.4. Número de registro en el Banco de Proyectos, Rubro Presupuestal, Certificado de Disponibilidad Presupuestal y Vigencia futura

DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y LA COMUNICACIÓN

BANCO DE PROYECTOS:
Nombre: Fortalecimiento de los sistemas de información e infraestructura de TIC de la Gobernación de Antioquia
BPIN/BPID: 2024003050159
Elemento: 16-0044
Vigente hasta: 20 de junio del 2026

RUBRO PRESUPUESTAL: 2320202008/173H/0-1010/C23011/160044
CDP: 3500057223, fecha de impresión: 13/03/2026, valor $640.683.000.
NOTA, de los recursos de este CDP se utilizará el valor de $564.898.989, el valor restante se le solicitará liberación de saldo a favor
PROYECTO: 16-0044
Vigencia futura: N/A

SECRETARIA SECCIONAL DE SALUD DE ANTIOQUIA

BANCO DE PROYECTOS:
Nombre: Fortalecimiento de la arquitectura empresarial y transformación digital en salud en el Departamento de Antioquia
BPIN/BPID: 2024003050143
Elemento PEP: 16-0043
Vigente hasta: 18 de junio de 2026

RUBRO PRESUPUESTAL: 2320202008/131D/0-OI2648/C23024/160043
CDP: 3500057236 fecha de impresión: 26/03/2026, valor: $171.200.000
PROYECTO: 160043
Vigencia futura: N/A

FÁBRICA DE LICORES Y ALCOHOLES DE ANTIOQUIA

BANCO DE PROYECTOS:
Nombre: N/A
BPIN/BPID: N/A
Elemento PEP: N/A
Vigente hasta: N/A

RUBRO PRESUPUESTAL: 2120202008/907A/0-FE1010
CDP: 3700014798, fecha de impresión: 17/03/2026, valor: $90.000.000
Vigencia futura: N/A

5 LOS CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE

De conformidad con la normativa aplicable por tratarse de una Selección Abreviada por Subasta Inversa Electrónica, se tendrá como único criterio de evaluación y selección el MENOR PRECIO OFERTADO.

El Artículo 2.2.1.1.2.2.2 del Decreto 1082 de 2015, en relación a los procesos de selección abreviada mediante subasta inversa señala que: La entidad Estatal debe determinar la oferta más favorable teniendo en cuenta las normas aplicables a cada modalidad de selección del contratista. Sobre el particular de la escogencia del contratista, el Artículo 2.2.1.2.1.2.4 del Decreto 1082 de 2015, dispone que la entidad estatal debe adjudicar el proceso de subasta inversa electrónica al oferente que haya presentado el lance más bajo.

Aunado a lo anterior, para poder participar del proceso contractual, se debe de cumplir con los requisitos que se establecen en el numeral 2 Artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015, el cual manifiesta: La oferta debe contener dos partes, la primera en la cual el interesado acredite su capacidad de participar en el proceso de contratación y acredite el cumplimiento de la Ficha Técnica; y la segunda parte debe contener el precio inicial propuesto por el oferente.

El Departamento verifica la capacidad jurídica, la experiencia, capacidad financiera y de organización que dé certeza que los proponentes cuenten con la organización e infraestructura que permita el cumplimiento de las obligaciones surgidas del contrato.

5.1 Requisitos Habilitantes y de Participación

La capacidad jurídica y las condiciones de experiencia, capacidad financiera y de organización de los proponentes serán objeto de verificación de cumplimiento como requisitos habilitantes para la participación en el proceso de selección y no otorgan puntaje.

5.1.1 Requisitos de Orden Jurídico

Todos los proponentes se deben presentar bajo alguna de las siguientes modalidades, siempre y cuando cumplan las condiciones exigidas en el Pliego de Condiciones:

Individualmente como: a) personas naturales nacionales o extranjeras; b) personas jurídicas nacionales o extranjeras, que se encuentren debidamente constituidas, previamente a la fecha de apertura del

proceso de selección, o c) como consorcios o uniones temporales que se constituyan con el único objeto de presentar propuesta y ejecutar el contrato, caso en el cual al proponente le será aplicable lo dispuesto en el artículo 7 de la Ley 80 de 1993, modificado por el artículo 3 de la Ley 2160 de 2021.

TODOS LOS PROPONENTES

Deben:

- Tener capacidad jurídica para la presentación de la propuesta.
- Tener capacidad jurídica para la celebración y ejecución del contrato.
- No estar incursos en ninguna de las causales de inhabilidad o incompatibilidad previstas en las leyes de Colombia, en especial las previstas en los artículos 8 y 9 de la Ley 80 de 1993, modificado por el artículo 6 de la Ley 2014 de 2019.
- Las personas jurídicas, proponentes y/o los miembros integrantes de los consorcios y/o uniones temporales deberán acreditar, cada uno, que su duración no será inferior a la del plazo del contrato y dos (02) años más.

LAS PERSONAS NATURALES Y JURÍDICAS

Las personas naturales deben aportar su cédula de ciudadanía y acreditar individualmente la inscripción en el Registro Único de Proponentes, en donde conste su actividad, y calidad.

Las personas jurídicas deben acreditar individualmente la inscripción en el Registro Único de Proponentes, así como el Certificado de Existencia y Representación Legal, en donde conste su existencia, representación legal y facultades del representante legal, el cual deberá ser expedido con una antelación no superior de treinta (30) días anteriores a la fecha de cierre de la Selección Abreviada mediante Subasta Inversa.

La duración de las personas jurídicas nacionales o extranjeras (tengan o no domicilio o sucursal en Colombia) deberán acreditar que el plazo de duración de la sociedad es como mínimo el plazo del contrato y dos (02) años más, dicha circunstancia se verificará en el Certificado de existencia y representación legal expedido por la autoridad competente.

En ambos casos, deberán aportar la Identificación Tributaria por medio del RUT (Registro Único Tributario).

PERSONAS NATURALES EXTRANJERAS

Adicional a todos los requisitos establecidos para participar en el presente proceso, las personas naturales extranjeras que pretendan presentar propuesta en el mismo deben presentar fotocopia de su cédula de extranjería o pasaporte.

PERSONAS NATURALES EXTRANJERAS CON DOMICILIO EN COLOMBIA

Las personas naturales extranjeras que tengan domicilio en Colombia deben estar inscritas en el Registro Único de Proponentes y deben anexar a su propuesta este documento.

PERSONAS NATURALES EXTRANJERAS SIN DOMICILIO EN COLOMBIA

Las personas naturales extranjeras sin domicilio en Colombia no requieren estar inscritos en el Registro Único de Proponentes. La entidad verificará directamente la información sobre la capacidad jurídica y las condiciones de experiencia, capacidad financiera y de organización, del artículo 2.2.1.1.1.5.2 Decreto 1082 de 2015. Adicionalmente, acreditarán un apoderado domiciliado en Colombia, debidamente facultado para presentar la propuesta y celebrar el contrato, así como también para representarla judicial y extrajudicialmente.

PERSONAS JURÍDICAS EXTRANJERAS

PERSONAS JURÍDICAS EXTRANJERAS CON DOMICILIO O SUCURSAL EN COLOMBIA

Sin perjuicio del cumplimiento de los requisitos establecidos en el presente pliego, deben presentar el Certificado de Existencia y Representación expedido por la Cámara de Comercio respectiva, expedido dentro de los treinta (30) días anteriores a la fecha de cierre del proceso de selección. Igualmente, deben estar inscritas en el Registro Único de Proponentes y deben anexar a su propuesta este documento.

PERSONAS JURÍDICAS EXTRANJERAS SIN DOMICILIO O SUCURSAL EN COLOMBIA

Sin perjuicio del cumplimiento de los requisitos establecidos en el presente pliego, deben presentar el Certificado de Existencia y Representación que en el país de origen les permite acreditar tal calidad, expedido dentro de los treinta (30) días anteriores a la fecha de cierre del proceso de selección. La entidad verificará directamente la información sobre la capacidad jurídica y las condiciones de experiencia, capacidad financiera y de organización del artículo 2.2.1.1.1.5.3 Decreto 1082 de 2015.

Las condiciones a exigir se deben señalar en el pliego, así como los parámetros de verificación y los documentos que se deben presentar. Adicionalmente, acreditarán un apoderado domiciliado en Colombia, debidamente facultado para presentar la propuesta y celebrar el contrato, así como también para representarla judicial y extrajudicialmente.

LOS CONSORCIOS Y UNIONES TEMPORALES (DILIGENCIAR ANEXO)
Información de interés general: Señor proponente: recuerde que este proceso de selección, se adelanta bajo las condiciones de la plataforma SECOP II, por tanto, en caso de presentar su propuesta bajo la figura de proponente plural (CONSORCIOS O UNIONES TEMPORALES) deberá realizar todos los trámites de su propuesta por medio de la plataforma mencionada. Para el efecto, se informa que existe una guía de Colombia Compra Eficiente que podrá encontrar en el siguiente link.

https://www.colombiacompra.gov.co/sites/cce_public/files/cce_documentos/20170323_guia_proponente_plural_version_revisada.pdf

Nota: De acuerdo a los términos de uso del Secop II, en los Procesos de Contratación se entienden como no presentadas las ofertas de proponentes plurales presentadas desde cuentas de proponentes

singulares y viceversa. Se sugiere revisar las indicaciones dadas en la “Guía rápida para la creación de proponentes plurales en el SECOP II” expedida por Colombia Compra Eficiente.

