



ANÁLISIS ECONÓMICO DEL SECTOR

15 de septiembre de 2026

1 OBJETO DEL CONTRATO

"ADQUISICIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE PLATAFORMAS DE CIBERSEGURIDAD QUE PERMITAN CORRELACIONAR SOLUCIÓN PROTECCIÓN DE ENDPOINT Y SERVIDORES CON EDR Y XDR Y PROTECCIÓN DE CORREO PARA LA ALCALDÍA DE TOCANCIPÁ".

2. NECESIDAD

La Alcaldía Municipal de Tocancipá, tiene como misión "en el marco constitucional y legal como ente territorial y modelo de desarrollo, generar las condiciones necesarias para la oportuna prestación de los servicios básicos y la garantía de los derechos fundamentales, soportado en una institucionalidad efectiva y transparente en el manejo de los recursos y promotora de la construcción de una ciudad segura que propicie el mejoramiento de la calidad de vida de la comunidad Tocancipeña".

Teniendo en cuenta que el propósito fundamental de la Alcaldía Municipal de Tocancipá es garantizar la continua, eficiente y oportuna prestación de servicios, se requiere contar con las herramientas tecnológicas que permitan desempeñar sus actividades administrativas eficientemente; para ello debe realizar actividades de protección, modernización, mejora y optimización de su plataforma tecnológica informática, y por ende, se requiere la adquisición, configuración y puesta en funcionamiento de plataformas de ciberseguridad que permitan correlacionar solución protección de ENDPOINT y servidores con EDR y XDR y protección de los correos electrónicos, en procura de un óptimo desarrollo de los sistemas de información y bases de datos en cada una de las áreas de la Entidad; en este sentido para el desarrollo de sus funciones administrativas, la Alcaldía del Municipio de Tocancipá cuenta con una infraestructura tecnológica compuesta por:

- Equipos de Cómputo Finales (Endpoints): Un parque informático aproximado de 500 equipos entre estaciones de trabajo (All-in-One, Workstations) y computadores portátiles, operados por los servidores públicos y contratistas en las distintas dependencias institucionales, los cuales ejecutan sistemas operativos Windows y macOS.
- Servidores e Infraestructura de Centro de Datos: Servidores físicos y virtualizados (bajo sistemas operativos Windows Server y distribuciones Linux) ubicados en el Data Center de la Sede Administrativa, Casa de Justicia y demás sedes de las dependencias, donde se alojan las bases de datos corporativas, sistemas de información financieros, tributarios y de gestión documental.
- Plataforma de Correo Electrónico Institucional: La entidad opera la solución de correo corporativo en la nube bajo la plataforma Microsoft 365, contando con un aproximado de 400 cuentas activas de correo institucional por donde circula información oficial y sensible.

Con el fin de garantizar la continuidad de la función administrativa y la prestación ininterrumpida de los servicios públicos a cargo del Municipio de Tocancipá, se requiere asegurar la protección integral del parque informático y tecnológico de las diferentes dependencias. Esta contratación tiene como propósito prevenir incidentes de seguridad de la información, tales como la fuga no autorizada de datos (DLP), infecciones por código malicioso o ciberataques (incluyendo Ransomware), garantizando la integridad, disponibilidad y confidencialidad de la información pública frente a amenazas informáticas que puedan comprometer el desempeño eficiente, oportuno y coordinado de las funciones institucionales.



Por lo anterior, la entidad requiere adquirir el licenciamiento de uso teniendo en cuenta que "El software se rige por licencias de utilización", es decir, en ningún momento un usuario compra un programa o se convierte en propietario de él, tan sólo adquiere el derecho de uso, incluso así haya pagado por él. Las condiciones bajo las cuales se permite el uso del software, o sea las licencias, son contratos suscritos entre los productores de software y los usuarios, los cuales protegen el software y hardware de los equipos de cómputo y servidores existentes, esto permitirá garantizar la seguridad de la información y evitar los incidentes y ataques informáticos que se están presentando en la infraestructura tecnológica de la Entidad.

La entidad requiere adquirir productos reconocidos en el mercado y que den fe de la protección amplia y suficiente en la protección de la información. Por ende, y como lo ha manifestado el Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, Subsección C, en Sentencia de fecha 14 de septiembre de 2011, Radicación 40251, la necesidad de exigir determinadas condiciones y especificaciones técnicas puntuales de los productos queda librada a la razonabilidad, discrecionalidad, ponderación y apreciación técnica de la entidad contratante, basándose en sus necesidades de seguridad.

En este sentido todas las soluciones brindadas para protección de correo y ciberseguridad para servidores (incluyendo Windows 2012 R2) y equipos de cómputo deben ser gestionadas en una sola consola iCloud en donde todas las soluciones generen telemetría, y en los reportes se evidencie una correlación de eventos de cada solución.

La Administración Municipal en cumplimiento al Plan de Desarrollo Municipal "TOCANCIPÁ SEGURA, EXPERIENCIA CON VISIÓN SOCIAL 2024-2027" "RECUPEREMOS EL PROGRESO", tiene contemplado dentro de sus proyectos el **Fortalecimiento a la gestión y dirección de la administración pública territorial del municipio de Tocancipá**, para recuperar la confianza ciudadana como única fuente de legitimidad gubernamental, a través del ejercicio de un gobierno transparente efectivo, eficaz y eficiente, determinando como meta de producto número 237 Mantener el 100% activos y en funcionamiento los servicios y medios tecnológicos en el cuatrienio, para contar así con Sistemas de Información eficientes y brindando confiabilidad en la información, la cual es responsabilidad del área de sistemas, quienes se encargan de hacer seguimiento al mantenimiento y a contribuir en el diseño, implementación de los sistemas de información de la Entidad.

La Secretaría Administrativa, a través de la Oficina de Sistemas, debe apoyar la contratación de las plataforma tecnológicas y servicios informáticos que requiere la entidad para el cumplimiento de sus funciones misionales y de apoyo, para lo cual debe garantizar la disponibilidad permanente de los servicios de Tecnología de Información (TI) para el acceso a las aplicaciones misionales y de apoyo, para el proceso de la gestión documental, desde la producción hasta la disposición final en todas las dependencias.

Por lo anteriormente expuesto y con el objetivo de cumplir y avanzar en las metas del Plan de Desarrollo, es necesario adquirir plataformas de ciberseguridad que permitan correlacionar solución protección de ENDPOINT Y SERVIDORES CON EDR Y XDR y protección de correo para la Alcaldía de Tocancipá, que incluya la configuración y puesta en funcionamiento de las mismas.

Teniendo en cuenta las características específicas de la necesidad, se definen más adelante en las especificaciones técnicas del objeto a contratar, los aspectos técnicos para la estructuración del proceso, entre los cuales están:

- Seguridad de la información y seguridad informática
- Administración, soporte y gestión de la plataforma tecnológica
- Mesa de servicio



- Acuerdo de niveles de servicio
- Equipo de especialistas

3. ASPECTOS GENERALES DEL MERCADO

3.1. CARACTERIZACIÓN DEL OBJETO A CONTRATAR

La modelización macroeconómica tradicional establece una partición funcional del mercado en tres sectores. Esta clasificación demarca los flujos de la cadena de suministro y el intercambio comercial en tres dominios sectoriales distintos: el Sector Primario (extracción y producción de materias primas), el Sector Secundario (transformación industrial de dichas materias) y el Sector Terciario (provisión de servicios, distribución y gestión). Esta segmentación analítica facilita la comprensión sistémica de las interdependencias productivas y la dinámica de valor agregado a lo largo del ciclo económico.

Sector Primario: este sector hace referencia a las actividades que se relacionan con la explotación de los recursos naturales pero que dicha actividad realiza la extracción mas no genera ningún tipo de transformación, tales como son: la ganadería, la pesca, la minería, la producción energética, la agricultura. El resultado de productos de este sector, por lo general pasa al sector secundario para su posterior transformación en un proceso industrial.

Sector Secundario: este sector se encuentra directamente relacionado con aquellas actividades las cuales toman las materias primas y realizan algún tipo de transformación de estas actividades normalmente se genera un producto terminado o semiterminado. Se pueden entonces encontrar empresas como: industria, construcción, energía.

Sector Terciario: El sector de servicios es el sector terciario de la economía encargado de las actividades de comercio, servicio y transporte; a diferencia de los sectores primario y secundario, el sector terciario no se encarga de producir sino de ofrecer y distribuir productos. Por este motivo, se le conoce como el sector del servicio de los materiales ya que no es transformadora o productora de materiales. En este sector se pueden encontrar servicios, tales como; comercio, bancos, educación, salud, comunicaciones, el transporte, las finanzas, el hotelaría, el turismo, el ocio, el espectáculo, entre otros.

Con lo anterior, el objeto contractual se encuentra enmarcado dentro del sector terciario conocido también como sector de servicios; en este orden de ideas a continuación, se presenta una breve descripción de cada una de las áreas de negocio identificadas en el sector:

Desarrollo de Aplicaciones alojadas en la WEB: Es un modelo de negocio de interés progresivo de la industria del Software que trata del suministro de herramientas que los usuarios pueden utilizar accediendo a un servidor web a través de Internet o de una intranet, mediante un navegador. Las empresas proveedoras de software (Proveedores de Aplicaciones de Servicios – ASP por sus siglas en inglés) promueven su acceso vía Internet, permitiendo al usuario pagar una cuota periódica para usar la aplicación, sin necesidad de instalarla en el ordenador del usuario.

Computación en la Nube: es un modelo de distribución de software donde el software y los datos que maneja se alojan en servidores de la compañía de -TI y se accede con un navegador web o un cliente fino especializado, a través de internet. La empresa provee el servicio de mantenimiento, operación diaria, y soporte del software usado por el cliente. Regularmente el software puede ser consultado en cualquier computador, esté presente en la empresa o no. Se deduce que la información, el procesamiento, los insumos y los resultados de la lógica de negocio del software están hospedados en la compañía.



Seguridad informática: los riesgos de la infraestructura computacional y de la información de las organizaciones les exigen controlar impactos potenciales respecto a incidentes que deben neutralizar. Las políticas de seguridad abren oportunidades de negocio a las empresas de software que ofrecen un portafolio de servicios de expertos en gestión y monitoreo de seguridad, que utilizan herramientas avanzadas de protección de las aplicaciones, soluciones especializadas, investigación y soluciones de productos y personal con conocimientos de los entornos de las amenazas.

Tecnologías transversales: se conocen también como tecnologías de propósito general que corresponden a sectores intensivos en conocimiento con múltiples campos de aplicación. Se caracterizan por ser aplicables en varios sectores industriales, mejoran en el tiempo y permiten la creación de nuevas tecnologías. Son importantes porque producen aumentos en la productividad y el crecimiento económico.

Sistemas Personales: incluyen servicios relacionados con los sistemas de identificación biométrica de identificación, mediante los cuales se captura, procesa y almacena información relacionada con rasgos físicos de las personas, como son las huellas dactilares, el ADN, la forma o silueta de la mano, los patrones de la retina o el iris y los aspectos faciales, para poder establecer o autenticar la identidad.

Planeación de Sistemas Orientados a Servicios: mediante la Arquitectura Orientada a Servicios (SOA) los procesos del negocio se ensamblan como un servicio integrado, en una sola aplicación, una sola pantalla y un solo inicio de sesión. El SOA facilita la evolución a modelos de negocios basados en la tercerización, permite la integración de tecnologías disímiles, mejora la visibilidad de la información a toda la organización y en general optimiza los procesos del negocio. La planificación, las herramientas y la infraestructura de la arquitectura del SOA requieren estándares y productos enfocados como un Enterprise Service Bus, un registro de servicios, un motor de procesos del negocio y un lenguaje que puede ser Java CAPS.

Testing de software: El software Testing es la comparación del comportamiento actual del software con el comportamiento deseado de acuerdo con especificaciones y requerimientos identificados. Para conocer el producto se estudia la documentación técnica, algunos procedimientos de prueba, casos de prueba y capacitación especial que las compañías proveen.

Mejora de Procesos: La oferta de estos servicios se fundamenta en los principios de la Calidad Total. Los procesos son secuencias repetitivas de actividades que desarrollan cotidianamente las personas, los grupos o las dependencias de una organización y que le permiten satisfacer las expectativas de los clientes y seguir en el mercado. Ante las quejas de los clientes, dificultades con los proveedores, problemas de costos, uso inadecuado de recursos o cambios del entorno que deban ser atendidos ineludiblemente, los procesos deben surtir acciones de mejora que optimicen la productividad con resultados de calidad total y riesgo mínimo. En este campo surgen las oportunidades de negocio para las empresas de SW&TI con el propósito de gestionar técnicas, herramientas y aplicaciones que generan la mejora del ciclo de planificar, ejecutar, comprobar y ejecutar, para que las organizaciones logren su nivel máximo de capacidad. Adicionalmente se promueven modelos para mejorar los procesos y fomentar la competitividad de la pequeña y mediana industria del software.

Integración de Redes: las empresas que ofrecen servicios de integración de redes están en condiciones de interconectar y ofrecer soporte a los equipos de cómputo con el fin de compartir los recursos tecnológicos de una organización entre sus empleados a través de redes para que los usuarios puedan utilizar los recursos disponibles como impresoras, bases de datos, archivos, internet. Las arquitecturas de cliente/servidor mantienen centralizada la seguridad y se usan para el manejo de grandes cantidades de datos. Los servidores manejan la seguridad de acceso a usuarios, recursos de hardware y software de la red, mientras que los clientes manejan las aplicaciones en sus PC locales¹⁰. Los servicios para redes de telecomunicaciones ofrecen consultoría, diseño, implementación,



administración, operación y soporte. Actualización, renovación, expansión y consolidación; integración de múltiples marcas; punto único de contacto; configuración, implementación y pruebas para ruteadores, switches y telefonía IP.

Integración de Sistemas: El uso de varias plataformas de Software en las organizaciones dificulta su gestión por las exigencias de intervención manual excesiva a la hora de sincronizar información en tiempos necesarios, por lo que los profesionales de las empresas TI son llamados a desarrollar actividades de integración de herramientas de automatización de plataformas como Unix, Linux, Windows, Mainframe, Oracle, SAP. Los servicios SW&TI reducen los errores de la intervención manual, mejoran el tiempo de finalización de trabajos y mejoran el control de las actividades de proceso por lotes.