Se entenderá por propuesta conjunta, una propuesta presentada en consorcio o unión temporal. En tal caso se tendrá como proponente, para todos los efectos, el grupo conformado por la pluralidad de personas y no las personas que lo conforman individualmente consideradas.

Podrán participar consorcios y uniones temporales, para lo cual se deberán cumplir los siguientes requisitos: Acreditar la existencia del consorcio o de la unión temporal, y específicamente la circunstancia de tratarse de uno u otro, aportando el documento de conformación donde conste de manera expresa en el acuerdo correspondiente, señalando las reglas básicas que regulan las relaciones entre ellos, los términos, actividades, condiciones.

Los proponentes indicarán si su participación es a título de consorcio o unión temporal, y deberán señalar los términos y extensión de su participación en la propuesta y en la ejecución del contrato, El proponente y/o los miembros integrantes de los consorcios y/o uniones temporales deberán acreditar, cada uno, que su duración no será inferior a la del plazo del contrato y dos (02) años más.

Los miembros del consorcio o de la unión temporal deberán designar la persona que, para todos los efectos, representará al consorcio o unión temporal y señalarán las reglas básicas que regulen las relaciones entre ellos y su responsabilidad, de conformidad con lo señalado en el parágrafo 1º del artículo 7º de la Ley 80 de 1993, modificado por el artículo 3 de la Ley 2160 de 2021.

La forma asociativa deberá constituirse para el presente proceso de selección y así lo señalará expresamente, indicando las reglas básicas que lo regirán, independiente que las personas naturales o jurídicas que lo conformen, sean las mismas que hayan constituido consorcios o uniones temporales para otros procesos. Dichas formas asociativas no podrán ser disueltas ni liquidadas durante la vigencia o prórrogas del contrato que se suscriba y dos (02) años más.

Deberán cumplir con lo estipulado en el artículo 7° de la Ley 80 de 1993, modificado por el artículo 3 de la Ley 2160 de 2021 y con los siguientes aspectos:

La forma asociativa deberá indicar el porcentaje de participación de cada uno de sus integrantes, la cual no podrá ser modificada. En el documento de conformación de la forma asociativa se deberá designar la persona que para todos los efectos la representará con sus responsabilidades y facultades.

En caso de ser adjudicatarios los Consorcios, Uniones Temporales u otras formas asociativas deberán presentar ante el Departamento de Antioquia el correspondiente RUT, cuyo NIT deberá ser único y exclusivo para cada contrato, lo anterior conforme el Decreto nacional 2460 de 2013.

De acuerdo con lo preceptuado en el Artículo 66 de la Ley 488 de 1998 y el Instructivo de aspectos tributarios de la Secretaría de Hacienda Departamental, las facturas o documentos equivalentes para pago deben ser expedidas directamente por la respectiva forma de asociación, cumpliendo los requisitos establecidos en el Estatuto Tributario y no por cada uno de sus integrantes. Para proceder con su respectivo pago debe indicarse, además, el nombre, el Nit de los integrantes del Proponente plural y el porcentaje de participación en el mismo.

Los integrantes de los consorcios o uniones temporales deberán ser personas naturales o jurídicas que cumplan individualmente con los requisitos exigidos en el presente Pliego de Condiciones, salvo los casos expresamente señalados.

Para los Consorcios o Uniones Temporales, se exige individualmente para cada integrante del consorcio o unión temporal el cumplimiento de estos Requisitos.

Si el representante del Consorcio o Unión Temporal es diferente a alguno de los integrantes persona natural o representante legal de la persona jurídica, el proponente deberá allegar la documentación que acredite la capacidad jurídica de la persona designada como representante por lo cual, también deberá allegar toda la documentación solicitada en los requisitos de orden jurídico.

CERTIFICADO DE RECIPROCIDAD

Conforme a lo establecido en el artículo 20 de la Ley 80 de 1993 y el parágrafo del artículo 1 de la Ley 816 de 2003 modificado por el artículo 51 del Decreto Ley 019 de 2012, se otorgará tratamiento de bienes y servicios nacionales a aquellos de origen extranjero.

DOCUMENTOS SUSCRITOS POR CONTADOR O REVISOR FISCAL

Los documentos y certificaciones que deban suscribir el contador público o revisor fiscal, según corresponda, deberán acompañarse de cédula de ciudadanía, copia de la tarjeta profesional y anexar certificado de antecedentes disciplinarios, expedido por la Junta Central de Contadores, este certificado debe estar vigente para la fecha de presentación de la propuesta (no mayor a 3 meses de expedición).

DOCUMENTOS QUE DEBEN ADJUNTARSE A LA PROPUESTA

Los documentos que acrediten los factores de escogencia deberán ser remitidos por el proponente al momento del cierre.

Los documentos relacionados con los requisitos de la propuesta que no afecten la asignación de puntaje, pueden ser aportados hasta el vencimiento del plazo otorgado por la entidad para entregarlos.

En el evento de que en la etapa de evaluación de las propuestas no se haya efectuado por parte de la entidad el requerimiento respectivo, el proponente podrá aportar los documentos que no afecten la asignación de puntaje hasta antes de la adjudicación.

La propuesta se deberá acompañar de los documentos necesarios para la verificación de la capacidad jurídica, financiera, económica, técnica, y de organización.

La información contenida en el certificado del registro de proponentes, será la base para allanar las reglas de cumplimiento e idoneidad, en las condiciones del Decreto 1082 de 2015 y el parágrafo 1º del artículo 5 de la Ley 1150 de 2007.

CARTA DE PRESENTACIÓN DE LA PROPUESTA

El formato de carta de presentación de la propuesta entregado por la entidad, deberá estar suscrito por las personas que allí se indican, de conformidad con el anexo.

CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL

Aportar Certificado de Existencia y Representación Legal o el Certificado de Registro Mercantil, expedido por la entidad competente, se exceptúa para el ejercicio de profesiones liberales. En caso de que el proponente sea consorcio, unión temporal u otra forma asociativa, cada uno de sus integrantes deben anexar la certificación correspondiente, el cual deberá ser expedido con una antelación no superior de treinta (30) días anteriores a la fecha de cierre del proceso.

Tratándose de sociedades extranjeras con sucursal en el país, la Existencia y Representación Legal se acreditará con el RUP, y en caso de no tener sucursal en el país, deberá aportar el documento que acredite la adquisición de la personería jurídica en el país de origen, el cual contenga como mínimo los siguientes datos:

• Nombre o razón social completa del proponente
• Tipo, número y fecha del documento de constitución o creación
• Fecha y clase de documento por el cual se reconoce la personería jurídica
• Duración de la entidad

Cuando en el documento aportado que acredita la existencia y representación legal de la persona jurídica extranjera no cuente con toda la información requerida, podrán adjuntar una certificación del representante legal de la sociedad extranjera o en su defecto del mandatario de la sucursal con los datos que faltan, la cual se entiende formulada bajo la gravedad del juramento.

Los documentos otorgados en el exterior deberán presentarse legalizados en la forma prevista en las normas vigentes sobre la materia.

El objeto social del proponente debe tener relación directa con el objeto de la contratación.

La expedición de dicho certificado no podrá tener una anterioridad superior a treinta (30) días calendario, contados a partir de la fecha de cierre del proceso.

CÉDULA DE CIUDADANÍA VIGENTE
Para el caso de los oferentes que se presenten en su condición de personas naturales o del representante legal si es persona jurídica.

AUTORIZACIÓN PARA CONTRATAR
Cuando el representante legal de la firma proponente, de conformidad con el Certificado de Existencia y Representación Legal expedido por la entidad competente, tenga limitada su capacidad para participar en el proceso de selección y suscribir el contrato, deberá presentar la autorización del órgano directivo correspondiente. En caso de que el proponente sea consorcio, unión temporal u otra forma asociativa, cada uno de sus integrantes debe anexar la certificación correspondiente. Cuando se actúe

en calidad de apoderado, deberá acreditarse tal condición, mediante documento legalmente otorgado (Artículo 24 de la Ley 962 de 2005).

CERTIFICADO DE INSCRIPCIÓN EN EL REGISTRO ÚNICO DE PROPONENTES

El Departamento de Antioquia, debe verificar con el Registro Único de Proponentes el cumplimiento de los requisitos habilitantes. Esta verificación se hará de acuerdo con el artículo 2.2.1.1.1.5.2 y 2.2.1.1.1.5.3 del Decreto 1082 de 2015 y el manual para determinar y verificar los requisitos habilitantes en Procesos de Contratación, expedido por Colombia Compra Eficiente.

La Agencia Nacional de Contratación Pública – Colombia Compra Eficiente emitió el Concepto C-480 de 2021, en el cual establece que la entidad contratante rechazará al proponente cuando la inscripción del RUP que realice, ya sea por primera vez o cuando han cesado sus efectos y debe volver a inscribirse, no esté en firme en la fecha prevista para el cierre del procedimiento de selección. Esto teniendo en cuenta que no es posible acreditar situaciones ocurridas con posterioridad al cierre del proceso. El acto de inscripción del RUP adquiere firmeza y presunción de legalidad a partir de la ejecutoria de este, de manera que únicamente el RUP en firme es plena prueba de las condiciones habilitantes de los proponentes.

De conformidad con el Concepto C-480 de 2021, tratándose del trámite de renovación, se reitera lo expresado en el sentido de que la persona que presentó la información para renovar su registro a más tardar el quinto día de abril de cada año, cumpliendo el requisito del artículo 2.2.1.1.1.5.1. y pese a que la renovación no esté en firme, es decir, mientras esté en trámite el proceso de renovación, puede participar en los procedimientos de selección, debiéndose tener en cuenta la información «antigua». De esta manera, en el período comprendido entre el momento de la solicitud de renovación y el de su firmeza, se debe emplear la información del RUP que está en firme antes de iniciar el trámite de renovación, cuyos efectos no habrían cesado y se encontraría vigente. Incluso, en caso de que el RUP con la información «antigua» se haya presentado válidamente antes del cierre del proceso y con posterioridad a este quede en firme el nuevo RUP, para la evaluación de las propuestas se deberá utilizar la información del registro presentado inicialmente.

Cuando se trate del trámite administrativo de la actualización, sucede algo similar que con la renovación, en el sentido de que si la actualización no estaba en firme para el momento del cierre del proceso, en la evaluación se tendrá en cuenta únicamente la información que estaba en firme para dicho momento.

Los proponentes deberán estar inscritos y clasificados en el Registro Único de Proponentes de la Cámara de Comercio de su jurisdicción, de acuerdo con las condiciones establecidas en el Título VI Registro Único de Proponentes –RUP del Decreto 1082 de 2015.

La renovación del RUP deberá llevarse a cabo a más tardar el quinto día hábil del mes de abril del presente año, de lo contrario cesarán los efectos de la inscripción.

El certificado constituye plena prueba respecto de la información verificada documentalmente y cuyo registro se encuentre en firme, firmeza que se produce diez (10) días hábiles después de su publicación en el Registro Único Empresarial (RUE).

La expedición de dicho certificado no podrá tener una anterioridad superior a treinta (30) días calendario, contados a partir de la fecha de cierre del proceso. En caso que el proponente sea consorcio, unión temporal u otra forma asociativa, cada uno de sus integrantes deben anexar la certificación correspondiente.

PROPONENTES EXTRANJEROS SIN DOMICILIO O SUCURSAL EN COLOMBIA

Sin perjuicio del cumplimiento de los requisitos establecidos en el presente pliego, deberá acreditar su existencia y representación legal a efectos de lo cual presentará un documento expedido por la autoridad competente en el país de su domicilio, con fecha de expedición igual o inferior a ciento veinte (120) días calendario anteriores a la fecha del cierre definitivo del presente proceso de selección, en el que conste su existencia, objeto y vigencia, y el nombre del representante legal de la sociedad o de la persona o personas que tengan la capacidad para comprometerla jurídicamente y sus facultades, y en el cual se señale expresamente que el representante no tiene limitaciones para presentar la Propuesta y suscribir el Contrato.

Cuando el representante legal tenga limitaciones estatutarias, se presentará adicionalmente copia del acta o documento en donde conste la decisión del órgano social correspondiente que autorice al representante legal para presentar la Propuesta, la suscripción del Contrato y para actuar en los demás actos requeridos para la contratación en el caso de resultar Adjudicatario.

En caso que el documento expedido por la autoridad competente del país de su domicilio, no contenga toda la información requerida, deberá acompañar a su oferta el o los documentos públicos o privados mediante los cuales acredite el cumplimiento de lo exigido por la Entidad.

Los anteriores requisitos se acreditarán de conformidad con la Ley vigente del País de origen de la sociedad proponente.

El proponente extranjero y los integrantes de los oferentes plurales extranjeros deberán diligenciar el Formulario correspondiente anexo en documentos del proceso en la plataforma del SECOP II, en el cual deberá manifestar bajo la gravedad del juramento que no tiene Sucursal en Colombia, ni ejerce actividades de comercio de carácter permanente en el país.

Para la presentación de la oferta no será necesario que se constituya una sucursal en Colombia pues esto es solo obligatorio si se resulta adjudicatario en Procesos de Contratación que tengan por objeto la construcción de obras o prestación de servicios, pues en estos dos casos, se entiende que la persona jurídica extranjera está ejerciendo negocios permanentes en Colombia".

Se aclara que si el oferente acredita que los servicios se prestaran en su totalidad fuera del territorio Colombiano no será necesario que se constituya una sucursal en Colombia.

Adicionalmente, acreditarán un apoderado domiciliado en Colombia, debidamente facultado para presentar la propuesta y celebrar el contrato, así como también para representarla judicial y extrajudicialmente.

APODERADO, PERSONA JURÍDICA EXTRANJERA

Las personas jurídicas extranjeras sin domicilio en Colombia deberán acreditar en el país un apoderado domiciliado en Colombia, debidamente facultado para presentar la propuesta, participar y comprometer a su representado en las diferentes instancias del presente proceso de selección, suscribir los documentos y declaraciones que se requieran así como el contrato ofrecido, suministrar la información que le sea solicitada, y demás actos necesarios de acuerdo con el proceso contractual, así como para representarla judicial o extrajudicialmente.

Dicho apoderado podrá ser el mismo apoderado único para el caso de personas extranjeras que participen en consorcio, unión temporal o promesa de sociedad futura, y en tal caso bastará para todos los efectos, la presentación del poder común otorgado por todos los participantes del consorcio, unión temporal o promesa de sociedad futura.

En todos los casos, deberán cumplirse todos y cada uno de los requisitos legales exigidos para la validez y oponibilidad en Colombia de documentos expedidos en el exterior, con el propósito de que puedan obrar como prueba conforme con lo dispuesto en los artículos 74 y 251 de la Ley 1564 de 2012 (Código General del Proceso), y el artículo 480 del código de comercio y las demás normas vigentes.

NOTA: Cuando el proponente extranjero, sin domicilio o sucursal en Colombia, provenga de un país que hace parte de la Convención de la Haya, sobre la “abolición de requisitos de legalización para documentos públicos extranjeros”, no se requiere de la Consularización a que se refiere en el párrafo anterior, sino que será suficiente que los documentos se adicionen con el certificado de “apostille”, por parte de la autoridad competente del país donde se origina el documento.

Anexo a este poder deberá allegarse copia de la cédula de ciudadanía del representante legal de la firma apoderada.

DECLARACIÓN JURAMENTADA PROPONENTE EXTRANJERO- FORMULARIO

El proponente extranjero y todos los integrantes de los oferentes plurales extranjeros deberán manifestar bajo la gravedad del juramento en escrito independiente suscrito por el representante legal que no tiene Sucursal en Colombia, ni ejerce actividades de comercio de carácter permanente en el país.

CONSULARIZACIÓN

De conformidad con lo previsto por el artículo 480 del Código de Comercio que señala: “Los documentos otorgados en el exterior se autenticarán por los funcionarios competentes para ello en el respectivo país, y la firma de tales funcionarios lo será a su vez por el cónsul colombiano o, a falta de éste, por el de una nación amiga, sin perjuicio de lo establecido en convenios internacionales sobre el régimen de los poderes.

Al autenticar los documentos a que se refiere este artículo los cónsules harán constar que existe la sociedad y ejerce su objeto conforme a las leyes del respectivo país.” Los proponentes deberán dar

cumplimiento a lo señalado en el citado artículo, respecto a los documentos otorgados o expedidos en el exterior, así como a la existencia de la respectiva sociedad.

Documento expedido en el exterior Cuando se trate de documentos de naturaleza pública otorgados en el exterior, de conformidad con lo previsto en la Ley 455 de 1998, no se requerirá del trámite de Consularización señalado en el numeral anterior, siempre que provenga de uno de los países signatarios de la Convención de La Haya del 5 de octubre de 1961, sobre abolición del requisito de legalización para documentos públicos extranjeros, aprobada por la Ley 455 de 1998.

En este caso solo será exigible la apostille, trámite que consiste en el certificado mediante el cual se avala la autenticidad de la firma y el título a que ha actuado la persona firmante del documento y que se surte ante la autoridad competente en el país de origen.

Conforme a la Circular Externa única de Colombia Compra, los proponentes podrán presentar documentos en un idioma distinto al castellano junto con la traducción simple al castellano. El proponente puede presentar con la oferta documentos con una traducción simple al castellano y entregar la traducción oficial al castellano dentro del plazo previsto para la subsanación.