Outsourcing de infraestructura: Las soluciones de alquiler de equipos ofrecen un amplio y flexible portafolio de productos y servicios a la medida mediante el alquiler de computadores, impresoras y dispositivos de red, a empresas, en las categorías de ofimática, especializados y móviles, así como asesoría, acompañamiento y servicio técnico. Por su parte, las soluciones cloud computing garantizan la infraestructura tecnológica de pago por uso según demanda, en centros de datos, donde se dispone de potentes servidores para alojar las aplicaciones de los clientes con medidas de seguridad que protegen permanentemente la información y mantienen disponibles las aplicaciones en todo momento. En esta área se dispone de los modelos SaaS, integraciones multiplataforma, conocimiento de los procesos de Back Office y de integradores de soluciones. El desarrollo del software en este modelo de negocio debe ser 100% web y disponer para su operación de una conexión a internet de banda ancha.

Ecosistema de Ciberseguridad Moderna (SOCaaS & Zero Trust): El ecosistema se basa en la transición de una seguridad perimetral tradicional hacia una arquitectura Zero Trust (ZTA), fundamentada en el principio de "nunca confiar, siempre verificar". Este ecosistema integra una identidad centralizada con autenticación multifactorial (MFA) y microsegmentación de red, complementada por un servicio de SOC-as-a-Service (SOCaaS) para el monitoreo continuo, detección (SIEM) y gestión de vulnerabilidades. Asimismo, incorpora soluciones de Endpoint Detection and Response (EDR) mediante agentes inteligentes en estaciones de trabajo (All-in-One y portátiles), garantizando el aislamiento preventivo y la respuesta inmediata ante incidentes críticos como ataques de Ransomware.

Servicios de migración y calidad de datos: estos servicios abarcan un portafolio de soluciones en áreas de identificación de riesgos relacionados con datos, desarrollo de planes de corrección y planes de mejora, controles de migración de datos, capacitación, cumplimiento de leyes y regulaciones. Para la correcta migración de datos, en el marco de la implementación de un sistema, se asiste al cliente con metodologías y herramientas que permita disponer de los datos con un nivel de calidad aceptable en el nuevo sistema. En el proceso de migración se controla la integridad de los datos en las etapas de extracción, transformación y carga para garantizar su calidad. La aprobación final de la migración de datos se realiza mediante la generación de reportes y del resultado de los controles para obtener la aprobación final del cliente de los resultados de la migración.

Soporte y mantenimiento de software: servicios de soporte de arquitectura y desarrollo para la restauración de operaciones dentro de los servidores de aplicaciones Web. Soporte técnico de la configuración y operación de los productos, servicios de configuración de red, identificación de fallas en los aplicativos, apoyo para superar contratiempos en la instalación de software, optimización de las aplicaciones en sus sitios de producción, mantenimiento de las bases de datos, instalación de parches y resolución de incidentes.



Capacitación y entrenamiento: las necesidades de capacitación técnica especializada en el área de tecnología generan múltiples oportunidades a las empresas SW&TI de contribuir en la optimización de los procesos TI de las empresas para los diferentes niveles jerárquicos, a través de centros de entrenamiento y capacitación con infraestructuras y materiales adecuados como ciber centros, salas de proyección, simulación, ejercicios y prácticas que se adelantan mediante módulos de duración breve.

Es indispensable aclarar que los dos primeros sectores producen bienes tangibles, por lo cual son considerados como sectores productivos. El tercer sector se considera no productivo, puesto que no produce bienes tangibles, pero, sin embargo, contribuyen a la formación del ingreso nacional y del producto nacional.

En virtud de la naturaleza tecnológica requerida por el Municipio de Tocancipá, la ejecución de las actividades dentro de este sector económico deberá estar en concordancia con los lineamientos de confianza y seguridad digital del Estado Colombiano. Para tal efecto, el futuro contratista deberá garantizar el cumplimiento de la Guía de Ciberseguridad expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC (G.CIB.01), integrando los controles necesarios para la mitigación de riesgos informáticos. Asimismo, en observancia de los estándares de publicidad, acceso a la información y transparencia de la gestión pública, el objeto contractual se desarrollará bajo los parámetros de la Resolución 1519 de 2020 expedida por el MINTIC, asegurando que la información y servicios digitales cumplan con los requisitos de accesibilidad, seguridad y estándares de información definidos por el MINTIC.

Por lo anterior, se ratifica que el Sector Económico al que pertenece el servicio requerido por el Municipio es el Sector Terciario o de Servicios.

3.2. PRODUCTOS INCLUIDOS DENTRO DEL SECTOR

Los productos de interés en el marco del proceso en trámite que incluye el sector en la actividad económica CIU División 62. Desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas), consultoría informática y actividades relacionadas), son las siguientes:

Plataformas de Protección de Endpoint (EPP) y Detección y Respuesta (EDR/XDR): Es un tipo de programa informático (software) que se diseña, escribe y se somete a pruebas para proteger sistemas, lo que se alinea directamente con las actividades de Desarrollo de sistemas informáticos y suministro de asistencia en relación con programas informáticos.

Sistemas de Seguridad de Correo Electrónico (Email Security): Son aplicaciones de software o servicios en la nube que ofrecen diversas capas de protección (antispam, antiphishing, antimalware) para la comunicación por correo. Su desarrollo y personalización para su implementación en sistemas de clientes caen bajo la División 62 (análisis, diseño, programación).

Servicios de Detección y Respuesta a Amenazas (MDR, XDR): Servicios especializados de administración e integración de instalaciones informáticas, orientados a la gestión técnica, monitoreo continuo y soporte operativo de soluciones de seguridad (incluyendo ciberseguridad avanzada y protección de canales de correo electrónico) para las plataformas de la entidad.

Servicios de Arquitectura y Planeación de Seguridad: Actividades de análisis funcional, diseño de ingeniería y estructuración técnica de la infraestructura de ciberseguridad, orientadas al dimensionamiento, configuración e implementación de soluciones para la protección de endpoints,



redes y correo electrónico. Estas labores se enmarcan directamente en las actividades de desarrollo, análisis y planificación de sistemas informáticos de la división.

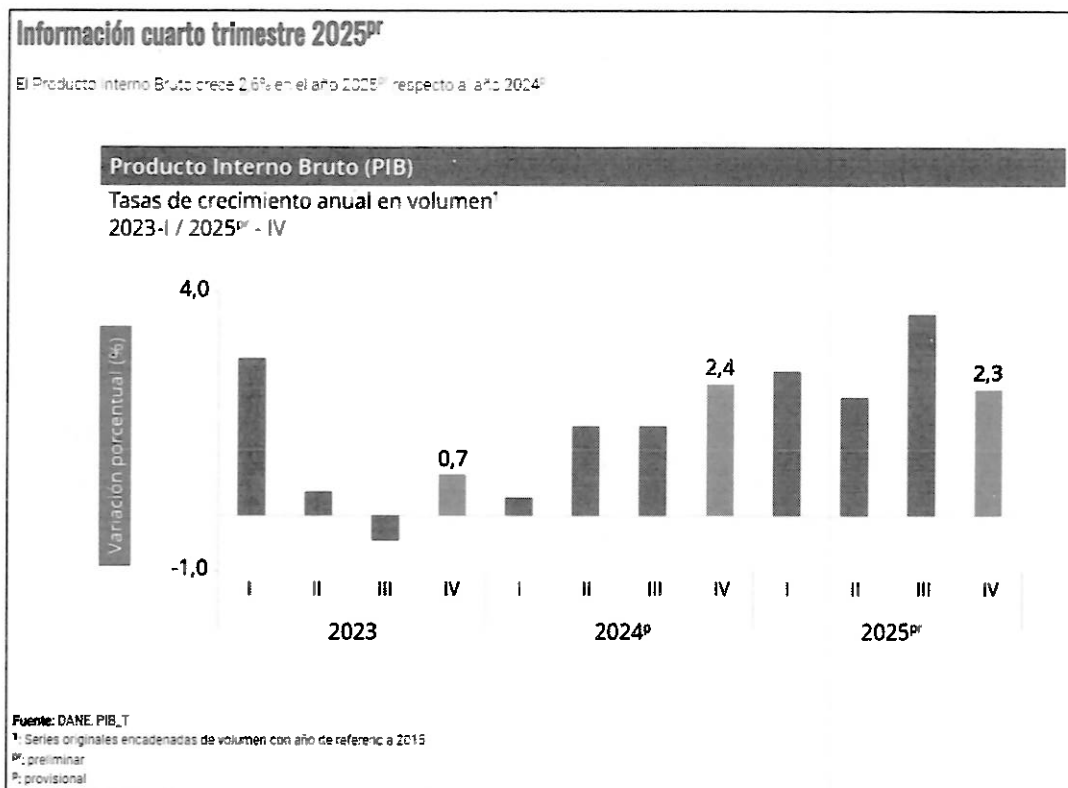
Plataformas de Seguridad Unificada Soluciones que integran múltiples funciones de seguridad (como ciberseguridad de endpoint y protección de correo) gestionadas a través de una consola. Su desarrollo y soporte son actividades centrales de la CIU 62.

3.3. AGENTES QUE INTERVIENEN EN EL SECTOR

- Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.
- Ministerio de Ciencia Tecnología e Innovación.
- Ministerio de Comercio, Industria y Turismo.
- Alcaldía municipal
- Empresas de desarrollo de software
- Empresas consultoras de ciberseguridad
- Agentes de soporte y regulación de TICs
- ColCERT / CSIRT Gobierno: (Coordinadores de respuesta a incidentes a nivel nacional).
- Instituciones educativas y centros de investigación de Software

3.4. CRECIMIENTO DE LA ECONOMÍA NACIONAL

Según los datos consolidados del DANE para el cierre de 2025, la economía colombiana registró un crecimiento anual del 0,6% en el Producto Interno Bruto (PIB). Las actividades que más contribuyeron a esta dinámica fueron: Agricultura, ganadería, caza, silvicultura y pesca, con un crecimiento del 3,9%; y Administración pública, educación y salud, con un 3,9%.



Durante el cuarto trimestre de 2025 (IV-2025), el PIB presentó un crecimiento anual del 0,3%. Las actividades con mayor impacto positivo en el valor agregado durante este periodo fueron: Agricultura (6,0%) y Administración pública (3,8%). Por el contrario, el sector de Comercio, transporte y servicios



de comida, que en periodos anteriores era motor de crecimiento, presentó una variación del -2,3%, reflejando un cambio en el gasto de los hogares.

Tabla 1. Valor agregado por actividad económica
Tasas de crecimiento en volumen¹
Cuarto trimestre 2025^{PR}

Actividad económica	Tasas de crecimiento (%)		
	Serie original		Serie ajustada por efecto estacional y calendario
	Año total	Anual	Trimestral
	2025 ^{PR} / 2024 ^P	2025 ^{PR} -IV / 2024 ^P -IV	2025 ^{PR} -IV / 2025 ^{PR} -III
Agricultura, ganadería, caza, silvicultura y pesca	3.1	-0.4	-2.6
Explotación de minas y canteras	-6.2	-2.9	1.2
Industrias manufactureras	1.9	1.0	-1.6
Suministro de electricidad, gas, vapor y aire acondicionado ²	1.1	2.9	0.8
Construcción	-2.8	-2.6	-1.5
Comercio al por mayor y al por menor ³	4.6	3.4	1.6
Información y comunicaciones	1.0	-1.2	-2.0
Actividades financieras y de seguros	2.8	0.7	-2.4
Actividades inmobiliarias	2.0	1.9	0.4
Actividades profesionales, científicas y técnicas ⁴	1.3	1.5	0.4
Administración pública, defensa, educación y salud ⁵	4.5	4.8	0.2
Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios ⁶	9.9	11.5	4.6
Valor agregado bruto	2.7	2.3	-0.1
Impuestos menos subvenciones sobre los productos	2.5	2.5	0.6
Producto Interno Bruto	2.6	2.3	0.1

Fuente: DANE P.B.T

^{PR} preliminar

^P provisional

Serie encadenadas de volumen con año de referencia 2015

² Suministro de electricidad, gas, vapor y aire acondicionado; Distribución de agua; evacuación y tratamiento de aguas residuales; gestión de desechos y actividades de saneamiento ambiental

³ Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida

⁴ Actividades profesionales, científicas y técnicas; Actividades de servicios administrativos y de apoyo

⁵ Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales

⁶ Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios; Actividades de los hogares individuales; actividades de empleadores; actividades no diferenciadas de los hogares individuales como productores de bienes y servicios

Información y comunicaciones

Para el cierre de 2025, el valor agregado del sector de Información y Comunicaciones registró un crecimiento anual del 1,1%. En el análisis trimestral (IV-2025), el sector reportó una variación anual del 0,1%. Este dato es fundamental para la Alcaldía de Tocancipá, pues confirma que el sector tecnológico, a pesar de la coyuntura, no ha entrado en terreno contractivo, permitiendo la continuidad de proyectos de transformación digital.



Tabla 8. Información y comunicaciones
Tasas de crecimiento en volumen¹
Cuarto trimestre 2025^{pc}

Actividad económica	Tasas de crecimiento (%)		
	Serie original		Serie ajustada por efecto estacional y calendario
	Año total	Anual	Trimestral
	2025 ^{pc} / 2024 ^p	2025 ^{pc} - IV / 2024 ^p - IV	2025 ^{pc} - IV / 2025 ^{pc} - III
Información y comunicaciones	1,0	-1,2	-2,0

Fuente: DANE PIB_T

^p preliminar

^{pc} provisional

Series encadenadas de volumen con año de referencia 2015.

Industria Manufacturera

La industria manufacturera presentó una variación anual del -3,5% al cierre de 2025. Específicamente, el segmento que agrupa la fabricación de productos informáticos, electrónicos y ópticos, junto con la instalación y mantenimiento especializado, reportó una caída del 5,2% en su producción real. Esto sugiere una estabilización en los precios de oferta ante la baja demanda industrial, siendo un momento óptimo para la adquisición pública de licencias y soporte técnico.

3.5. CRECIMIENTO DE LA ECONOMÍA COLOMBIANA

Al cierre de la vigencia 2025, la economía colombiana registró un crecimiento consolidado del 1.8% al 2.0% (según datos preliminares del DANE y proyecciones del Banco de la República), superando la meta inicial. Durante el cuarto trimestre de 2025, el desempeño se vio impulsado por la estabilización de las tasas de interés, lo que dinamizó la inversión en bienes de capital y tecnología.

Específicamente, el sector de Información y Comunicaciones presentó una dinámica favorable, destacando los siguientes puntos:

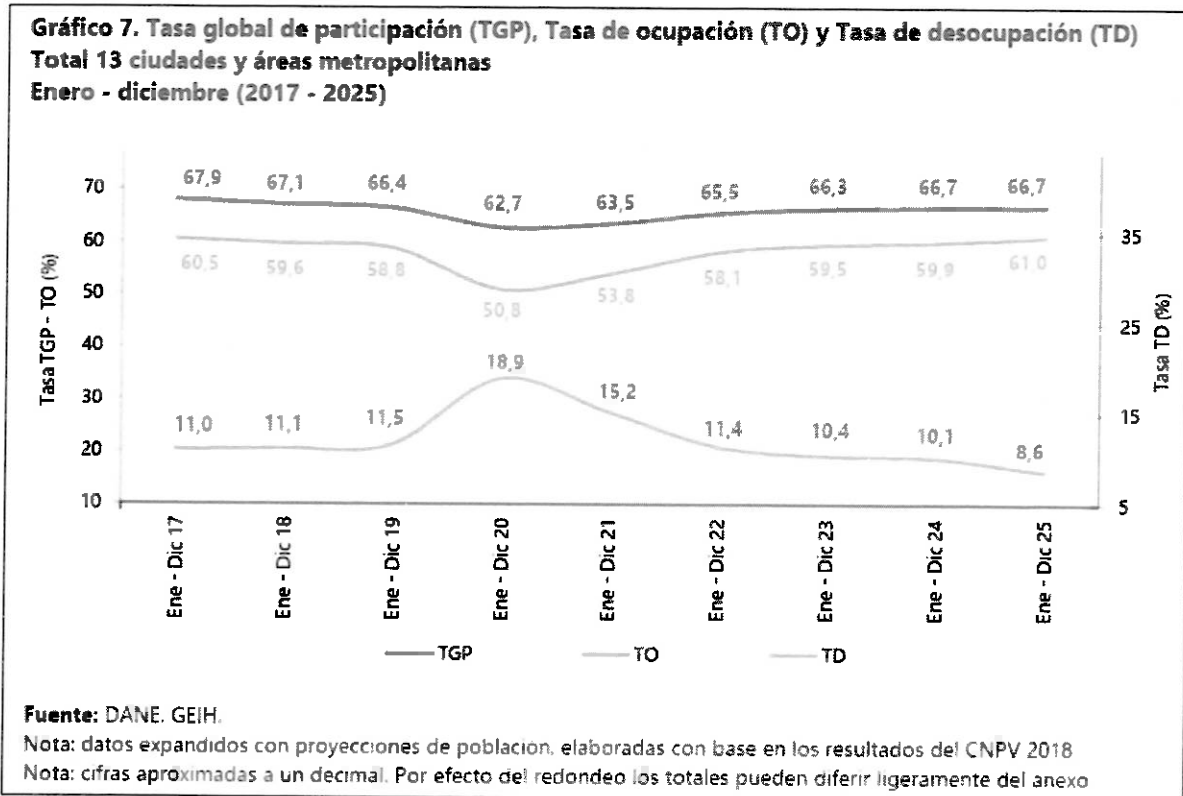
- **Desempeño Sectorial:** Las actividades de información y comunicaciones crecieron un 1.4% durante el último trimestre de 2025, impulsadas por la renovación de infraestructuras críticas y la adopción de servicios en la nube.
- **Manufactura y Tecnología:** Aunque el sector manufacturero presentó variaciones negativas durante gran parte del año, el subsector de fabricación de productos informáticos y electrónicos mostró una recuperación hacia el cierre de 2025, con una variación positiva del 1.1%, facilitando la disponibilidad de hardware especializado para ciberseguridad.
- **Contexto de Ciberseguridad:** La demanda por soluciones EDR y XDR ha crecido exponencialmente debido al aumento de ataques de ransomware en el sector público, convirtiendo la "Transformación Digital Segura" en una prioridad de gasto estatal.
- **Inflación y TRM:** Con una inflación anual que cerró 2025 cerca del 5.5% - 6.0%, los costos de licenciamiento internacional (tasados en USD) han tenido una presión al alza, lo que justifica



la necesidad de una contratación que garantice estabilidad de precios mediante el modelo de prestación de servicios.

3.6. MERCADO LABORAL

Para el cuarto trimestre de 2025 (octubre-diciembre), la tasa de desocupación del total nacional se situó en el 9.1%, lo que representó una ligera variación respecto al cierre del año anterior, reflejando una resiliencia en el sector de servicios y tecnología. La Tasa Global de Participación (TGP) para el cierre de la vigencia 2025 se ubicó en el 64.2%, mientras que la Tasa de Ocupación (TO) alcanzó el 58.4%.



Estas cifras demuestran una recuperación consolidada en los centros poblados y cabeceras municipales, donde la demanda de perfiles técnicos especializados en Tecnologías de la Información y Ciberseguridad ha mantenido una tendencia al alza, impactando los costos de implementación y soporte técnico para soluciones tipo EDR/XDR.

3.7. ASPECTOS COMERCIALES EN EL PROCESO DE CONTRATACIÓN

Se puede hablar entonces de dos formas de vender software: usar un software desarrollado a medida del proceso a implementar o usar un software comercial que ya haga las funciones necesarias, en este sentido se puede hablar de dos formas de contratación del software; en el mercado de ciberseguridad de alta gama (EDR/XDR), la comercialización se rige principalmente por el modelo de Suscripción de Software como Servicio (SaaS).

La oferta identifica que los grandes fabricantes (Tier 1) operan bajo esquemas de Canal Indirecto Especializado, garantizando soporte local y transferencia de conocimiento. Las modalidades identificadas son:

- Canal Indirecto: Los fabricantes operan a través de mayoristas (Wholesalers) y socios de negocios (Partners/Resellers). En Colombia, estos socios deben estar certificados bajo



categorías (Gold, Platinum, etc.) para garantizar la idoneidad técnica. Este modelo permite a la Alcaldía contar con soporte preventivo y correctivo de primer nivel en territorio nacional.

- **Acuerdos Marco de Precios (Tienda Virtual del Estado):** Los instrumentos agregados de demanda de software vigentes en la TVEC (como Software III o Gobierno Nube) están estructurados para licenciamiento ofimático, infraestructura como servicio (IaaS/PaaS) o software general de productividad. Ninguno incluye la solución unificada de ciberseguridad requerida, la cual exige de manera integral y correlacionada: agentes inteligentes de prevención y respuesta en tiempo real (Endpoint Detection and Response - EDR y Extended Detection and Response - XDR), visibilidad de amenazas multinivel (endpoints, servidores y correo electrónico), consola de administración unificada SaaS, respuesta automatizada ante incidentes de ransomware y la integración con servicios de configuración, puesta en funcionamiento y transferencia de conocimiento.
- **Modelos de Licenciamiento:** Se observa una tendencia al licenciamiento "Per User" o "Per Endpoint" con facturación anual. El mercado ya no ofrece licencias "perpetuas" para soluciones de seguridad en la nube (Cloud Native), lo que obliga a la entidad a proyectar el gasto en el rubro de inversión para servicios recurrentes.

EL SECTOR EN LA ECONOMÍA COLOMBIANA

Para caracterizar el tejido empresarial de software y servicios de ciberseguridad en Colombia a 2025, se toman como referencia los datos de Fedesoft y el Observatorio TI:

- **Industria en Crecimiento:** El sector TI representa aproximadamente el 2.9% del PIB nacional, con un ecosistema de más de 12,000 empresas activas.
- **Especialización en Ciberseguridad:** El sector presenta una alta especialización en SOC (Security Operations Center) y servicios gestionados, impulsado por el Documento CONPES 3995 de confianza y seguridad digital.
- **El mercado de ciberseguridad (EDR/XDR) en Colombia es altamente competitivo,** con presencia directa de fabricantes globales y una red capilar de canales (Partners) certificados en niveles Gold/Platinum.
- **Orientación a la Nube:** La industria ha migrado de la venta de licencias perpetuas a modelos SaaS (Software as a Service), lo que facilita el despliegue en entidades territoriales como la Alcaldía de Tocancipá.

La industria TI en Colombia ha evolucionado hacia un ecosistema altamente especializado en la integración de sistemas y la exportación de servicios, donde el desarrollo de software a la medida y la comercialización de soluciones empaquetadas bajo modelo SaaS (Software as a Service) dominan el mercado. Según el reporte Colombia Tech Report 2025, la industria ha logrado una mayor institucionalidad gracias al apoyo de programas de inversión extranjera, consolidando al país como un hub regional de ciberseguridad. A diferencia de años anteriores, se observa una transición desde el desarrollo netamente "a la medida" hacia la implementación de soluciones de ciberseguridad globalmente estandarizadas (EDR/XDR) que son adaptadas y soportadas por canales locales certificados. No obstante, el sector aún enfrenta retos en la sincronización de alianzas empresariales profundas, manteniendo una estructura donde las multinacionales lideran las exportaciones, mientras que el mercado interno es atendido por una red competitiva de integradores especializados en servicios de consultoría y soporte técnico de alto nivel.

CAPACIDADES EMPRESARIALES

En general, el sector en Colombia está compuesto por algunas empresas internacionales y un gran número de micro y pequeñas empresas nacionales. Para estas empresas nacionales no existe una



especialización definida ni una diferenciación con productos propios, así una empresa puede atender a varios sectores. La asesoría informática y el desarrollo de software a medida son las actividades más destacadas. El mapa empresarial del sector software y servicios en Colombia muestra un tejido empresarial atomizado, con predominancia de micro y pequeñas empresas, fuerte concentración en Bogotá y baja especialización. Las oportunidades de crecimiento están en la asociatividad, la internacionalización y la especialización en nichos de mercado, mientras que los principales retos son la profesionalización, la innovación y la articulación entre actores del sector.

Tipología Empresas	Segmentos	Productos Propios	Servicios
Unas 2.000 empresas (2010) 55% micro, 34% pequeña, 9% mediana, 2% grande. Cundinamarca: 62%, Antioquia: 12%, Pacífico: 8	Comercialización, parametrización y configuración de software importado; c	Sin alta especialización en productos y servicios empaquetados	Consultoría en informática, gestión de tecnologías de la información y redes.

De acuerdo con los resultados obtenidos en la Encuesta de Tecnologías de la Información y las Comunicaciones en Hogares (ENTIC Hogares), el porcentaje de personas de 5 y más años que usaron herramientas de Inteligencia Artificial a través de Internet, según sexo, Total nacional, Cabecera y Centros poblados y rural disperso.

4. ASPECTO TÉCNICO

En desarrollo y cumplimiento del objeto contractual, el contratista deberá cumplir con la **Ficha Técnica** de los servicios y productos requeridos, contenida en el **Anexo No. 1** y las siguientes especificaciones técnicas:

4.1. PROTECCIÓN ENDPOINT

Se requiere una solución integral y unificada anti-malware de seguridad para endpoints, que combine múltiples capacidades de protección en un solo agente y consola de administración, la solución debe tener una consola para definir políticas de seguridad para la prevención de amenazas, control de acceso y cumplimiento, protección de datos, despliegue y actualizaciones de agentes del Endpoint, La solución debe incluir una Gestión Basada en nube en modalidad SaaS que permite gestionar equipos, con su debido licenciamiento, puesta en funcionamiento, soporte de fábrica y garantía. La solución requerida debe proveer como mínimo:

La solución propuesta debe ser capaz de unificar la visibilidad, detección, investigación y respuesta a amenazas a través de múltiples vectores de ataque, incluyendo endpoints, servidores, redes, correo electrónico y entornos en la nube.

Consola de Administración

La consola de administración debe ser una solución SaaS (Software as a Service) que proporcione capacidades robustas de informes y monitoreo. Debe ofrecer filtros preconstruidos para facilitar la visualización y corrección de equipos que requieran atención. Es fundamental que la consola genere un registro de auditoría seguro, supervisando toda la actividad para asegurar el cumplimiento normativo, facilitar auditorías de seguridad, análisis forenses y solución de problemas. Además, la consola debe permitir la gestión centralizada de políticas de seguridad y la visualización unificada de eventos de seguridad a través de múltiples vectores de ataque, incluyendo endpoints, red, correo electrónico y entornos en la nube. Debe contar con capacidades de gestión de casos colaborativa y mapeo automático a frameworks de amenazas como MITRE ATT&CK para una mejor contextualización de las detecciones.



Protección de Endpoint

La solución debe ofrecer protección de ciberseguridad para estaciones de trabajo, laptops, dispositivos móviles y servidores, operando en tiempo real y mediante escaneos programados. Debe ser capaz de detectar, bloquear y limpiar virus, troyanos, gusanos, spyware, aplicaciones potencialmente no deseadas (PUA), adware y comportamientos sospechosos en sistemas operativos Windows, Linux y Mac. La detección de malware debe incluir análisis en pre-ejecución y comprobación de comportamiento malicioso para identificar amenazas desconocidas. Es crucial que la solución impida la reconfiguración, deshabilitación o desinstalación no autorizada de sus componentes, incluso por parte de administradores locales, mediante mecanismos de protección como contraseñas. Debe verificar todos los archivos accedidos en tiempo real, incluso durante el arranque del sistema, y realizar una limpieza automática de elementos maliciosos. La protección debe extenderse a funciones críticas en navegadores de Internet (Safe Browsing) y prevenir ataques de vulnerabilidades web a través de exploits. La solución debe aplicar análisis de comportamiento durante la ejecución para detectar desbordamientos de búfer y otras anomalías. Además, debe permitir la autorización de detecciones maliciosas y la exclusión de directorios y archivos específicos del escaneo.

Control de Dispositivos y Aplicaciones

La solución debe permitir el monitoreo y control de dispositivos extraíbles (USB, discos duros externos, CD/DVD, interfaces de red inalámbrica, módems, Bluetooth, infrarrojos, MTP, PTP) aplicando políticas tanto a usuarios como a dispositivos. Debe contar con control de aplicaciones para monitorear e impedir la ejecución o instalación de aplicaciones que puedan afectar la productividad o el rendimiento de la red, reconociendo y bloqueando automáticamente aplicaciones basadas en su huella digital (hash). La lista de aplicaciones controlables debe actualizarse automáticamente, permitiendo la liberación o bloqueo de aplicaciones o categorías específicas. Las detecciones de aplicaciones controladas deben ofrecer opciones de permitir y alertar o bloquear y alertar.