Así mismo, para el término de traslado estos documentos deben cumplir con el requisito de legalización y apostille previstos en el artículo 251 del Código General del Proceso.

Serán aceptados los documentos presentados por las personas jurídicas extranjeras con los cuales se acredita su existencia y representación legal teniendo en cuenta su propia legislación.

REGISTRO ÚNICO TRIBUTARIO (RUT)

Documento expedido por la Dirección de Impuestos y Aduanas Nacionales, donde aparezca claramente el NIT del proponente. En caso de Consorcio y/o Unión Temporal, cada uno de sus miembros deberá aportar el respectivo registro.

Para el caso de personas naturales y jurídicas extranjeras, documento similar, expedido por la autoridad competente.

APORTES PARAFISCALES Y DE SEGURIDAD SOCIAL (DILIGENCIAR ANEXO)

El proponente deberá acreditar que se encuentra al día en el pago de aportes al Sistema de Seguridad Social Integral (salud, pensiones y ARL), y aportes parafiscales mediante certificación suscrita por el revisor fiscal y/o representante legal, en aquellos casos que sea procedente. De conformidad con lo dispuesto en la Ley 789 de 2002, cuando se trate de personas jurídicas, se deberá certificar que se han efectuado los pagos dentro de los últimos seis (6) meses anteriores a la fecha de cierre del proceso de selección. No obstante, lo anterior, el proponente deberá encontrarse al día por todo concepto de aportes al sistema de seguridad social integral y a los parafiscales.

Además, en los casos en que el certificado de paz y salvo de seguridad social y aportes parafiscales sea suscrito por el contador o revisor fiscal, deberá allegarse la cédula del contador o revisor fiscal, la

tarjeta profesional y los antecedentes disciplinarios emitido por la Junta Central de Contadores con fecha de expedición no mayor a 3 meses a la fecha de cierre del proceso.

Adicionalmente, cuando el proponente se encuentre exento de realizar el pago de aportes parafiscales (SENA e ICBF), deberá también realizar una manifestación suscrita por el revisor fiscal y/o representante legal, según corresponda, que acredite su condición de beneficiario de dicha exoneración al cumplir con los presupuestos normativos del artículo 114-1 del Estatuto Tributario adicionado por el artículo 65 de la Ley 1819 de 2016.

Cuando se trate de consorcio o uniones temporales, cada uno de sus miembros integrantes, deberá aportar los certificados aquí exigidos.

Cuando el proponente sea persona natural, deberá acreditar que se encuentra al día en el pago de aportes al Sistema de Seguridad Social Integral (salud, pensiones y ARL), mediante certificación suscrita por el mismo, acompañada de las planillas de pago al sistema se seguridad social.

CERTIFICADOS DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA Y DE LA PROCURADURÍA GENERAL DE LA NACIÓN

Certificado vigente tanto para el representante legal como de la persona jurídica a la que representan, de no estar incurso en causal de inhabilidad, de conformidad con el Boletín de Responsables Fiscales de la Contraloría General de la República y la certificación de antecedentes disciplinarios de la Procuraduría General de la Nación, los cuáles serán verificados por el Departamento de Antioquia.

Para realizar dicha verificación de antecedentes fiscales acceder al siguiente link:
https://www.contraloria.gov.co/control-fiscal/responsabilidad-fiscal/certificado-de-antecedentes-fiscales

Para verificar antecedentes disciplinarios de la Procuraduría General de la Nación acceder al siguiente link:
https://www.procuraduria.gov.co/portal/Certificado-de-Antecedentes.page

Para el caso de modalidades de asociación y de personas jurídicas diferentes a las sociedades de capital, este requisito debe ser cumplido por todos los socios y representantes legales de las sociedades participantes.

Cuando se trate de consorcio o uniones temporales, cada uno de sus miembros integrantes, deberá aportar los certificados aquí exigidos, tanto para el representante legal como de la persona jurídica a la que representan.

VERIFICACIÓN DE ANTECEDENTES JUDICIALES

La Administración Departamental verificará que no registren antecedentes judiciales de conformidad con el Artículo 94 del Decreto Ley 019 de 2012, respecto del proponente y el representante legal y todos los socios de las personas jurídicas, consorcios o uniones temporales o cualquier otra forma de asociación, con excepción de las sociedades de capital, las cuales deberán suplir dicho requisito con

la manifestación escrita y expresa por parte del representante legal que ninguno de los socios registran antecedentes judiciales.

Para realizar dicha verificación acceder al siguiente link:
http://antecedentes.policia.gov.co:7003/WebJudicial/.

CERTIFICADO DEL REGISTRO NACIONAL DE MEDIDAS CORRECTIVAS

Conforme lo ordena el artículo 183 de la Ley 1801 de 2016 Código Nacional de Policía y Convivencia. Aportar reporte del Registro Nacional de Medidas Correctivas, del proponente persona natural y/o persona jurídica. En caso de aparecer en dicho reporte, se dará aplicación al contenido del numeral 4 del artículo 183 de la Ley 1801 de 2016, Código Nacional de Policía.

Para realizar dicha verificación acceder al siguiente link:
https://srvpsi.policia.gov.co/PSC/frm_cnp_consulta.aspx

Cuando se trate de consorcio o uniones temporales, cada uno de sus miembros integrantes, deberá aportar los certificados aquí exigidos, para el representante legal de la persona jurídica a la que representan.

CERTIFICADO DE INHABILIDADES, INCOMPATIBILIDADES O CONFLICTOS DE INTERÉS

No podrán presentar propuesta quienes se encuentren incursos en causales de inhabilidades e incompatibilidades que les impidan celebrar contratos con entidades públicas, de acuerdo con la Constitución Política de 1991, Ley 80 de 1993, el Art. 18 de la Ley 1150 de 2007, Ley 1474 de 2011, Ley 1778 de 2016, Ley 2195 de 2022 y demás normas aplicables que la modifique y/o adicione.

Debe diligenciarse el formato correspondiente.

Cuando se trate de consorcio o uniones temporales, cada uno de sus miembros integrantes, deberá aportar los certificados aquí exigidos.

CERTIFICADO ANTICORRUPCIÓN / LISTA CLINTON

El proponente deberá diligenciar el formato anexo en donde manifieste bajo la gravedad del juramento que ni el, ni sus accionistas o socios y/o sus administradores, miembros de junta directiva, representantes legales, apoderados, revisor fiscal, o quienes hagan sus veces:

a) Están incluidos en la lista de la ONU emitida por el Consejo de Seguridad de las Naciones Unidas, o la lisa emitida por la Oficina de Control de Activos Extranjeros (OFAC) también conocida como Lista Clinton, ni en ninguna otra lista restrictiva emitida por organismos nacionales o internacionales, policiales, judiciales o de investigación con igual fin.
b) Han participado en actividades de lavado de activos o financiamiento del terrorismo. El proponente o contratista según aplique, entiende y acepta que en el evento de incurrir en cualquiera de las situaciones referidas en los literales anteriores, su propuesta será rechazada de plano, o si se

materializa durante la relación contractual con el Departamento de Antioquia, esta entidad dará por terminado el contrato de manera unilateral.

En el caso de las modalidades asociativas, como consorcios o uniones temporales, entre otras, esta declaración se debe realizar en la propuesta o contrato según el caso, por cada uno de los integrantes de la figura jurídica interviniente.

GARANTÍA DE SERIEDAD DE LA PROPUESTA

Por un valor correspondiente al diez por ciento (10%) del Presupuesto Oficial y con una vigencia de tres (3) meses contados a partir de la fecha de cierre del proceso de selección, a favor de entidades estatales. Esta garantía podrá consistir en una póliza expedida por compañías de seguros legalmente autorizadas para funcionar en Colombia o en una garantía bancaria o patrimonio autónomo.

En el caso de declaratoria de desierta, la entidad procederá a devolver la garantía de seriedad de la oferta a los proponentes que lo soliciten por escrito.

La no presentación de la garantía o póliza de seriedad de la oferta, dará lugar al rechazo de la propuesta, de conformidad con lo prescrito en el parágrafo 3 del artículo 5 de la Ley 1882 de 2018.

En caso de presentarse proponentes plurales (consorcios o uniones temporales), la póliza de seriedad de la propuesta deberá ser tomada a nombre del consorcio o unión temporal, indicando el nombre de cada uno de sus integrantes y debe de estar suscrita por el representante legal del mismo.

CUBRIMIENTO DE LA GARANTÍA DE SERIEDAD

La garantía de seriedad de la oferta cubrirá los perjuicios derivados del incumplimiento del ofrecimiento, en los siguientes eventos:

- Retiro de la oferta después de vencido el plazo para su presentación
- La no suscripción del contrato sin justa causa por parte del proponente seleccionado.
- La no ampliación de la vigencia de la garantía de seriedad de la oferta cuando el término previsto en los pliegos para la adjudicación del contrato se prorrogue o cuando el término previsto para la suscripción del contrato se prorrogue, siempre y cuando esas prórrogas no excedan un término de tres meses.
- La falta de otorgamiento por parte del proponente seleccionado, de la garantía de cumplimiento exigida por la entidad para amparar el incumplimiento de las obligaciones del contrato.