Prevención de Intrusiones y Fuga de Datos

La solución debe incluir prevención de intrusión en el host (HIPS) para monitorear y bloquear código con comportamiento malicioso antes de su ejecución. Debe poseer protección contra fugas o pérdida de datos sensibles (DLP) en el agente de protección, considerando el contenido, la extensión del archivo y múltiples destinos. Debe identificar información confidencial (números de tarjetas de crédito, cuentas bancarias, pasaportes, direcciones, teléfonos, correos electrónicos) incluso si los documentos no están clasificados, utilizando listas de control de contenido (CCL) preconfiguradas y permitiendo la adición de reglas personalizadas. Las acciones ante la detección de datos sensibles deben incluir bloqueo, registro del evento en la consola de administración web o consulta al usuario.

Control Web y Monitoreo de Cambios

La solución debe incluir control web para gestionar el acceso a sitios inapropiados, con al menos 12 categorías predefinidas y la posibilidad de crear listas blancas y negras. Debe monitorear cambios (creaciones o modificaciones) en carpetas y archivos críticos del sistema, basándose en una lista predefinida y personalizable para sistemas operativos Windows Server 2012 R2 o superior. Además, debe generar una lista blanca de aplicaciones para Windows Server 2008 R2 o superior, permitiendo la ejecución exclusiva de aplicaciones autorizadas.

Detección Proactiva de Nuevas Amenazas



La solución debe contener funcionalidad de protección contra amenazas de día cero mediante tecnología de deep learning (sin firmas). Debe ser capaz de detectar amenazas desconocidas en memoria y realizar detección y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria. Asimismo, debe detectar y bloquear troyanos y gusanos, entre otros malwares, por comportamiento de los procesos en memoria. La solución no debe requerir la descarga de firmas de ningún tipo. Debe analizar el comportamiento de nuevos procesos al ser ejecutados, complementando la exploración programada. Además, debe contar con funcionalidad de análisis forense para entender la causa raíz de los problemas, detallando procesos y subprocesos ejecutados, lectura y escritura de archivos, y claves de registro. Debe bloquear y proteger contra amenazas desconocidas potencialmente sospechosas (PUA) y permitir la generación de excepciones ante falsos positivos.

Protección Proactiva contra Ransomware

La solución debe contar con capacidad de protección contra ransomware basada en comportamiento, incluyendo la remediación de la acción de encriptación de los ransomware. Debe detectar el cifrado malicioso de forma local o remota y proteger el sector de booteo (Master Boot Record). Es fundamental que la solución sea capaz de restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware. Además, debe informar a la consola de administración web con todo el detalle del incidente, incluyendo un análisis de causa raíz, sin la necesidad de instalar otro agente o dispositivo en la red.

Protección contra Vulnerabilidades y Técnicas de Explotación

La solución debe tener la capacidad de bloquear ataques basados en la explotación de vulnerabilidades conocidas o de día cero. Debe contar con detección y protección contra las siguientes técnicas de explotación:

- Enforce Data Execution Prevention
- Mandatory Address Space Layout Randomization
- Bottom-up ASLR
- Null Page (Null Dereference Protection)
- Heap Spray Allocation
- Dynamic Heap Spray
- Stack Pivot
- Stack Exec (MemProt)
- Stack-based ROP Mitigations (Caller)
- Branch-based ROP Mitigations (Hardware Assisted)
- Structured Exception Handler Overwrite (SEHOP)
- Import Address Table Filtering (IAF)
- Load Library
- Reflective DLL Injection
- Shellcode
- VBScript God Mode
- Wow64
- Syscall

Además, la solución debe contar con mitigación de inyección de códigos en procesos, protección contra robo de credenciales, protección contra malware escondido en aplicaciones legítimas (code cave), prevención de migración de procesos maliciosos, prevención de escalamiento de privilegios y prevención de modificación de claves de registro para la ejecución de código arbitrario. Estas capacidades son cruciales para una defensa profunda contra ataques avanzados.

Reducción de la Superficie de Amenazas



La solución debe contribuir significativamente a la reducción de la superficie de ataque, incluyendo las siguientes funcionalidades:

- ✓ **Protección web y control web:** Bloqueo de acceso a sitios maliciosos o no autorizados, con categorización y políticas personalizadas. Debe permitir la creación de listas blancas y negras.
- ✓ **Reputación de descargas:** Evaluación automática del riesgo de archivos descargados mediante consultas en la nube, bloqueando archivos maliciosos antes de su ejecución.
- ✓ **Control de aplicaciones (Application Control):** Impedir que aplicaciones no autorizadas se ejecuten en los endpoints, utilizando listas blancas o bloqueo por hash. Debe actualizarse automáticamente y permitir la gestión de categorías de aplicaciones.
- ✓ **Control de periféricos (Device Control):** Permitir o bloquear el uso de dispositivos USB, almacenamiento externo, impresoras, y otros periféricos, aplicando políticas por usuario, grupo y ubicación. Debe soportar la integración con directorios de usuarios como Active Directory o Azure AD para aplicar controles contextuales.
- ✓ **Prevención de fuga de datos (DLP):** Detección y bloqueo del intento de extraer información confidencial según contenido y contexto (archivos, dispositivos, red). Debe incluir listas de control de contenido (CCL) preconfiguradas para información sensible (números de tarjetas de crédito, cuentas bancarias, pasaportes, direcciones, teléfonos, correos electrónicos) y permitir la adición de reglas personalizadas.
- ✓ **Bloqueo de servidor (Allowlisting):** Permitir la ejecución exclusiva de software previamente autorizado en sistemas críticos, protegiéndolos contra código no deseado. Esta funcionalidad es especialmente relevante para servidores Windows Server 2008 R2 o superior.

La solución debe asegurar la compatibilidad con políticas granulares por usuario, grupo y ubicación, y una integración fluida con servicios de directorio para la aplicación de controles contextuales. Además, debe soportar la generación de logs auditables centralizados para el cumplimiento de regulaciones.

Prevención de Amenazas (EDR/XDR)

La solución debe incorporar capacidades avanzadas de prevención de amenazas, tanto a nivel de Endpoint Detection and Response (EDR) como de Extended Detection and Response (XDR), para una defensa proactiva y adaptativa. Estas capacidades incluyen:

- ✓ **Protección contra Ransomware (CryptoGuard):** Tecnología de protección contra ransomware que detecta cifrado malicioso en tiempo real, incluso si se origina en otro equipo de la red. Debe incluir protección del Master Boot Record (MBR) para bloquear ransomware que intente modificarlo, y la capacidad de restaurar automáticamente los archivos cifrados por un proceso malicioso.
- ✓ **Defensas Contextuales Adaptativas:** La solución debe ajustar dinámicamente las medidas de defensa según la criticidad del endpoint, su ubicación y el nivel de amenaza detectado. Esto permite una protección más granular y eficiente.
- ✓ **Prevención basada en Inteligencia Artificial (Deep Learning):** Análisis de archivos antes de su ejecución sin necesidad de firmas, lo que es crucial para la protección contra amenazas de día cero y malware desconocido. Debe incluir la capacidad de detectar y bloquear aplicaciones potencialmente no deseadas (PUA), como adware o toolbars.
- ✓ **Live Protection (Cloud Lookup):** Verificación instantánea en la nube de archivos o URLs ante cualquier sospecha, utilizando inteligencia de amenazas actualizada.
- ✓ **Análisis de Comportamiento:** Monitoreo en tiempo real de la conducta de procesos para detectar comportamientos maliciosos que los antivirus tradicionales podrían pasar por alto. Esto incluye la detección de inyecciones de código, desbordamientos de búfer y otras técnicas de explotación.
- ✓ **Anti-Exploit con Múltiples Mitigaciones:** Defensa robusta contra técnicas de explotación, incluyendo más de 60 mitigaciones para proteger contra inyecciones de código, ROP (Return-Oriented Programming), heap spray y buffer overflow. Esto asegura la protección contra ataques que buscan aprovechar vulnerabilidades en software legítimo.
- ✓ **Integración AMSI:** Escaneo de scripts en tiempo real utilizando la interfaz antimalware de Windows para una detección temprana de amenazas basadas en scripts.



- ✓ **Detección de Tráfico Malicioso e IPS:** Visibilidad sobre conexiones de red maliciosas y protección activa contra exploits a nivel de red, actuando como un sistema de prevención de intrusiones (IPS).
- ✓ **Monitorización de Integridad de Archivos (FIM):** Detección de modificaciones no autorizadas en archivos del sistema o aplicaciones críticas, especialmente en servidores, para identificar actividades sospechosas o maliciosas.
- ✓ **Datos Exhaustivos en el Dispositivo y la Nube:** Recopilación de datos detallados para análisis en tiempo real o histórico, facilitando la investigación de incidentes.
- ✓ **Retención de Datos en la Nube:** Capacidad de retención de datos de eventos de seguridad por un período mínimo de 90 días, lo cual es fundamental para el cumplimiento de normativas forenses y de auditoría.

Es importante que el motor de protección funcione eficazmente sin conexión a internet (protección offline) y que los eventos y datos del endpoint se integren nativamente con una plataforma XDR para una correlación multivectorial completa.

Detección (EDR/XDR)

La solución debe proporcionar capacidades avanzadas de detección que abarquen tanto el EDR como el XDR, permitiendo una visibilidad integral y una identificación precisa de amenazas. Estas capacidades incluyen:

- ✓ **Detección de Eventos Sospechosos en Endpoint:** Identificación de cambios anómalos, ejecuciones inusuales o procesos ocultos en los dispositivos finales.
- ✓ **Priorización con Inteligencia Artificial:** Utilización de modelos de riesgo para jerarquizar alertas, lo que ayuda a los analistas a enfocarse en las amenazas más críticas y reales.
- ✓ **Asignación Automática a MITRE ATT&CK:** Cada detección debe ser contextualizada automáticamente dentro de la matriz MITRE ATT&CK, facilitando el análisis táctico y la comprensión del comportamiento del atacante.
- ✓ **Detección en Contenedores Linux:** Soporte específico para la detección de amenazas en ambientes modernos como Docker o Kubernetes, asegurando la protección de infraestructuras basadas en contenedores.
- ✓ **Correlación de Eventos entre Productos:** Capacidad clave para una plataforma XDR, que permite ver la progresión de un ataque a través de múltiples capas de seguridad (correo, red, endpoint, servidor, cloud), unificando la información para una visión completa del incidente.

Es fundamental que el sistema se integre con SIEMs (Security Information and Event Management) y otras herramientas SOC (Security Operations Center) para ampliar la visibilidad y mejorar la capacidad de respuesta. Además, debe soportar la detección en entornos híbridos y BYOD (Bring Your Own Device).

Investigación (EDR)

La solución debe proporcionar herramientas robustas para la investigación de incidentes, permitiendo a los analistas comprender a fondo la naturaleza y el alcance de las amenazas. Las capacidades clave incluyen:

- ✓ **Gráficos de Análisis de Causa Raíz (RCA):** Visualización completa del camino del ataque, desde la intrusión inicial hasta la carga útil final, facilitando la comprensión de la secuencia de eventos.
- ✓ **Casos Automáticos y Manuales:** Capacidad para agrupar eventos relacionados y tratarlos como un incidente completo, mejorando la organización y gestión de las investigaciones.
- ✓ **Live Discover y Consultas Programadas:** Herramientas potentes para buscar patrones de amenaza en tiempo real o con periodicidad, permitiendo la caza proactiva de amenazas.
- ✓ **Asistencia de IA Generativa para Consultas:** Ayuda a los analistas a redactar consultas avanzadas sin necesidad de ser expertos en lenguajes estructurados, democratizando el acceso a la información de seguridad.
- ✓ **Exportación de Datos Forenses:** Los eventos deben poder exportarse para cumplir con requerimientos regulatorios o peritajes externos, asegurando la cadena de custodia de la evidencia.

- ✓ **Información de Amenazas (Threat Intelligence):** Contextualización de las detecciones con indicadores de compromiso (IOC) y fuentes externas de inteligencia de amenazas, enriqueciendo la investigación.
- ✓ **Integración de IA Generativa para Gestión de Casos:** Mejora la eficiencia del Centro de Operaciones de Seguridad (SOC) con ayuda automatizada para la redacción y documentación de casos.

Es crucial que la solución asegure soporte para inteligencia de amenazas en tiempo real y que los datos almacenados puedan ser exportados legalmente según las normativas locales aplicables.

Respuesta (EDR/XDR)

La solución debe ofrecer capacidades de respuesta rápidas y eficientes para contener y remediar las amenazas detectadas. Las funcionalidades clave incluyen:

- ✓ **Limpieza Automática de Malware:** La solución debe ser capaz de remover el malware y restaurar el sistema sin intervención manual, minimizando el impacto de los incidentes.
- ✓ **Reversión de Cifrado de Ransomware:** Capacidad para restaurar automáticamente los archivos comprometidos en un ataque de ransomware, recuperando la información sin necesidad de copias de seguridad externas.
- ✓ **Finalización de Procesos:** El EDR debe detener procesos maliciosos activos tan pronto como se detectan, impidiendo su propagación y ejecución.
- ✓ **Aislamiento de Endpoints:** La solución debe permitir el aislamiento automático de endpoints cuando se detecta una amenaza grave, conteniendo el incidente y evitando la propagación lateral.
- ✓ **Respuesta Automatizada por Tipo de Amenaza:** La capacidad de automatizar la respuesta según el tipo de amenaza, permitiendo una acción en segundos en el caso de ataques severos, es crucial para minimizar el tiempo de permanencia de los atacantes.

4.2. PROTECCIÓN EMAIL

- La consola de administración debe ser Saas
- La solución debe tener Protección contra phishing por suplantación de identidad con procesamiento de lenguaje natural
- Manejo de protocolos SPF, DKIM y DMARC
- La solución debe realizar Análisis de reputación
- La solución brinda Protección de antispam, escaneo de malware y sandbox cloud
- Debe poder realizar Detección de URL maliciosas y Reescritura de URL en el momento del clic además de brindar Detección de anomalías del encabezado
- Debe permitir Filtrar por país de origen e idiomas
- Análisis de nombres para mostrar (VIP y marcas)
- Debe contar con Verificaciones de dominios similares
- Políticas DLP de múltiples reglas para grupos y usuarios individuales
- Debe contar con Listas de control de contenido (financieros, contenidos confidenciales, información de salud y PII)
- Cifrado TLS aplicado
- Estándar S/MIME
- Autenticación del remitente
- Cifrado de mensajes y archivos adjuntos basado en push
- La solución debe ofrecer un control integral sobre el flujo de correo electrónico, asegurando la seguridad en todas las direcciones. También escanear minuciosamente tanto los mensajes entrantes para detectar amenazas como los salientes para prevenir la fuga de datos y el spam.
- La solución debe permitir la implementación de políticas a nivel de dominio, grupo y usuario.
- Se debe ofrecer un control granular sobre el correo sospechoso a través de la cuarentena de administrador y usuario, permitiendo a los administradores revisar y liberar mensajes, mientras que los usuarios pueden gestionar sus propios correos en cuarentena.