MULTAS O SANCIONES O DECLARACIÓN JURAMENTADA

El ANEXO MULTAS Y SANCIONES debe ser diligenciado y firmada por el proponente si ha sido objeto de multas y/o sanciones a consecuencia de incumplimientos cualquiera sea su denominación, de lo contrario deberá suscribir el ANEXO DECLARACIÓN JURAMENTADA.

TRATAMIENTO DE DATOS PERSONALES

De conformidad con lo dispuesto en la Ley 1581 de 2012 y de conformidad con lo señalado en el Decreto 1074 de 2015, el proponente deberá diligenciar el formato anexo “Autorización para el tratamiento de datos personales”.

5.1.2 Requisitos de Orden Técnico

5.1.2.1 Experiencia Habilitante Del Proponente

CERTIFICACIÓN HABILITANTE

EL PROPONENTE debe entregar una certificación expedida por el fabricante en la cual se avale como canal apto para la distribución y/o comercialización, puesta en operación, pruebas y entrega a satisfacción, de las plataformas de antimalware.

EXPERIENCIA HABILITANTE

El proponente deberá acreditar experiencia hasta máximo tres (3) contratos cuyo objeto y/o alcance esté relacionado con el objeto del presente proceso. Los contratos con los cuales pretenda acreditar la experiencia deberán estar inscritos en el RUP de conformidad con lo establecido en el acápite anterior, además deberán estar ejecutados, terminados y/o liquidados con entidades públicas y/o privadas y su sumatoria deberá ser igual o mayor al 50% del valor del presupuesto oficial expresado en SMMLV. Estos deberán estar debidamente certificados en el Registro Único de Proponentes e identificados en el clasificador de bienes y servicios, en algunos de los siguientes códigos UNSPSC:

GRUPO:	E - Productos de Uso Final
SEGMENTO:	43000000 - Difusión de Tecnologías de Información y Telecomunicaciones
FAMILIA:	43230000 - Software
CLASE:	43233200 - Software de seguridad y protección
PRODUCTO:	43233200 - Software de seguridad y protección
CLASIFICACION:	E - Productos de uso final
SEGMENTO:	43000000 - Difusión de Tecnologías de Información y Telecomunicaciones
FAMILIA:	43220000 - Equipos o plataformas y accesorios de redes multimedia o de voz y datos
CLASE:	43222500 - Equipo de seguridad de red
PRODUCTO:	43222500 - Equipo de seguridad de red

El proponente deberá cumplir con la totalidad de los ítems exigidos en el documento técnico anexo a estos estudios y documentos previos, los requerimientos mencionados en el literal 2.1.1 Alcance del Objeto Contractual, 2.2. Especificaciones técnicas, 2.2.5. Codificación del bien, obra o servicio según las Naciones Unidas – UNSPSC y las respectivas certificaciones de estos estudios y documentos previos, además de los requerimientos de los diferentes documentos de perfeccionamiento de este proceso contractual.

5.1.2.1.1 Acreditación de la experiencia requerida

Por lo anterior, las certificaciones a enviar por parte de los interesados deberán contener:

- Número del contrato, cuando aplique
- Nombre o razón social de la empresa o persona contratante
- Objeto del contrato
- Valor del contrato
- Plazo de ejecución del contrato
- Fecha de iniciación del contrato
- Fecha de terminación del contrato
- Nombre y firma de la persona que expide la certificación.
- Alcance, actividades y/o obligaciones cuando se requiere acreditar actividades específicas.
- Si los contratos fueron ejecutados bajo la modalidad de consorcio o unión temporal, deberá informar el porcentaje de participación y el valor correspondiente a cada contratista en forma separada.
- Si un Proponente adquiere experiencia en un contrato como integrante de un Proponente plural, la experiencia derivada de ese contrato corresponde a la ponderación del valor del contrato por el porcentaje de participación.

Las certificaciones expedidas por la entidad contratante se pueden complementar adjuntando acta de recibo a satisfacción, acta de liquidación, copias del contrato o convenio. La Entidad podrá verificar la veracidad y autenticidad de las certificaciones presentadas a través de los mecanismos que considere pertinentes. Los contratos o convenios que se encuentren en ejecución, a la fecha de cierre del presente proceso, no serán tenidos en cuenta para la verificación de la experiencia.

La experiencia de los proponentes que por su naturaleza no requieren de inscripción en el Registro único de Proponentes, será validadas a través de las certificaciones contractuales y su contenido deberá corresponder con el que se exige en el presente numeral.

Tratándose de proponentes plurales se tendrá en cuenta lo siguiente: i) uno de los integrantes debe aportar como mínimo el cincuenta por ciento (50%) de la experiencia exigida; ii) los demás integrantes deben acreditar al menos el cinco por ciento (5%) de la experiencia requerida; y iii) sin perjuicio de lo anterior, solo uno de los integrantes, si así lo considera pertinente, podrá no acreditar experiencia. En este último caso, el porcentaje de participación del integrante que no aporta experiencia en la estructura plural no podrá superar el cinco por ciento (5%).

La experiencia debe ser cumplida por cada uno de los integrantes de la modalidad de asociación, en el código UNSPSC anteriormente relacionado.

Si los contratos fueron ejecutados bajo la modalidad de consorcio o unión temporal, se tomará el valor correspondiente al porcentaje de participación que hubiere tenido en los mismos.

En caso de acreditar, experiencia de los socios o accionistas, cuando la sociedad tiene menos de 3 años de constitución, se deberá aportar el acta de constitución del proponente, o el documento idóneo donde conste la conformación accionaria del proponente.

En el evento en que dos o más proponentes aporten una misma información y está presente inconsistencias, se solicitará la aclaración respectiva a cada uno de ellos y sólo se tendrá en cuenta aquella que esté demostrada.

Cuando la Entidad en desarrollo de la verificación de la Experiencia requiera confirmar información adicional del proponente, podrá solicitar los documentos que considere necesarios para el esclarecimiento de la información, tales como certificaciones adicionales o cualquier otro soporte.

En aquellos casos en que por las características del objeto a contratar se requiera verificar información adicional a la contenida en el RUP, el proponente podrá aportar uno o algunos de los documentos que se establecen a continuación, para que la entidad realice la verificación en forma directa. Los mismos deberán estar debidamente diligenciados y suscritos por el contratante, el contratista o el interventor, según corresponda. En caso de existir discrepancias entre dos (2) o más documentos aportados por el proponente para la acreditación de experiencia, se tendrá en cuenta el orden de prevalencia establecido a continuación:

a) Acta de liquidación
b) Acta de entrega, terminación, final o de recibo definitivo.
c) Certificación de experiencia. Expedida con posterioridad a la fecha de terminación del contrato en la que conste el recibo a satisfacción de la obra contratada debidamente suscrita por quien esté en capacidad u obligación de hacerlo.
d) Acta de inicio o la orden de inicio. La misma sólo será válida para efectos de acreditar la fecha de inicio.
e) Para los contratos que hayan sido objeto de cesión, el contrato deberá encontrarse debidamente inscrito y clasificado en el RUP o en uno o alguno de los documentos considerados como válidos para la acreditación de experiencia de la empresa cesionaria, según aplique. La experiencia se admitirá para el cesionario y no se reconocerá experiencia alguna al cedente.

5.1.2.1.2 EXPERIENCIA CRITERIO DIFERENCIAL

5.1.2.1.2.1 MIPYME

El proponente que cuente con la calidad de MIPYME, de acuerdo a los criterios de clasificación empresaria, definidos en el artículo 2.2.1.13.2.2 del Decreto 1074 de 2015, Único Reglamentario del Sector Comercio, Industria y Turismo, podrá acreditar la experiencia con hasta cuatro (4) contratos cuyo objeto y/o alcance esté relacionado con el objeto del presente proceso. Los contratos con los cuales pretenda acreditar la experiencia deberán estar inscritos en el RUP de conformidad con lo establecido en el acápite anterior, además deberán estar ejecutados y terminados, y su sumatoria deberá ser igual o mayor al 50% del valor del presupuesto oficial expresado en SMMLV. Estos deberán estar debidamente certificados en el Registro Único de Proponentes e identificados en el clasificador de bienes y servicios, en los siguientes códigos:

GRUPO: E - Productos de Uso Final
SEGMENTO: 43000000 - Difusión de Tecnologías de Información y Telecomunicaciones
FAMILIA: 43230000 - Software
CLASE: 43233200 - Software de seguridad y protección
PRODUCTO: 43233200 - Software de seguridad y protección

CLASIFICACION: E - Productos de uso final
SEGMENTO: 43000000 - Difusión de Tecnologías de Información y Telecomunicaciones
FAMILIA: 43220000 - Equipos o plataformas y accesorios de redes multimedia o de voz y datos
CLASE: 43222500 - Equipo de seguridad de red
PRODUCTO: 43222500 - Equipo de seguridad de red

De los contratos presentados para acreditar la experiencia (máximo 4), el proponente deberá cumplir experiencia específica con la capacidad jurídica, técnica y financiera para brindar Servicio de soporte técnico de la plataforma de protección Endpoint y herramientas en seguridad informática, con el fin de enfrentar las amenazas cibernéticas, así como de afrontar, visualizar y analizar las situaciones que implican riesgos de seguridad de la información para la Entidad.