- Debe tener Banners de correo electrónico entrante (remitente confiable, externo, no confiable)
- Debe permitir Sincronización de AD o sincronización de Azure AD
- Integración mediante API (sin interrupción de flujo de correo, Microsoft nube

Se debe contar con una única consola de administración para la protección de endpoints, servidores, email y firewall. Esta consolidación no es una opción, sino una necesidad estratégica para la ciberseguridad de la entidad y permite una visibilidad completa y correlacionada de todas las amenazas, una respuesta unificada y más rápida a incidentes, y una gestión drásticamente simplificada que reduce la complejidad operativa y los errores humanos, los cuales deben estar dados de acuerdo con la siguiente tabla técnica:

DESCRIPCION DEL BIEN	CANT
Solución integral y unificada anti-malware de seguridad para endpoints, que combine múltiples capacidades de protección en un solo agente y consola de administración, la solución debe tener una consola para definir políticas de seguridad para la prevención de amenazas, control de acceso y cumplimiento, protección de datos, despliegue y actualizaciones de agentes del Endpoint, La solución debe incluir una Gestión Basada en nube en modalidad SaaS que permite gestionar equipos, con su debido licenciamiento, puesta en funcionamiento, soporte de fábrica y garantía. La solución requerida debe proveer como mínimo: • Gestión Basada en la Nube (SaaS) sin requerir infraestructura de gestión local. • Consola de Administración Única, para administrar todas las capacidades de protección (anti-malware, control de acceso, DLP, etc.), políticas, informes y despliegue de agentes. • Agente Único (Single Agent), ejecutarse en el endpoint mediante un único agente liviano que integre todas las funcionalidades de seguridad requeridas. • Soporte Multiplataforma, soportar como mínimo los siguientes sistemas operativos empresariales: Windows (Escritorio/Servidor), macOS y Linux • Despliegue y Actualizaciones Centralizadas • Alta Disponibilidad y Escalabilidad • Prevención de Ejecución de Malware, Capacidad de detección y bloqueo de amenazas conocidas • Detección sin Firma (Heurística/Comportamental), análisis heurístico, inteligencia artificial o machine learning para detectar y bloquear malware de día cero y amenazas polimórficas • Protección Específica contra Ransomware. • Análisis de Comportamiento del Sistema (Endpoint Detection and Response - EDR), recolección de telemetría de endpoints y la visibilidad de la cadena de eventos del ataque. • Análisis y Control de Aplicaciones, Capacidad para identificar y bloquear la ejecución de aplicaciones no autorizadas o potencialmente no deseadas • Control de Dispositivos Periféricos (USB/Removibles) • Firewall de Host Bidireccional, módulo de firewall capaz de definir políticas de tráfico entrante y saliente. • Control de Contenido Web y Filtrado de URL, aplicar políticas de filtrado de contenido por categorías para mejorar la productividad y seguridad. • Prevención de Pérdida de Datos (Data Loss Prevention - DLP) Básico, monitorear y bloquear la transferencia de datos sensibles. • Soporte Técnico de Fábrica 24/7	500
Solución integral y unificada anti-malware de seguridad para endpoints, que combine múltiples capacidades de protección en un solo agente y consola de administración, la solución debe tener una consola para definir políticas de seguridad para la prevención de amenazas, control de acceso y cumplimiento, protección de datos, despliegue y actualizaciones de agentes desde los servidores, La solución debe incluir una Gestión Basada en nube en modalidad SaaS que permite gestionar equipos, con su debido licenciamiento, puesta en funcionamiento, soporte de fábrica y garantía. La solución requerida debe proveer como mínimo: • Soporte Extendido para SO de Servidor, garantizar soporte total (funcionalidad completa de prevención, EDR y XDR) • Visibilidad EDR en Tiempo Real, donde el sistema debe recolectar telemetría crítica de bajo nivel: actividad de red saliente/entrante • Correlación XDR y Movimiento Lateral, correlacionar eventos de seguridad entre el servidor y otros endpoints • Capacidad de establecer políticas de Whitelisting (lista blanca) que permitan la ejecución solo de aplicaciones y servicios previamente aprobados. • Control de Acceso y Puertos de Red permitir la definición de políticas de red basadas en el rol del servidor	10

• Firewall de Host Bidireccional, módulo de firewall capaz de definir políticas de tráfico entrante y saliente. • Control de Contenido Web y Filtrado de URL, aplicar políticas de filtrado de contenido por categorías para mejorar la productividad y seguridad. • Prevención de Pérdida de Datos (Data Loss Prevention - DLP) Básico, monitorear y bloquear la transferencia de datos sensibles. • Soporte Técnico de Fábrica 24/7	
Protección de correo electrónico que combine capacidades de filtrado multicapa con tecnologías de inteligencia artificial para detectar y bloquear amenazas avanzadas como phishing, ransomware y ataques BEC con sandboxing integrado para análisis dinámico de archivos adjuntos y URLs, junto con cifrado automático para emails sensibles y políticas de DLP . Debe ofrecer integración con plataformas de colaboración en la nube (Microsoft 365) sin requerir agentes adicionales, y contar con una consola de gestión centralizada y reporting detallado para cumplimiento normativo. La consola de administración debe ser SaaS y contener las siguientes especificaciones: •La solución debe tener Protección contra phishing por suplantación de identidad con procesamiento de lenguaje natural •Manejo de protocolos SPF,DKIM y DMARC •La solución debe realizar Análisis de reputación •La solución brinda Protección de antispam, escaneo de malware y sandbox cloud •Debe poder realizar Detección de URL maliciosas y Reescritura de URL en el momento del clic además de brindar Detección de anomalías del encabezado •Debe permitir Filtrar por país de origen e idiomas •Análisis de nombres para mostrar (VIP y marcas) •Debe contar con Verificaciones de dominios similares •Políticas DLP de múltiples reglas para grupos y usuarios individuales •Debe contar con Listas de control de contenido (financieros, contenidos confidenciales, información de salud y PII) •Cifrado TLS aplicado •Estándar S/MIME •Autenticación del remitente •Cifrado de mensajes y archivos adjuntos basado en push •La solución debe ofrecer un control integral sobre el flujo de correo electrónico, asegurando la seguridad en todas las direcciones. También escanear minuciosamente tanto los mensajes entrantes para detectar amenazas como los salientes para prevenir la fuga de datos y el spam. •La solución debe permitir la implementación de políticas a nivel de dominio, grupo y usuario. •Se debe ofrecer un control granular sobre el correo sospechoso a través de la cuarentena de administrador y usuario, permitiendo a los administradores revisar y liberar mensajes, mientras que los usuarios pueden gestionar sus propios correos en cuarentena. •Debe tener Banners de correo electrónico entrante (remitente confiable, externo, no confiable) •Debe permitir Sincronización de AD o sincronización de Azure AD •Integración mediante API (sin interrupción de flujo de correo, Microsoft nube	400
Protección de sistemas operativos desatendidos para equipos servidores con funcionalidades de EDR y XDR: • Soporte Extendido para SO Antiguos, para versiones de sistemas operativos de servidor que hayan alcanzado su Fin de Vida como Windows Server 2008/2012, o versiones específicas de RHEL/CentOS • Protección sin Conexión (Offline Protection) mantener una alta eficacia de detección y prevención incluso si el servidor desatendido pierde temporalmente la conexión con la consola SaaS • Correlación de Endpoints y Servidores capaz de diferenciar y correlacionar automáticamente los eventos de seguridad entre servidores y endpoints de usuario • Detección de Anomalías de Comportamiento (UEBA Ligero) incluyendo algoritmos para establecer una línea base del comportamiento normal de los servidores desatendidos y alertar sobre desviaciones anómalas • Prevención de Pérdida de Datos (Data Loss Prevention - DLP) Básico, monitorear y bloquear la transferencia de datos sensibles. • Soporte Técnico de Fábrica 24/7	1
Servicios profesionales de ingeniería para implementación y soporte de las soluciones de protección de endpoints, servidores, email, inventario de activos, gestión de vulnerabilidades y control remoto.	1

4.3. CARTAS Y CERTIFICACIONES.



El proponente debe aportar certificación emitida por el fabricante de cada solución ofertada con vigencia no mayor a 30 días dirigida al presente proceso de selección en la cual se informe que el proponente es partner autorizado de la marca ofertada y tiene contrato comercial vigente con la fábrica dentro del nivel de membresía más alto estipulado por el fabricante.

Las soluciones presentadas deben ser reconocidas en el mercado de ciberseguridad por evaluadores correspondientes.

Para contar con una solución reconocida en el mercado, confirmar que el fabricante de la solución ofertada debe tener cobertura sobre los entornos Windows y Linux, debe respaldar sus tácticas de ciberseguridad por MITRE ATT&CK.

4.4. PERSONAL REQUERIDO

Los servicios que ofrece deberán contar con el respaldo de personal idóneo para el ejercicio de cada una de las actividades requeridas. En consecuencia, el proponente deberá acreditar que cuenta con el personal y entregar las hojas de vida con los certificados solicitados de al menos el siguiente personal para la ejecución del objeto contractual:

INGENIERO DE SOPORTE E IMPLEMENTACION	
Rol	Líder profesional de Implementación
Actividades	Implementar y configurar la solución ofertada, la cual comprende la ejecución técnica de la instalación y configuración de la solución ofertada, siguiendo las directrices y mejores prácticas del fabricante; la validación de funcionalidad mediante la realización de pruebas integrales y la subsanación de cualquier anomalía identificada. Realizar la transferencia de conocimiento al personal interno a través de sesiones de capacitación y formalizar todo el ciclo de trabajo con la entrega de un informe técnico detallado que valide la implementación, configuración final y la formación impartida al equipo operativo de la entidad.
Profesión u Oficio	Título profesional ingeniería en electrónica, Sistemas, Telecomunicaciones o afines. Tarjeta o matrícula profesional.
Experiencia General	Dos (02) años de experiencia profesional contada a partir de la fecha de expedición de la Tarjeta Profesional
Experiencia Específica	En proyectos relacionados con seguridad de la información y/o seguridad informática como auditor, analista, director, y/o consultor, cuya duración acumulada mínima sea de tres (3) años
Cantidad Requerida	UNO (01)
Requisitos	Hoja de Vida, con los respectivos soportes de estudios realizados y certificaciones laborales que acrediten su experiencia. Diploma de Profesional, tarjeta y antecedentes profesionales expedidos por el COPNIA, judiciales, disciplinarios, fiscales y medidas correctivas. Carta de compromiso del cumplimiento y disponibilidad de asistir a las instalaciones de la Entidad del 100%, de acuerdo con lo establecido en las especificaciones técnicas y obligaciones específicas del contratista.
Es necesario precisar que se debe anexar esta información con la presentación de la oferta.	
Cada certificación de experiencia deberá contener la siguiente información:	
- Nombre de la entidad o persona contratante que certifica, dirección y teléfono. - Objeto del contrato, obligaciones, alcance o condiciones sean iguales al objeto de la presente selección o comprendan dentro de sus actividades las que forman parte del objeto a celebrar. - Fecha de inicio y finalización del contrato o de suscripción del contrato. - Firma de la persona que expide la certificación	



Estudios en el exterior:

En caso de ser presentados títulos académicos obtenidos en el exterior, de conformidad con la Circular externa única CCE-EICP-MA-06 Versión 2 de fecha 15 de julio de 2022, los códigos equivalentes en la clasificación Internacional normalizada de educación -CINE, que para Colombia aplica de la CINE-F 2013. A. C, de conformidad con lo establecido en la Resolución 1791 del 3 de julio de 2018, expedida por el DANE especificando nivel y campo de aplicación que se tendrán en cuenta para el proceso de conformidad con la siguiente tabla:

Requisito Solicitado	Nivel CINE-F 2013	Código Nivel	Campo CINE-F 2013	Código Campo
Título Profesional: Ingeniería en Electrónica, Sistemas, Telecomunicaciones o afines.	Educación Terciaria, Nivel 6 (Grado o equivalente)	6	06 ingeniería, Industria y Construcción	06
			Subcampo específico (Sistemas, Telecomunicaciones, Electrónica)	061 ingeniería y profesiones afines
Tarjeta o Matrícula Profesional	No aplica código CINE (Es requisito de ejercicio profesional, no de nivel educativo).	N/A	No aplica código CINE	N/A
Equivalencia de Títulos Académicos (Exterior)	Educación Terciaria, Nivel 6 (Grado o equivalente)	6	06 ingeniería, Industria y Construcción	06

En virtud de la naturaleza tecnológica requerida por el Municipio de Tocancipá, la ejecución de las actividades deberá estar en concordancia con los lineamientos de confianza y seguridad digital del Estado Colombiano. Asimismo, en observancia de los estándares de publicidad, acceso a la información y transparencia de la gestión pública, el objeto contractual se desarrollará bajo los parámetros de la Resolución 1519 de 2020 expedida por el MINTIC, asegurando que la información y servicios digitales cumplan con los requisitos de accesibilidad, seguridad y estándares de información definidos por el MINTIC.

5. ASPECTOS REGULATORIOS





Que el artículo 2 de la Constitución Política de Colombia dispone que *"son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo"*.

Que el artículo 209 ibidem prevé que *"la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado (...)"*.

Que el artículo 311 ibidem dicta que *"Al municipio como entidad fundamental de la división político-administrativa del Estado le corresponde prestar los servicios públicos que determine la ley, construir las obras que demande el progreso local, ordenar el desarrollo de su territorio, promover la participación comunitaria, el mejoramiento social y cultural de sus habitantes y cumplir las demás funciones que le asignen la Constitución y las leyes"*.

Que el inciso segundo del artículo 339 ibidem establece que *"Las entidades territoriales elaborarán y adoptarán de manera concertada entre ellas y el gobierno nacional, planes de desarrollo, con el objeto de asegurar el uso eficiente de sus recursos y el desempeño adecuado de las funciones que les hayan sido asignadas por la Constitución y la ley. Los planes de las entidades territoriales estarán conformados por una parte estratégica y un plan de inversiones de mediano y corto plazo"*.

Que la Ley 1341 de 2009 *"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"* señala como Política de Estado el desarrollo de las Tecnologías de la Información y las Comunicaciones la cual involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir entre otros fines a la producción de bienes y servicios, al desarrollo social, la productividad, competitividad y la inclusión social.

El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

Esta Ley transforma el Ministerio de Comunicaciones en el Ministerio de Tecnologías de la Información y las Comunicaciones, creando un marco normativo para el desarrollo del sector y la promoción del acceso y uso de las TIC a través de la masificación, el impulso a la libre competencia, el uso eficiente de la infraestructura y en especial el fortalecimiento de la protección de los derechos de los usuarios. Con el Decreto 1078 de 2015 y sus modificaciones *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"* se identifican las entidades del sector, se busca compilar la normatividad vigente expedida por el Gobierno Nacional mediante las facultades reglamentarias conferidas por el numeral 11 del artículo 189 de la Constitución Política al Presidente de la República para la cumplida ejecución de las leyes en el sector de Tecnologías de la Información y las Comunicaciones que aplican a las entidades del sector de Tecnologías de la Información y las Comunicaciones.



La Ley 1978 de 2019 *"Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones"* busca alinear los incentivos de los agentes y autoridades del sector de Tecnologías de la Información y las Comunicaciones (TIC), aumentar su certidumbre jurídica, simplificar y modernizar el marco institucional del sector, focalizar las inversiones para el cierre efectivo de la brecha digital y potenciar la vinculación del sector privado en el desarrollo de los proyectos asociados, así como aumentar la eficiencia en el pago de las contraprestaciones y cargas económicas de los agentes del sector.

Con el Decreto 1064 de 2020 *"Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones"*, se definen los objetivos del Ministerio, las funciones, la nueva estructura con sus funciones en torno al fortalecimiento de las TIC.

Que mediante la Ley 2108 de 2021 *"Ley de internet como servicio público esencial y universal"* o *"Por medio de la cual se modifica la ley 1341 de 2009 y se dictan otras disposiciones"* establece como fin último de intervención del Estado en el Sector TIC el propender por el servicio universal a las Tecnologías de la Información y las Comunicaciones.

Que el Decreto 767 de 2022 *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"* señala que la Política de Gobierno Digital se desarrollará a través de un esquema que articula los elementos que la componen, así: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo, entendidos así:

"(...)

4. Líneas de Acción: Los sujetos obligados ejecutarán acciones orientadas a desarrollar servicios y procesos inteligentes, tomar decisiones basadas en datos y consolidar un Estado abierto, con el fin de articular las Iniciativas Dinamizadoras de la Política de Gobierno Digital. Estas Líneas de Acción se materializarán en las sedes electrónicas de cada uno de los sujetos obligados, siguiendo los estándares señalados para tal fin.

4.1. Servicios y Procesos Inteligentes: Esta línea de acción busca que los sujetos obligados desarrollen servicios y procesos digitales, automatizados, accesibles, adaptativos y basados en criterios de calidad, a partir del entendimiento de las necesidades del usuario y su experiencia, implementando esquemas de atención proactiva y el uso de tecnologías emergentes.

4.2. Decisiones Basadas en Datos: Esta línea de acción busca promover el desarrollo económico y social del país impulsado por datos, entendiéndolos como infraestructura y activos estratégicos, a través de mecanismos de gobernanza para el acceso, intercambio, reutilización y explotación de los datos, que den cumplimiento a las normas de protección y tratamiento de datos personales y permitan mejorar la toma de decisiones y la prestación de servicios de los sujetos obligados.

(...)"

Que es un compromiso del Gobierno nacional garantizar la implementación de estrategias necesarias para contribuir con la eficiencia de la administración y gestión de los recursos públicos. La implementación de estas estrategias demanda la aplicación y uso de instrumentos adecuados para el manejo de la información que es fundamental para la toma de decisiones e inversión del presupuesto público, la optimización de los recursos, la transparencia y efectividad en las intervenciones y los



procesos internos de planeación, formulación, seguimiento y evaluación de la gestión pública integralmente.

Que con la incorporación de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de las funciones y compromisos de las entidades estatales, así como en el cumplimiento de las metas de los planes de desarrollo, se busca maximizar los beneficios ofreciendo mejores servicios a la comunidad y a las instituciones, de manera más eficiente y transparente, tanto en las actividades internas como en la interacción con otras entidades públicas y privadas, con la comunidad y ciudadanía en general, facilitando las relaciones del ciudadano con la Administración.

Se busca, entre otras cosas, garantizar la priorización de las acciones de manera que se beneficie la población más vulnerable, procurando la intervención de los grupos sociales que más lo necesitan; facilitando la toma de decisiones, el acceso y administración de la información, mediante datos y cifras confiables en tiempo real, con oportunidad, menor riesgo en la información, seguimiento y actualización permanente y optimización del gasto público.

6. ESTUDIO DE LA OFERTA Y LA DEMANDA

4.5. OFERTA

La oferta para el sector público de acuerdo con la ubicación georreferencial de la Entidad se segmenta principalmente en dos tipos de proveedores:

Proveedores de Soluciones Especializadas (Software de Línea): Estos son los competidores más directos, ya que ofrecen productos probados y estandarizados para la gestión municipal.

Fábricas de Software y Empresas de Desarrollo a la Medida: Esta oferta es clave para el desarrollo de sistemas que no están cubiertos por el software de línea o que requieren una integración profunda.

En cumplimiento de las directrices emitidas por la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE) para el análisis del sector económico y la estructuración del presupuesto oficial, la Alcaldía de Tocancipá adelantó la consulta en las bases de datos abiertos de Compra Pública e instrumentos de Abastecimiento Estratégico. Con base en los códigos de la clasificación UNSPSC asociados al objeto contractual (43233200 - Software de seguridad y protección de datos, 81111800 - Servicios de seguridad de la información y 43232800 - Software de correo electrónico), se identificó el histórico de contratación pública en entidades de similares características e instituciones del orden nacional, analizando las modalidades de selección, valores adjudicados y proveedores recurrentes para soluciones de correlación EDR/XDR y protección de correo electrónico.

La Secretaría de Hacienda realiza el análisis para establecer los indicadores financieros teniendo en cuenta las empresas del mercado que se encuentran dentro de las actividades comercio al por mayor de computadores, equipo periférico y programas de informática y actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas). De igual manera para establecer el valor promedio de la contratación se solicitaron cotizaciones a las empresas CORPORACIÓN MAESTRES SAS y ML TR3S SAS. Las empresas consultadas por las Secretaría de Hacienda son:



Empresas de Desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas), consultoría informática y actividades relacionadas. en TOCANCIPA

Empresa	Localidad	Departamento	Teléfono
ADC DE COLOMBIA SISTEMAS POS S A S	TOCANCIPA	CUNDINAMARCA	3166686283
SOLUCIONES TECNOLOGICAS & INFORMATICAS SAS	TOCANCIPA	CUNDINAMARCA	6018697512
INGENIERIA RECURSOS Y SISTEMAS S A S	TOCANCIPA	CUNDINAMARCA	3142988060
SST NETWORK SAS	TOCANCIPA	CUNDINAMARCA	3123485748
SERVICIOS ECOLOGICOS Y TECNOLOGICOS S A S	TOCANCIPA	CUNDINAMARCA	3004931007
WAREVAL S A S	TOCANCIPA	CUNDINAMARCA	3125068328
PREVENTION RISK LABORAL SAS	TOCANCIPA	CUNDINAMARCA	3107797706
GAMMASYSTEM S A S	TOCANCIPA	CUNDINAMARCA	3132701512
ELIANS CONSULTING SAS	TOCANCIPA	CUNDINAMARCA	3115460654
FOTOVOLTAICA SAS	TOCANCIPA	CUNDINAMARCA	3134915476

Cabe señalar que la información recopilada a través de los diferentes mecanismos y herramientas que disponen las entidades públicas y privadas, información de internet, se encuentran en constante actualización para evidenciar efectiva y ágilmente datos concretos frente a la caracterización requerida, que permita validar o identificar en el sector empresarial los lineamientos normativos que entraron en vigor frente al tema en mención, especialmente por la reserva de la información.

ANALISIS DE MIPYMES

En Colombia las MIPYMES (Micro, Pequeña y Mediana Empresa) representan el 99,5% de las empresas formales, generan el 79% del empleo y aportan el 40% al PIB, por lo que son un motor fundamental para el crecimiento económico, la generación de empleo y la reducción de la pobreza.

Se debe resaltar que todas estas personas naturales y/o jurídicas, cuentan con experiencia, capacidad financiera, organizacional y jurídica suficiente; por lo cual las sitúan, sin perjuicio de las exigencias de la entidad dentro del proceso de selección entre los posibles oferentes que eventualmente podrían tener la idoneidad para ejecutar el objeto del contrato.

Con el propósito de garantizar la libre concurrencia, la pluralidad de oferentes y promover la participación de la industria nacional, la Oficina de Sistemas (TIC) de la Alcaldía de Tocancipá adelantó el estudio de mercado enfocado en identificar MiPymes (Micro, Pequeñas y Medianas Empresas) y proveedores especializados en ciberseguridad domiciliados en Colombia. Dicho análisis permitió verificar la oferta técnica y comercial disponible para la adquisición, configuración, integración y puesta en funcionamiento de una solución integral que correlacione plataformas de protección de Endpoint y Servidores (EDR y XDR) con sistemas avanzados de protección de correo electrónico. Lo anterior, con el fin de fortalecer la postura de seguridad digital del Municipio y atender los requerimientos normativos de confidencialidad e integridad de la información pública.

Dado que la información específica de las bases de datos públicas de MiPymes de proveedores directos de la Alcaldía de Tocancipá no está disponible en tiempo real y que las MiPymes de ciberseguridad pueden ser numerosas, se han identificado empresas y proveedores especializados en EDR/XDR, protección de email y protección de endpoints en Colombia que cumplen con el objeto requerido por la entidad, en este sentido se tienen algunas empresas identificadas así:



Nombre de la Empresa	Ubicación Principal (Colombia)	Sitio Web	Objeto Social/Especialidad Relevante
Nsit S.A.S.	Sabaneta (Medellín), Bogotá	https://www.nsit.com.co	Ciberseguridad integral para PyMEs, Análisis de Brecha , SIEM Básico , EDR/XDR , Pruebas de Penetración, Respuesta a Incidentes.
WiCom Networks	Sin datos de ubicación específica, pero Partner local.	https://wicom.net.co	Partner de Bitdefender GravityZone, especializado en EDR/XDR y MDR 24/7 , incluyendo protección de endpoints, servidores y correo .
Biglinks / Seqrite	Soporte técnico en Colombia	https://biglinks.co	Plataforma de defensa activa XDR para empresas en Colombia, correlacionando <i>endpoints</i> , red y correo . Soluciones escalables para PyMES.
Elliptical SAS	Sin datos de ubicación específica.	https://elliptical.com.co	Soluciones tecnológicas en Ciberseguridad. Especializados en EDR , SIEM , Seguridad Perimetral, Protección de Correo Electrónico y WAF .
Globaltek Security	Sede Administrativa: Teléfono (+57) 310 233 5760	https://globaltek.co	Ciberseguridad Resiliente Automatizada (CsRA) . Consultoría especializada (ISO 27001), Soluciones de seguridad, implementador RPA.
2Secure SAS	Sin datos de ubicación específica.	https://2secure.co	Consultoría y servicios TI, Seguridad de la Información , Desarrollo de software, Informática Forense, con experiencia en diversos campos de la seguridad.
GRUPO ORUSS	Sin datos de ubicación específica.	https://grupooruss.com	(Mencionado en directorios como empresa líder en Ciberseguridad en Colombia). Ofrece soluciones y consultoría de seguridad.

Con el anterior análisis se concluye que existen MiPymes en el país que pueden proveer la compraventa objeto de contratación y por tanto pueden participar dentro del proceso, por lo cual se procede a establecer Criterios diferenciales para ellas, teniendo en cuenta lo contenido en el artículo 2.2.1.2.4.2.18 del Decreto 1082 de 2015, adicionado por el artículo 3 del Decreto 1860 de 2021, que promuevan y faciliten la participación en el procedimiento de selección competitivos de las MiPymes domiciliadas en Colombia.

Para el efecto, en función de los criterios de clasificación empresarial, se procede a analizar uno a uno los requisitos diferenciales establecidos en la norma citada, determinando cuales sí o no se aplicarán para promover y facilitar su participación en el proceso de selección que se adelantará, así:

CRITERIOS DIFERENCIALES PARA MYPIMES



Que atendiendo al artículo 2.2.1.2.4.2.18. Criterios diferenciales para Mipyme en el sistema de compras públicas del Decreto 1082 de 2015, (adicionado por el artículo 3 del Decreto 1860 del 24 de diciembre de 2021) con el fin de reglamentar los artículos 30, 31, 32, 34 y 35 de la Ley 2069 de 2020, en lo relativo al Sistema de compras públicas y se dictan otras disposiciones, las Entidades Estatales indistintamente de su régimen de contratación, establecerán condiciones habilitantes diferenciales que promuevan y faciliten la participación en los procedimientos de selección competitivos de las Mipyme domiciliadas en Colombia.

En virtud de lo anterior, la entidad procederá a efectuar el análisis correspondiente para determinar cuál (es) será (n) el (los) criterio(s) diferencial(es) para las MiPymes a fin de facilitar su participación en el proceso de selección que se adelantará, así:

a) Tiempo de experiencia.