Se puede satisfacer la necesidad con la contratación de las plataformas de protección de ENDPOINT y herramientas de seguridad informática de acuerdo con las especificaciones técnicas detalladas en el numeral 2.2 Especificaciones técnicas.

Las condiciones contenidas en el numeral 5.1.2.1.1 Acreditación de la experiencia requerida, aplicarán al presente requisito, excepto la disposición respecto a la acreditación de experiencia en proponentes plurales, la cual aplica la siguiente:

Tratándose de proponentes plurales se tendrá en cuenta lo siguiente: i) uno de los integrantes debe aportar como mínimo el cincuenta por ciento (50%) de la experiencia exigida; ii) los demás integrantes deben acreditar al menos el cinco por ciento (5%) de la experiencia requerida; y iii) sin perjuicio de lo anterior, solo uno de los integrantes, si así lo considera pertinente, podrá no acreditar experiencia, en todo caso este integrante que no acredite experiencia deberá acreditar la condición de Mipyme de acuerdo con lo dispuesto en el presente numeral. En este último caso, el porcentaje de participación del integrante que no aporta experiencia en la estructura plural no podrá superar el diez por ciento (10%).

La experiencia debe ser cumplida por cada uno de los integrantes de la modalidad de asociación, en alguno de los códigos UNSPSC anteriormente relacionados.

Si los contratos fueron ejecutados bajo la modalidad de consorcio o unión temporal, se tomará el valor correspondiente al porcentaje de participación que hubiere tenido en los mismos.

De conformidad con el artículo 2.2.1.2.4.2.18 del Decreto 1860 de 2021, para que un proponente, singular o plural, pueda acceder a criterios diferenciales para Mipyme en el presente proceso, deberá acreditar su condición de la siguiente manera:

1. Las personas naturales mediante certificación expedida por ellos y un contador público, adjuntando copia del registro mercantil, en el que se certifique el cumplimiento de los criterios para ser Mipyme, de conformidad con en el artículo 2.2.1.13.2.2 del Decreto 1074 de 2015.

2. Las personas jurídicas mediante certificación expedida por el representante legal y el contador o revisor fiscal, si están obligados a tenerlo, adjuntando copia del certificado de existencia y representación legal expedido por la Cámara de Comercio o por la autoridad competente para expedir dicha certificación, en el que se certifique el cumplimiento de los criterios para ser Mipyme, de conformidad con en el artículo 2.2.1.13.2.2 del Decreto 1074 de 2015. En todo caso, las Mipyme también podrán acreditar esta condición con la copia del certificado del Registro Único de Proponentes, el cual deberá encontrarse vigente al cierre del proceso.

Nota 1: En todo caso, las Mipyme también podrán acreditar esta condición con la copia del certificado del Registro Único de Proponentes, el cual deberá encontrarse vigente y en firme al momento de su presentación.

Nota 2: Los proponentes aportarán la copia del registro mercantil, del certificado de existencia y representación legal o del Registro Único de Proponentes, según corresponda conforme a las reglas precedentes, con una fecha de máximo sesenta (60) días calendario anteriores al cierre del proceso.

Nota 3: Tratándose de proponentes plurales, los criterios diferenciales y los puntajes adicionales solo se aplicarán si por lo menos uno de los integrantes acredita la calidad de Mipyme y tiene una participación igual o superior al diez por ciento (10%) en el consorcio o la unión temporal.

Nota 4: Si los requisitos de acreditación de criterios diferenciales son objeto de subsanación, no se podrá otorgar los puntajes al momento de la calificación de las propuestas.

EMPRENDIMIENTOS Y EMPRESAS DE MUJERES.

En cumplimiento de lo preceptuado en los artículos 2.2.1.2.4.2.14 y 2.2.1.2.4.2.1.5 del Decreto 1860 de 2021, se podrá acreditar la experiencia para emprendimientos y empresas de mujeres de la siguiente manera:
El proponente que cuente con la calidad de emprendimientos o empresas de mujeres que trata el artículo 2.2.1.2.4.2.14 y 2.2.1.2.4.2.1.5 del Decreto 1860 de 2021 podrá acreditar la experiencia con máximo cuatro (4) certificaciones de experiencia, relacionadas directamente con el objeto y/o alcance del presente proceso. Los contratos con los cuales pretenda acreditar la experiencia deberán estar inscritos en el RUP de conformidad con lo establecido en el acápite anterior, además deberán estar ejecutados y terminados, y su sumatoria deberá ser igual o mayor al 50% del valor del presupuesto oficial en SMMLV y deberán estar debidamente certificados en el Registro Único de Proponentes, identificados en el clasificador de bienes y servicios, en el siguiente código:

GRUPO: E - Productos de Uso Final
SEGMENTO: 43000000 - Difusión de Tecnologías de Información y Telecomunicaciones
FAMILIA: 43230000 - Software
CLASE: 43233200 - Software de seguridad y protección
PRODUCTO: 43233200 - Software de seguridad y protección

CLASIFICACION: E - Productos de uso final
SEGMENTO: 43000000 - Difusión de Tecnologías de Información y Telecomunicaciones
FAMILIA: 43220000 - Equipos o plataformas y accesorios de redes multimedia o de voz y datos

CLASE: 43222500 - Equipo de seguridad de red
PRODUCTO: 43222500 - Equipo de seguridad de red

Las demás condiciones contenidas en el numeral anterior, ACREDITACIÓN DE LA EXPERIENCIA REQUERIDA, aplicarán al presente requisito.

No se tendrán en cuenta para la evaluación los contratos que no estén registrados en el RUP. La información se verificará a partir de los contratos reportados en el Registro Único de Proponentes hasta el tercer nivel, cuya sumatoria sea mayor o igual al 50% del presupuesto oficial en SMMLV.

Si los contratos fueron ejecutados bajo la modalidad de consorcio o unión temporal, se tomará el valor correspondiente al porcentaje de participación que hubiere tenido en los mismos.

Si la propuesta es presentada en Consorcio o Unión Temporal u otra forma asociativa, dentro de los contratos certificados en el RUP, cada uno de los integrantes deberá acreditar su experiencia de acuerdo con el porcentaje de su participación del mismo y en todo caso el proponente plural deberá cumplir con el sumatorio total del 50% del presupuesto oficial.

PROCEDIMIENTO PARA LA ACREDITACIÓN DE CALIDAD DE EMPRENDIMIENTO O EMPRESA DE MUJERES

Para que el proponente pueda acreditar la calidad de emprendimientos o empresas de mujeres, deberá aportar y cumplir con las condiciones del Artículo 2.2.1.2.4.2.14 del Decreto 1082 de 2015, adicionado por el artículo 3º del Decreto 1860 de 2021, además, deberá de aportar toda la información y documentación necesaria para acreditar dicha(s) condición(es) de la siguiente manera:

1. Cuando más del cincuenta por ciento (50%) de las acciones, partes de interés o cuotas de participación de la persona jurídica pertenezcan a mujeres y los derechos de propiedad hayan pertenecido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección. Esta circunstancia se acreditará mediante certificación expedida por el representante legal y el revisor fiscal, cuando exista de acuerdo con los requerimientos de ley, o el contador, donde conste la distribución de los derechos en la sociedad y el tiempo en el que las mujeres han mantenido su participación.

1. Cuando por lo menos el cincuenta por ciento (50%) de los empleos del nivel directivo de la persona jurídica sean ejercidos por mujeres y éstas hayan estado vinculadas laboralmente a la empresa durante al menos el último año anterior a la fecha de cierre del Proceso de Selección en el mismo cargo u otro del mismo nivel.

Se entenderá como empleos del nivel directivo aquellos cuyas funciones están relacionadas con la dirección de áreas misionales de la empresa y la toma de decisiones a nivel estratégico. En este sentido, serán cargos de nivel directivo los que dentro de la organización de la empresa se encuentran ubicados en un nivel de mando o los que por su jerarquía desempeñan cargos encaminados al cumplimiento de funciones orientadas a representar al empleador.

Esta circunstancia se acreditará mediante certificación expedida por el representante legal y el revisor fiscal, cuando exista de acuerdo con los requerimientos de ley, o el contador, donde se señale de manera detallada todas las personas que conforman los cargos de nivel directivo del proponente, el número de mujeres y el tiempo de vinculación. La certificación deberá relacionar el nombre completo y el número de documento de identidad de cada una de las personas que conforman el nivel directivo del proponente. Como soporte, se anexará copia de los respectivos documentos de identidad, copia de los contratos de trabajo o certificación laboral con las funciones, así como el certificado de aportes a seguridad social del último año en el que se demuestren los pagos realizados por el empleador.

2. Cuando la persona natural sea una mujer y haya ejercido actividades comerciales a través de un establecimiento de comercio durante al menos el último año anterior a la fecha de cierre del proceso de selección. Esta circunstancia se acreditará mediante la copia de cédula de ciudadanía, la cédula de extranjería o el pasaporte, así como la copia del registro mercantil.

3. Para las asociaciones y cooperativas, cuando más del cincuenta por ciento (50%) de los asociados sean mujeres y la participación haya correspondido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección. Esta circunstancia se acreditará mediante certificación expedida por el representante legal.

Nota 1. Respecto a los incentivos contractuales para los emprendimientos y empresas de mujeres, las certificaciones de trata el presente artículo deben expedirse bajo la gravedad de juramento con una fecha de máximo treinta (30) días calendario anteriores a la prevista para el cierre del procedimiento de selección.

Nota 2. Tratándose de proponentes plurales, los criterios diferenciales y los puntajes adicionales solo se aplicarán si por lo menos uno de los integrantes acredita que es emprendimiento y empresa de mujeres bajo los criterios dispuestos en el artículo precedente y que tiene una participación igualo superior al diez por ciento (10%) en el consorcio o la unión temporal.

El proponente deberá diligenciar el ANEXO: EMPRENDIMIENTOS Y EMPRESAS DE MUJERES, y aportar todos los documentos necesarios para acreditar la condición., dispuesto en el pliego de condiciones.

5.1.2.3. Otros requisitos de orden técnico

Ver Anexo 1 Especificaciones Técnicas

.

5.1.2 Requisitos de Orden Financiero

De conformidad con lo establecido en el numeral 15 del artículo 25 de la Ley 80 de 1993, Artículo 6 de la Ley 1150 de 2007 modificado por el artículo 221 del Decreto Ley 019 de 2012 y el Decreto 1082 de 2015, según corresponda, de acuerdo con la actividad a contratar, la capacidad financiera será objeto de verificación a todos los proponentes, sin calificarse por cuanto no es factor de comparación de las ofertas.

Con respecto del año 2024, se conserva lo establecido en el parágrafo transitorio 3º del artículo 2.2.1.1.1.5.2. de la Subsección 5 de la Sección 1 del Capítulo 1 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015 adicionado por el artículo 1º del del Decreto 1041 de 2022, reglamenta:

> *"PARÁGRAFO TRANSITORIO 3. En el año 2023, para efectos de la inscripción o renovación del Registro Único de Proponentes, el interesado reportará la información contable de que tratan los numerales 1.3 y 2.3 de este artículo, correspondiente a los últimos tres (3) años fiscales anteriores al respectivo acto.*
>
> *En aquellos eventos en que el proponente no tenga la antigüedad suficiente para aportar la información financiera correspondiente a los tres (3) años descritos en el inciso anterior, podrá acreditar dicha información desde su primer cierre fiscal.*
>
> *El proponente que tenga o haya tenido inscrita en la cámara de comercio la información de la capacidad financiera y organizacional de los años 2020 y/o 2021, no deberá presentar la información que repose en la respectiva cámara de comercio, la cual conservará la firmeza para efectos de su certificación.".*

Esto se debe a que la información vigente en la matrícula del RUP se mantiene en firme, hasta que sea sustituida con una renovación, actualización, o en caso de que el proponente no renueve su matrícula oportunamente. Para el año 2024, los proponentes podrán registrar sus solicitudes de renovación de matrícula en el RUP a más tardar el 5 de abril.

De conformidad con el Concepto C-480 de 2021, tratándose del trámite de renovación, se reitera lo expresado en el sentido de que la persona que presentó la información para renovar su registro a más tardar el quinto día de abril de cada año, cumpliendo el requisito del artículo 2.2.1.1.1.5.1 y pese a que la renovación no esté en firme, es decir, mientras esté en trámite el proceso de renovación, puede participar en los procedimientos de selección, debiéndose tener en cuenta la información «antigua». De esta manera, en el período comprendido entre el momento de la solicitud de renovación y el de su firmeza, se debe emplear la información del RUP que está en firme antes de iniciar el trámite de renovación, cuyos efectos no habrían cesado y se encontraría vigente. Incluso, en caso de que el RUP con la información «antigua» se haya presentado válidamente antes del cierre del proceso y con posterioridad a este quede en firme el nuevo RUP, para la evaluación de las propuestas se deberá utilizar la información del registro presentado inicialmente.

Para el caso descrito anteriormente en cuanto a la renovación y actualización, el proponente deberá remitir la constancia que acredite a la entidad haber presentado y radicado el trámite de renovación del RUP ante la Cámara de Comercio a más tardar el 5 día hábil del mes de abril a fin de poder verificar la vigencia del mismo.

Los proponentes que terminan su año contable en una fecha distinta al 31 de diciembre, deben actualizar la información financiera en la fecha correspondiente, sin perjuicio de la obligación de renovar el RUP de acuerdo con lo establecido en el artículo 2.2.1.1.1.5.1 del Decreto 1082 de 2015.

Para garantizar la participación de las personas extranjeras no inscritas en el Registro Único de Proponentes por no tener domicilio o sucursal en el país, deberán aportar la información para verificar

su capacidad financiera, presentando certificación firmada por el Representante Legal, acompañada de traducción al idioma español, con los valores re-expresados a la moneda funcional colombiana, a la tasa de cambio de la fecha de cierre de los estados financieros, avalados con la firma de un Contador Público con Tarjeta Profesional expedida por la Junta Central de Contadores de Colombia.

Para obtener los indicadores cuando el proponente sea un Consorcio, Unión Temporal u otra forma de asociación, se aplicará el procedimiento de Suma de los componentes de los indicadores contenido en el Manual para determinar y verificar los requisitos habilitantes en los Procesos de Contratación de Colombia Compra Eficiente.

Todos los cálculos aritméticos que se realicen para la determinación de los indicadores de proponentes plurales se aproximarán por exceso o por defecto a la centésima del valor, así: cuando la milésima sea igual o superior a 5, se aproximará por exceso, y cuando sea inferior a 5 se aproximará por defecto.
El Departamento de Antioquia si lo considera necesario, se reserva la facultad de solicitar información adicional, con el fin de verificar y/o aclarar los datos reportados en los certificados requeridos.

Los indicadores a verificar serán los siguientes:

Índice de Liquidez: Activo corriente sobre pasivo corriente: Mayor o igual a 1,01
Nivel de Endeudamiento: Pasivo total sobre activo total: Menor o igual al 0,75
Razón de Cobertura de Intereses: Utilidad operacional sobre gasto intereses: Mayor o igual a 0,56.

Cuando el proponente no tenga en su contabilidad, la cuenta de pasivo corriente (es decir que su valor sea cero), cuyo resultado daría indeterminado, se podrá habilitar en el requisito, siempre que el activo corriente sea positivo

Para el cálculo del indicador de cobertura de intereses, cuando el proponente no tenga en su contabilidad, la cuenta de gasto de intereses, (es decir que su valor sea cero), cuyo resultado daría indeterminado, se podrá habilitar en el requisito, siempre que la utilidad operacional sea positiva.

Para la acreditación del requisito de capital de trabajo, se tomarán los valores del activo corriente y pasivo corrientes contenidos en el RUP y la Entidad realizará el cálculo respectivo.

El Departamento de Antioquia, considera necesario evaluar los indicadores de capital de trabajo como indicador adicional para asegurar que los proponentes cuenten con los recursos económicos suficientes para iniciar la ejecución del contrato y la compra de los elementos necesarios para la ejecución.

Si el proponente es un consorcio, unión temporal o promesa de sociedad futura, su capital de trabajo corresponde a la sumatoria simple de los capitales de trabajo acreditados por cada uno de sus integrantes.

5.1.3 Requisitos de Capacidad Organizacional

Para verificar el cumplimiento se tomará la información que aparezca en el RUP según las mismas indicaciones dadas en el numeral anterior.

Rentabilidad del patrimonio:
Utilidad operacional dividida por el patrimonio. Mayor o igual que 0,08

Rentabilidad del activo:
Utilidad operacional dividida por el activo total: Mayor o igual que 0,02

5.2 Criterios de Evaluación

De conformidad con lo dispuesto en el numeral 3° del artículo 5° de la Ley 1150 de 2007, al tratarse de bienes de características técnicas uniformes, se tendrá como único criterio de evaluación el menor precio ofrecido, para lo cual se seguirá el procedimiento establecido en el artículo 2.2.1.2.1.2.2 y siguientes del Decreto Único Reglamentario 1082 de 2015. La propuesta económica más favorable será la que ofrezca el menor precio ofertado en la subasta, el cual está determinado por la sumatoria del valor total de lo requerido en el formato de oferta económica.

Factor precio: Por tratarse de una selección abreviada mediante subasta inversa el criterio de evaluación es el factor precio.

Nota: Sera causal de rechazo si la proponente oferta valores superiores para cada uno de los precios unitarios establecidos por la entidad y/o superior al presupuesto oficial.