La experiencia del proponente o la antigüedad en el mercado, permite evidenciar el conocimiento en el sector económico al que pertenezca y el tiempo que ha permanecido en el mismo, sin embargo este criterio no ha sido determinante para la estructuración del presente proceso, en razón a que la entidad considera que la antigüedad en el mercado no es una garantía de mejores resultados o de más calidad en el servicio o bien que se pretende adquirir con el proceso de contratación, es así para establecer los requisitos habilitantes del presente proceso no se tuvo en cuenta este criterio, pues aunado a lo anterior, incluir este requerimiento podría limitar la pluralidad de oferentes frente a proponentes que cuentan con experiencia en la ejecución de contratos que tienen relación con el objeto del presente proceso, pero que no cuentan con una antigüedad determinada, por lo tanto al no ser un criterio utilizado por la entidad para definir los requisitos habilitantes, tampoco será utilizado como criterio diferencial para las MiPymes.

b) Número de contratos para la acreditación de la experiencia

Que en razón a que la entidad requiere que los proponentes adjudicatarios cuenten con experiencias plurales y múltiples, que permitan evidenciar la suficiente idoneidad y la experiencia en la ejecución de diversos contratos y actividades prestación de servicios de conectividad similares a la que se pretenden adelantar, se considera por parte de la entidad, que este es un criterio determinante en el proceso y por tanto con la finalidad de beneficiar a las MiPymes, se establecerán condiciones más exigentes respecto a los proponentes que concurren al procedimiento de selección que no sean MiPymes y por lo tanto el criterio habilitante quedará de la siguiente manera en el proceso a adelantar:

Experiencia General Habilitante

La entidad como requisito mínimo habilitante solicita que el proponente acredite la experiencia con hasta dos (2) contratos celebrados con entidades públicas y/o privadas, cuyo objeto y/o alcance esté relacionado con la Adquisición, instalación, configuración y puesta en funcionamiento de soluciones de seguridad iguales y/o similares a las características solicitadas, cuyos valores finales o cuantías de los mismos sumados sea igual o mayor al cien por ciento (100 %) del presupuesto oficial asignado por la entidad, expresado en SMMLV, contratos que deben encontrarse reportados en el RUP, identificados en los códigos UNSPSC que se enuncian a continuación, hasta el tercer nivel:

Código	Nombre
43233200	Software de seguridad y protección
81111500	Ingeniería de software o hardware



En este sentido y como parte del análisis previo, se tendrán en cuenta como criterio diferencial para el proceso de selección en cuestión: **EXPERIENCIA DIFERENCIAL HABILITANTE PARA MIPYME:** Los proponentes MIPYME domiciliados en Colombia, deberán acreditar la celebración, ejecución y liquidación con máximo tres (3) contratos celebrados con entidades públicas o privadas cuyo objeto y/o alcance esté relacionado con la Adquisición, instalación, configuración y puesta en funcionamiento de soluciones de seguridad iguales y/o similares a las características solicitadas, cuyos valores finales o cuantías de los mismos sumados sea igual o mayor al cien por ciento (100 %) del presupuesto oficial asignado por la entidad, expresado en SMMLV, contratos que deben encontrarse reportados en el RUP, identificados en los códigos UNSPSC que se enuncian a continuación, hasta el tercer nivel:

Código	Nombre
43233200	Software de seguridad y protección
81111500	Ingeniería de software o hardware

Tratándose de proponentes plurales, los criterios diferenciales 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: En caso de acreditar su experiencia habilitante mediante este criterio diferencial, deberá manifestarlo de manera expresa en su oferta.

Se aclara que el factor diferencial para MYPIME es el número de contratos, los demás requisitos respecto de la acreditación de la experiencia serán de cumplimiento en su totalidad por el proponente.

c) y d). Índices de capacidad financiera y organizacional:

Dado que las MiPymes representan el 99% de la economía colombiana, la generación de indicadores financieros está presentando el comportamiento de una económica cuyo impulso es resultado de la operación de MiPymes por lo que no resulta procedente la determinación de indicadores de capacidad financiera y organizacional diferenciales pues menos del 1% de las empresas del país se clasifican como grandes empresas. Así las cosas, NO se establecen indicadores diferenciales de capacidad financiera y organizacional para las MIPYMES.

e) Valor de la garantía de seriedad de la oferta.

La garantía de seriedad de la oferta se exige a los proponentes para cubrir la sanción derivada del incumplimiento de la oferta, en los siguientes eventos:

- A. La no ampliación de la vigencia de la garantía de seriedad de la oferta cuando el plazo para la adjudicación o para suscribir el contrato es prorrogado, siempre que tal prórroga sea inferior a tres (3) meses.
- B. El retiro de la oferta después de vencido el plazo fijado para la presentación de las ofertas
- C. La no suscripción del contrato sin justa causa por parte del adjudicatario.
- D. La falta de otorgamiento por parte del proponente seleccionado de la garantía de cumplimiento del contrato.

El artículo 2.2.1.2.3.1.9 del Decreto 1082 de 2015 establece la suficiencia de la garantía de seriedad de la oferta, determinando que debe estar vigente desde la presentación de la oferta y hasta la aprobación de la garantía de cumplimiento del contrato y su valor debe ser equivalente al diez por ciento (10%) del presupuesto oficial estimado del Proceso de Contratación.



Teniendo en cuenta el valor del presupuesto oficial definido, el Municipio no considera viable y conveniente establecer el valor de la garantía de seriedad de la oferta como criterio diferencial, ya que con ella se está garantizando entre otros el riesgo de no suscripción del contrato, siendo su porcentaje un factor determinante como mecanismo coercitivo de incumplimiento, así como reparatorio en caso de materialización del riesgo.

CRITERIOS DIFERENCIALES PARA EMPRENDIMIENTOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD:

Que atendiendo al artículo 2.2.1.2.4.2.7.3. Incorporación de criterios habilitantes diferenciales en favor de los emprendimientos y empresas de personas con discapacidad del Decreto 1082 de 2015 (adicionado por el artículo 1 del Decreto 0287 del 19 de marzo de 2026), que establece que en los procesos competitivos (licitación pública, selección abreviada y concurso de méritos) adelantados por entidades no sometidas al Estatuto General de Contratación de la Administración Pública, deberán establecer requisitos habilitantes diferenciales o ajustados en materia de experiencia, capacidad financiera u organizacional, o el valor de la garantía de seriedad de la oferta, con el fin de promover la participación de emprendimientos y empresas de personas con discapacidad con domicilio en el territorio nacional.

En virtud de lo anterior, la entidad procederá a efectuar el análisis correspondiente para determinar cuál (es) será (n) el (los) criterio(s) diferencial(es) para los emprendimientos y empresas de personas con discapacidad a fin de promover su participación en el proceso de selección que se adelantará, así:

a) Experiencia.

Que en razón a que la entidad requiere que los proponentes adjudicatarios cuenten con experiencias plurales y múltiples, que permitan evidenciar la suficiente idoneidad y la experiencia en la ejecución de diversos contratos y actividades prestación de servicios de conectividad similares a la que se pretenden adelantar, se considera por parte de la entidad, que este es un criterio determinante en el proceso y por tanto con la finalidad de beneficiar a los emprendimientos y empresas de personas con discapacidad, se establecerán condiciones más exigentes respecto a los proponentes que concurren al procedimiento de selección que no sean emprendimientos y empresas de personas con discapacidad y por lo tanto el criterio habilitante quedará de la siguiente manera en el proceso a adelantar:

Experiencia General Habilitante

La entidad como requisito mínimo habilitante solicita que el proponente acredite la experiencia con hasta dos (2) contratos celebrados con entidades públicas y/o privadas, cuyo objeto y/o alcance esté relacionado con la Adquisición, instalación, configuración y puesta en funcionamiento de soluciones de seguridad iguales y/o similares a las características solicitadas, cuyos valores finales o cuantías de los mismos sumados sea igual o mayor al cien por ciento (100 %) del presupuesto oficial asignado por la entidad, expresado en SMMLV, contratos que deben encontrarse reportados en el RUP, identificados en los códigos UNSPSC que se enuncian a continuación, hasta el tercer nivel:

Código	Nombre
43233200	Software de seguridad y protección
81111500	Ingeniería de software o hardware



En este sentido y como parte del análisis previo, se tendrán en cuenta como criterio diferencial para el proceso de selección para los **EMPRESARIOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD** así: Los proponentes que sean emprendimientos y empresas de personas con discapacidad, deberán acreditar la celebración, ejecución y liquidación con máximo tres (3) contratos celebrados con entidades públicas o privadas cuyo objeto y/o alcance esté relacionado con la Adquisición, instalación, configuración y puesta en funcionamiento de soluciones de seguridad iguales y/o similares a las características solicitadas, cuyos valores finales o cuantías de los mismos sumados sea igual o mayor al cien por ciento (100 %) del presupuesto oficial asignado por la entidad, expresado en SMMLV, contratos que deben encontrarse reportados en el RUP, identificados en los códigos UNSPSC que se enuncian a continuación, hasta el tercer nivel:

Código	Nombre
43233200	Software de seguridad y protección
81111500	Ingeniería de software o hardware

Tratándose de proponentes plurales, los criterios diferenciales solo se aplicarán si por lo menos uno de los integrantes acredite una participación no inferior al diez por ciento (10%) en el consorcio o la unión temporal, aportando la experiencia requerida, como mínimo, en una proporción equivalente a su participación en la conformación del proponente plural.

NOTA: En caso de acreditar su experiencia habilitante mediante este criterio diferencial, deberá manifestarlo de manera expresa en su oferta.

Se aclara que el factor diferencial para emprendimientos y empresas de personas con discapacidad es el número de contratos, los demás requisitos respecto de la acreditación de la experiencia serán de cumplimiento en su totalidad por el proponente.

b) Capacidad financiera y organizacional:

En cumplimiento del artículo 5 de la Ley 1150 de 2007, el artículo 2.2.1.1.1.5.3 del Decreto 1082 de 2015 y las directrices emitidas por Colombia Compra Eficiente, la Alcaldía de Tocancipá ha determinado los requisitos de Capacidad Financiera y Organizacional con base en el análisis del sector, evaluando las condiciones específicas del mercado del software de ciberseguridad (protección de endpoint, EDR, XDR y correo) y los riesgos asociados a la ejecución del contrato.

En atención a la Ley 2069 de 2020 (Ley de Emprendimiento) y al Decreto 1860 de 2021, la Entidad procedió a evaluar la procedencia de aplicar indicadores financieros y organizacionales diferenciales para las MiPymes de la siguiente manera:

- **Proporcionalidad de los Indicadores Generales:** Los indicadores exigidos para el presente proceso (Liquidez, Nivel de Endeudamiento, Cobertura de Intereses, Rentabilidad sobre el Patrimonio y Rentabilidad sobre el Activo) han sido calibrados a partir de la mediana del sector económico correspondiente según el RUP (Servicios de Tecnologías de la Información / Ciberseguridad), garantizando que no constituyan una barrera de entrada innecesaria para las Micro, Pequeñas y Medianas Empresas.
- **Aplicación de Medidas Diferenciales e Incentivos:** (Seleccionar la alternativa que aplique al proceso):
 - **Opción A** (Si el proceso se limita a MiPymes conforme al Art. 2.2.1.2.4.2.2 del Decreto 1082 de 2015): Al limitarse la convocatoria a MiPymes locales/nacionales, los indicadores de capacidad financiera exigidos han sido ajustados a los rangos mínimos razonables del



segmento MiPyme del sector TIC, permitiendo la acreditación del cumplimiento sin exigir métricas propias de la gran industria.

- Opción B (Si el proceso es de mayor cuantía o licitación/subasta abierta): En caso de concurrencia de MiPymes, se aplicará el puntaje adicional por promoción de la industria nacional y participación de MiPymes, conforme al artículo 2.2.1.2.4.2.14 del Decreto 1082 de 2015, manteniendo requisitos habilitantes proporcionales que eviten la restricción de la libre competencia

c) Valor de la garantía de seriedad de la oferta.

La garantía de seriedad de la oferta se exige a los proponentes para cubrir la sanción derivada del incumplimiento de la oferta, en los siguientes eventos:

- A. La no ampliación de la vigencia de la garantía de seriedad de la oferta cuando el plazo para la adjudicación o para suscribir el contrato es prorrogado, siempre que tal prórroga sea inferior a tres (3) meses.
- B. El retiro de la oferta después de vencido el plazo fijado para la presentación de las ofertas
- C. La no suscripción del contrato sin justa causa por parte del adjudicatario.
- D. La falta de otorgamiento por parte del proponente seleccionado de la garantía de cumplimiento del contrato.

El artículo 2.2.1.2.3.1.9 del Decreto 1082 de 2015 establece la suficiencia de la garantía de seriedad de la oferta, determinando que debe estar vigente desde la presentación de la oferta y hasta la aprobación de la garantía de cumplimiento del contrato y su valor debe ser equivalente al diez por ciento (10%) del presupuesto oficial estimado del Proceso de Contratación.

Teniendo en cuenta el valor del presupuesto oficial definido, el Municipio no considera viable y conveniente establecer el valor de la garantía de seriedad de la oferta como criterio diferencial, ya que con ella se está garantizando entre otros el riesgo de no suscripción del contrato, siendo su porcentaje un factor determinante como mecanismo coercitivo de incumplimiento, así como reparatorio en caso de materialización del riesgo.

FOMENTO A LA EJECUCIÓN DE CONTRATOS ESTATALES POR PARTE DE POBLACIÓN EN POBREZA EXTREMA, DESPLAZADOS POR LA VIOLENCIA, PERSONAS EN PROCESO DE REINTEGRACIÓN O REINCORPORACIÓN Y SUJETOS DE ESPECIAL PROTECCIÓN CONSTITUCIONAL.

Que atendiendo lo establecido en el artículo 2.2.1.2.4.2.16. del Decreto 1082 de 2015 (adicionado por el artículo 3 del Decreto 1860 del 24 de diciembre de 2021), que establece que en los Procesos de Contratación, las Entidades Estatales indistintamente de su régimen de contratación, fomentarán en los pliegos de condiciones o documento equivalente que los contratistas destinen al cumplimiento del objeto contractual la provisión de bienes o servicios por parte de población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional, garantizando las condiciones de calidad, sin embargo, teniendo en cuenta el objeto a contratar se considera que no es conveniente la aplicación de este fomento en el presente proceso de contratación ya que podría ser una limitación a la participación, pues el Municipio una vez consultadas las bases de datos de la Secretaría de Desarrollo Económico, Secretaria de Gobierno y la Secretaria de la Familia e Integración Social no cuenta con registros que permitan indicar que en este Municipio se encuentre domiciliada población especial con protección constitucional que



pueda suministrar los bienes y servicios requeridos por el Municipio dentro del presente proceso de contratación.

4.6. DEMANDA

En cumplimiento del artículo 2.2.1.1.6.1 del Decreto 1082 de 2015 y siguiendo las directrices del Modelo de Abastecimiento Estratégico de la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente (ANCP-CCE), la Alcaldía de Tocancipá adelantó la consulta y caracterización de la demanda estatal utilizando los tableros de control y herramientas de analítica de datos institucionales (disponibles en el portal Datos de Compra Pública / Abastecimiento Estratégico).