6. EL ANALISIS DEL RIESGO Y LA FORMA DE MITIGARLO

Los riesgos pueden ser definidos como un evento que puede generar efectos adversos y de distinta magnitud en el logro de los objetivos del Proceso de Contratación o en la ejecución de un contrato.

Será previsible en la medida que el mismo sea identificable y cuantificable en condiciones normales. A continuación, en el siguiente cuadro se establecerá la tipificación y estimación del riesgo para el presente proceso:

Ver anexo: Matriz de riesgos.

7. LAS GARANTÍAS QUE LA ENTIDAD ESTATAL CONTEMPLA EXIGIR EN EL PROCESO DE CONTRATACIÓN

Buscando minimizar cualquier perjuicio que pudiera sufrir el Departamento de Antioquia derivado de las obligaciones surgidas en la ejecución del presente contrato, en la etapa de planeación del proceso se realizó un análisis del objeto, valor, obligaciones y de los riesgos previsibles contemplados en la matriz del contrato.

En virtud de lo anterior, se estima necesario la exigencia de garantías que aseguren el cumplimiento del contrato de conformidad con lo establecido en el Decreto Reglamentario 1082 de 2015: En el evento que la suficiencia de la garantía sea superior y/o supere el término de vigencia mínimo establecido en el mencionado decreto se deberá justificar

Descripción Amparo	Porcentaje	Vigencia

Garantía de Seriedad	10% del Presupuesto oficial	Desde la presentación de la oferta y hasta la aprobación de la garantía de cumplimiento del contrato.
Cumplimiento del Contrato	10% sobre el valor total del contrato	Por el término de duración del contrato y seis (06) meses más, con la nota de ampliar la vigencia hasta la liquidación del contrato.
Calidad del Servicio	10% sobre el valor del contrato	Por el término de duración del contrato y seis (06) meses más.

Tabla No.13 – Garantías que Aseguran Cumplimiento.

JUSTIFICACIÓN DE EXIGENCIA DE GARANTÍAS

Cumplimiento del contrato. De conformidad con el inciso 5° del artículo 7° de la Ley 1150 de 2007 y el artículo 2.2.1.2.3.1.1., 2.2.1.2.3.1.7., y 2.2.1.2.3.1.12. del Decreto 1082 de 2015, la exigencia de esta garantía, su valor y su plazo, se justifica en el amparo que cubre a la Entidad Estatal de los perjuicios derivados de: (a) el incumplimiento total o parcial del contrato, cuando el incumplimiento es imputable al contratista; (b) el cumplimiento tardío o defectuoso del contrato, cuando el incumplimiento es imputable al contratista; (c) los daños imputables al contratista; y (d) el pago del valor de las multas y de la cláusula penal pecuniaria.

Este amparo comprende además el pago del valor de las MULTAS Y DE LA CLÁUSULA PENAL PECUNIARIA que se hayan pactado en el contrato garantizado, lo anterior de acuerdo al artículo 2.2.1.2.3.1.12 del Decreto 1082 de 2015. En el presente caso se exige por el término del contrato hasta la liquidación del contrato, es decir, seis (06) meses con la anotación de hasta la liquidación del contrato, según lo establecido en la normatividad contractual. Igualmente se considera que se hace necesario solicitar un cubrimiento del 10 por ciento (10%) por cuanto la posibilidad de que se presente alguna falla en el cumplimiento del contrato es moderada y la afectación sería alta.

Calidad del servicio. Este amparo cubre a la Entidad Estatal por los perjuicios derivados de la deficiente calidad del servicio prestado. El amparo de calidad del servicio cubre a la entidad estatal contratante de los perjuicios imputables al contratista garantizado que surjan con posterioridad a la terminación del contrato y que se deriven de (i) la mala calidad o insuficiencia de los productos entregados con ocasión de un contrato de consultoría, o (ii) de la mala calidad del servicio prestado, teniendo en cuenta las condiciones pactadas en el contrato. Por una cuantía igual al 10 por ciento (10%) del valor total del contrato y tendrá una vigencia durante el plazo del contrato y seis (06) meses con la anotación de hasta la liquidación del contrato. Como quiera que estamos ante un servicio prestado por un tercero, es preciso que haya una buena calidad, significando ello que no es sólo el cumplimiento, sino que el servicio tenga una buena calidad, máxime cuando se trata de garantizar un servicio oportuno, basado en grandes estándares de calidad de presentación del servicio y calidad de los entregables para el desarrollo correcto del mismo.

El contratista se obliga al restablecimiento, reposición o ampliación de la garantía por su valor, cuando éste se haya visto reducido o agotado por razón de las reclamaciones efectuadas. En cualquier evento en que se aumente o adicione el valor del contrato o se prorrogue su término, **EL CONTRATISTA** deberá ampliar el valor de la garantía otorgada o ampliar su vigencia según el caso. El incumplimiento

de la obligación del **CONTRATISTA** de mantener la suficiencia de la garantía, facultará al **DEPARTAMENTO DE ANTIOQUIA** a declarar la caducidad del contrato.

8. LA INDICACIÓN DE SI EL PROCESO DE CONTRATACION ESTA COBIJADO POR UN ACUERDO COMERCIAL

Ver Anexo Acuerdos Comerciales.

9 CONVOCATORIAS LIMITADAS A MIPYME

De conformidad con el artículo 5 del Decreto 1860 del 24 de diciembre de 2022, el cual modificó el artículo 2.2.1.2.4.2.2 del Decreto 1082 de 2015, el cual señala:

> *"ARTÍCULO 2.2.1.2.4.2.2. Convocatorias limitadas a Mipyme. Las Entidades Estatales independientemente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos, deben limitar la convocatoria de los Procesos de Contratación con pluralidad de oferentes a las Mipyme colombianas con mínimo un (1) año de existencia, cuando concurran los siguientes requisitos:*
>
> *1. El valor del Proceso de Contratación sea menor a ciento veinticinco mil dólares de los Estados Unidos de América (US$125.000), liquidados con la tasa de cambio que para el efecto determina cada dos años el Ministerio de Comercio, Industria y Turismo.*
>
> *2. Se hayan recibido solicitudes de por lo menos dos (2) Mipyme colombianas para limitar la convocatoria a Mipyme colombianas. Las Entidades Estatales independientemente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos, deben recibir estas solicitudes por lo menos un (1) día hábil antes de la expedición del acto administrativo de apertura, o el que haga sus veces de acuerdo con la normativa aplicable a cada Proceso de Contratación (…)"*

Por tratarse el presente proceso de una selección abreviada mediante subasta inversa electrónica, cuyo valor es inferior a 125.000 dólares, se determina que el mismo **NO** sería objeto de limitación a MIPYMES en los términos del Artículo 5 del Decreto 1860 de 2021, que modificó el Artículo 2.2.1.2.4.2.2. del Decreto de 1082 de 2015.

10. RESOLUCIÓN POR MEDIO DE LA CUAL SE CONFORMÓ EL COMITÉ ASESOR Y EVALUADOR DEL PROCESO CONTRACTUAL

Mediante Resolución No **2026060053001** del 17 de 03 de 2026 se designó el Comité Asesor y Evaluador y sus integrantes, así

Rol Jurídico: **JENNY MARCELA OTÁLORA GÓMEZ**, Profesional Universitario, Secretaría de Talento Humano y Servicios Administrativos

Rol Logístico: **PEDRO SAIR BARBOSA CORDOBA**, Profesional Universitario, Secretaría de Talento Humano y Servicios Administrativos

Rol Técnico: **MARÍA CRISTINA GIRALDO OSPINA,** Directora Tecnología e Información – Secretaría de Talento Humano y Servicios Administrativos
JHON FREDY BORJA CARVAJAL – Profesional Universitario - Dirección de Tecnología e Información.

11 TIPO DE SUPERVISIÓN Y/O INTERVENTORIA

La supervisión será en modalidad interna y de tipo C. Se realizará una supervisión interna, toda vez que la solución a contratar es de conocimiento técnico del personal de la Dirección de Tecnología e Información, estando dentro del campo del conocimiento y experticia propia del personal de la Gobernación de Antioquia.

12. **ANEXOS**

- Anexo estudios Previos
- CDP´s
- Resolución de designación del Comité Asesor y Evaluador.
- BPID´s (Certificado de Banco de Proyectos).
- Propuestas
- Matriz de riegos
- presupuesto oficial
- Análisis del sector
- Acuerdos comerciales

PEDRO SAIR BARBOSA CORDOBA
Profesional Universitario
Dirección de Tecnología e Información
Rol Logístico

JHON FREDY BORJA CARVAJAL
Profesional Universitario
Dirección de Tecnología e Información
Rol Técnico

JENNY MARCELA OTALORA GOMEZ
Profesional Universitario
Dirección de Tecnología e Información
Rol Jurídico

MARIA CRISTINA GIRALDO OSPINA
Directora
Dirección de Tecnología e Información

Fecha de creación: Medellín, 23/04/2026

Fecha de Aprobación: Medellín, 24/04/2026