De la consulta realizada a los datos integrados del SECOP II y la Tienda Virtual para los códigos del Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC) 43233200 (Software de seguridad y protección) y 81111500 (Servicios informáticos / Ingeniería de software/hardware), se evidencia lo siguiente:

- Comportamiento y Tendencia de la Demanda: A nivel territorial y en el Departamento de Cundinamarca, las entidades públicas del orden municipal presentan un comportamiento de compra orientado a la transición de licenciamientos tradicionales de antivirus hacia ecosistemas integrados de ciberseguridad en la nube (SaaS). Las contrataciones promedio oscilan entre periodos de 12 meses para protección de endpoints, servidores y buzones corporativo.
- Histórico y Antecedentes Locales: Se verificó el histórico contractual del Municipio de Tocancipá (vigencias anteriores en antivirus y seguridad perimetral), evidenciando la necesidad de escalar hacia soluciones con capacidades correlacionadas de EDR (Endpoint Detection and Response), XDR (Extended Detection and Response) y Email Security para mitigar riesgos de ataques avanzados (Ransomware, Phishing y explotación de vulnerabilidades).
- Consolidación de Precios de Referencia: El análisis de la demanda a través de las bases de datos transaccionales de SECOP II permitió identificar contratos similares ejecutados por entidades territoriales y descentralizadas (tales como la Unidad de Restitución de Tierras - URT, TransMilenio S.A. y alcaldías de la subregión de Sabana Centro como Funza y Sopó), sirviendo como marco de referencia para estructurar las especificaciones del Anexo Técnico y corroborar la consistencia de los valores obtenidos en el estudio de mercado.

Los procesos de contratación presentados en la Administración municipal nos muestran que la demanda ha sido consistente y creciente por soluciones de Ciberseguridad enfocadas específicamente en la Protección Antivirus/Antimalware y en menor medida, en la Continuidad del Negocio (Backup y Recuperación), dentro del Municipio de Tocancipá; esto implica que la protección de ciberseguridad se debe enfocar en la interoperabilidad y los servicios de migración y configuración para evitar brechas de seguridad durante la transición.

En procesos de contratación del Municipio de Tocancipá relacionados con el objeto y/o alcance del presente proceso de selección se relacionan, entre otros, los siguientes:

PROVEEDOR	No. PROCESO	OBJETO	TIPO DE CONTRATO	TIPO DE PROCESO	CUANTÍA
CONSULTORIA TÉCNICA Y SERVICIOS DE INGENIERÍA COTEC SAS	CONTRATO 455 DE 2022	RENOVACIÓN DEL LICENCIAMIENTO DE SOFTWARE DE PROTECCIÓN ANTIVIRUS PARA LOS EQUIPOS DE CÓMPUTO DE PROPIEDAD DEL MUNICIPIO DE TOCANCIPÁ DURANTE TRES (3) AÑOS, PARA LAS	COMPRAVENTA	Menor Cuantía	\$ 49,368,000



		ESTACIONES DE TRABAJO WINDOWS (PC) Y SERVIDORES MS WINDOWS/ LINUX.			
FRONTECH S.A.S	CONTRATO 308 DE 2016	ADQUISICIÓN DE LICENCIA DE ANTIVIRUS ESET MAIL SECURITY PARA LAS CUENTAS DE CORREO EXCHANGE DEL MUNICIPIO DE TOCANCIPÁ POR 2 AÑOS	COMPRAVENTA	Contratación Directa	\$ 10,000,000
SERVICIO E INTEGRACION SAS	CMC 003 PMT 2020	SUMINISTRO, INSTALACIÓN Y CONFIGURACIÓN DE DIECIOCHO (18) LICENCIAS ANTIVIRUS PARA LOS EQUIPOS COMPUTO DE LA PERSONERÍA MUNICIPAL DE TOCANCIPÁ Y LOS QUE SE ENCUENTRAN EN COMODATO	Suministro	Mínima Cuantía	\$ 2,708,100
FRONTECH S.A.S.	CONTRATO 548 MT 2018	RENOVACIÓN ANTIVIRUS ESET ENDPOINT PROTECTION ADVANCE Y SOLUCIÓN DE BACKUP Y RECUPERACIÓN PARA ESTACIONES DE TRABAJO POR TRES (3) AÑOS	Compraventa	Contratación Directa	\$ 31,423,140

En este mismo sentido se utiliza un criterio de proximidad geográfica, relevancia económica y poblacional dentro del departamento de Cundinamarca; en los cuales se evidencia la tendencia a contratar Soluciones EDR, XDR y Antimalware, lo que marca la pauta de soluciones de endpoint que las entidades de todos los niveles (incluidos municipios) están buscando.

Mediante consultas realizadas en el SECOP II a través de Datos Abiertos, se ve reflejada la tendencia de la demanda hacia soluciones EDR (Endpoint Detection and Response), que ofrecen una protección mucho más avanzada contra ransomware y malware avanzado; de acuerdo con los procesos contractuales en la subregión Sabana Centro y el entorno de Cundinamarca, basada en los tipos de procesos recurrentes y la evidencia de Planes de Seguridad:

ITEM	MUNICIPIO	No. PROCESO	OBJETO	TIPO DE CONTRATO	TIPO DE PROCESO	CUANTÍA
1	MUNICIPIO DE MOSQUERA	SA-031-2025	PRESTACIÓN DE SERVICIOS PARA IMPLEMENTAR LA LICENCIA DE SOFTWARE QUE PERMITA LA DETECCIÓN Y REMEDIACIÓN DE VULNERABILIDADES Y AMENAZAS DE CIBERSEGURIDAD DE LA ALCALDÍA DE MOSQUERA.	PRESTACIÓN DE SERVICIOS	Menor Cuantía	\$ 85.848.500
2	MUNICIPIO DE GACHANCIPÁ	SASI 012-2025	ADQUISICIÓN DE 120 LICENCIAS DE SOFTWARE ANTIVIRUS CON CONSOLA DE ADMINISTRACIÓN CLOUD PARA LOS EQUIPOS DE CÓMPUTO DE LA ADMINISTRACIÓN DE GACHANCIPÁ Y ADQUISICIÓN DE UN PROXY FIREWALL PARA LA ADMINISTRACIÓN DE LA RED DE LA ALCALDÍA MUNICIPAL DE GACHANCIPÁ	SUMINISTROS	Selección abreviada subasta inversa	\$ 73.018.676
3	ALCALDIA MUNICIPAL FUSAGASUGA	SA 2024-0727	ADQUISICION E INSTALACION DE CORTAFUEGOS, SERVIDORES, ANTIVIRUS, LICENCIAMIENTO Y OTROS EQUIPOS TECNOLOGICOS Y PERIFERICOS CON EL PROPOSITO DE FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DE LA ALCALDÍA MUNICIPAL DE FUSAGASUGÁ.	COMPRAVENTA	Selección abreviada menor cuantía	\$ 492.418.928
4	ALCALDIA MUNICIPAL DE BOJACA	MC. 023-2025	ADQUISICIÓN DE LICENCIAS DE OFFICE 365, LICENCIAS DE ANTIVIRUS CORPORATIVO PARA PROVEER SERVICIOS DE SOFTWARE EN EQUIPOS DE CÓMPUTO DE LA ALCALDÍA DE BOJACÁ CUNDINAMARCA	COMPRAVENTA	Mínima Cuantía	\$ 29.999.025





5	ALCALDÍA MUNICIPAL DE SOPO	MC-022-2024	RENOVACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE 210 LICENCIAS DE SOFTWARE ANTIVIRUS BITDEFENDER GRAVITYZONE BUSINESS SECURITY, CON CONSOLA DE ADMINISTRACIÓN CLOUD Y RENOVAIÓN DE LA LICENCIA DE SEGURIDAD PERIMETRAL Y DE EQUIPO SOPHOS XG230 (FIREWALL) DE LA ALCALDÍA MUNICIPAL DE SOPO	COMPRAVENTA	Mínima cuantía	\$ 36.335.293
---	----------------------------	-------------	---	-------------	----------------	---------------

Links de Consulta de los procesos

ITEM	LINK DE CONSULTA
1	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.8922654&isFromPublicArea=True&isModal=true&asPopupView=true
2	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.8330157&isFromPublicArea=True&isModal=true&asPopupView=true
3	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7150930&isFromPublicArea=True&isModal=true&asPopupView=true
4	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.8710019&isFromPublicArea=True&isModal=true&asPopupView=true
5	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7182180&isFromPublicArea=True&isModal=true&asPopupView=true

4.7. ANÁLISIS DE PRECIOS DE MERCADO

De conformidad con lo establecido en el Decreto 1082 de 2015, la Alcaldía de Tocancipá analizó las condiciones del mercado y los mecanismos de agregación de demanda vigentes.

Revisada la Tienda Virtual del Estado Colombiano administrada por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente (ANCP-CCE), se constató que la entidad se encuentra en un periodo de transición tecnológica. Para la fecha de estructuración de este proceso, se encuentra en desarrollo la licitación pública del primer Acuerdo Marco de Precios exclusivo para el Sector de Ciberseguridad (Proceso CCENEG-094-1-2026). Al no estar este instrumento en operación definitiva con catálogo de precios unitarios disponibles para órdenes de compra directas, la Alcaldía de Tocancipá cuenta con la autonomía jurídica para acudir a las modalidades ordinarias de selección previstas en el Estatuto General de Contratación de la Administración Pública, garantizando la continuidad de la seguridad digital municipal.

Para determinar el presupuesto oficial bajo condiciones de libre competencia y pluralidad de oferentes, la entidad remitió solicitudes de cotización técnica y económica con base en especificaciones transversales (neutralidad tecnológica). Se recibieron y evaluaron formalmente las ofertas de los siguientes integradores especializados del mercado nacional: CORPORACIÓN MAESTRE SAS y ML TR3S SAS. Los análisis de los precios unitarios, al igual que otros Costos, se encuentran dentro del Documento Anexo "Estudio de Mercado".

Como resultado del estudio de mercado, se obtuvieron ofertas económicas válidas que reflejan las condiciones de precios del sector para la vigencia de ejecución. Con el fin de estructurar el presupuesto oficial bajo los principios de economía y responsabilidad fiscal, se tomó el promedio aritmético de las cotizaciones que se recibieron de las empresas CORPORACION MAESTRES SAS y ML TR3S SAS, dando como resultado un promedio que refleja el precio de mercado del servicio requerido por la Entidad.

COTIZACIONES PROVEEDORES		
ÍTEM	EMPRESA	COTIZACIÓN





1	CORPORACIÓN MAESTRE SAS	\$	97,784,343
2	ML TR3S SAS	\$	101,695,913
TOTAL, PRESUPUESTO		\$	99,740,128

Los análisis de los precios unitarios, al igual que otros Costos, se encuentran dentro del Documento Anexo "Estudio de Mercado".

5. ESTIMACION DE PRESUPUESTO OFICIAL

En cumplimiento de lo estipulado en el Decreto 1082 de 2015, la Alcaldía de Tocancipá adelantó el estudio económico de mercado para la adquisición, configuración y puesta en funcionamiento de las plataformas de ciberseguridad (EDR, XDR y protección de correo). Para el efecto, se remitieron solicitudes de cotización a firmas idóneas especializadas del sector tecnológico B2B, cuyo resultado se encuentra contenido dentro del Documento Anexo "Estudio de Mercado".

Se concluye que el presupuesto oficial estimado de acuerdo con el valor promedio de las cotizaciones recibidas asciende a la suma **NOVENTA Y NUEVE MILLONES SETECIENTOS CUARENTA MIL CIENTO VENTIOCHO PESOS M/CTE. (\$ 99.740.128)**. Este valor incluye todos los costos directos e indirectos, impuestos, tasas, contribuciones, retenciones, demás gravámenes, tarifas y erogaciones tanto del orden municipal, departamental y nacional, que se causen por el hecho de su celebración, ejecución y liquidación, y sean aplicables al valor del contrato a celebrar.

6. FORMA DE PAGO

El valor del contrato será por el valor de la propuesta que resulte ganadora.

El Municipio de Tocancipá pagará al contratista el valor total en un **ÚNICO PAGO** una vez entregados los servicios, previa suscripción del acta de inicio y el cumplimiento de los siguientes requisitos: i) Factura o cuenta de cobro. ii) Informe presentado por el contratista con soporte fotográfico acompañado de los respectivos soportes de entrega, debidamente recibido por el supervisor. iii) Certificación de ingreso de los bienes al Almacén General del Municipio iv) Certificación de cumplimiento a satisfacción expedida por el supervisor del contrato. v) Soportes del pago de aportes al Sistema Integral de Seguridad Social y pago de parafiscales. vi) Los demás documentos que sean necesarios para corroborar el cumplimiento de las obligaciones.

Si las facturas no reúnen los requisitos exigidos y presentan errores en los valores facturados, o de cualquier otra índole, serán devueltas al contratista sin tramitar y no correrán términos para su pago, situación que conoce y acepta el contratista.

7. ANÁLISIS DE RIESGOS

Matriz de Riesgos (elaborado conforme al Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación, expedido por la Agencia Nacional para la Contratación Pública - Colombia Compra Eficiente), el cual se determina de la siguiente manera:

Para los efectos previstos en el artículo 4 de la Ley 1150 de 2007, se entienden como riesgos involucrados en la contratación todas aquellas circunstancias que de presentarse durante el desarrollo y ejecución del contrato, tienen la potencialidad de alterar el equilibrio económico del contrato, pero que dada su previsibilidad se regulan en el marco de las condiciones inicialmente pactadas en los



contratos y se excluyen así del concepto de imprevisibilidad de que trata el artículo 27 de la Ley 80 de 1993. El riesgo será previsible en la medida que el mismo sea identificable y cuantificable en condiciones normales.

El Proponente deberá efectuar sus propias estimaciones y cálculos y, con fundamento en los mismos, adoptar la decisión de asumir la asignación de riesgos, así como la que se derive de las estipulaciones del Contrato de la naturaleza de este. Como consecuencia de lo anterior, no procederán reclamaciones del Contratista basadas en el acaecimiento de alguno de los riesgos que fueran asumidos por éste y consecuentemente El municipio de Tocancipá no hará reconocimiento alguno, ni se entenderá que ofrece garantía alguna al Contratista que permita eliminar o mitigar los efectos causados por la ocurrencia de alguno de los riesgos que se le asignan, salvo que dicho reconocimiento o garantía se encuentren expresamente pactadas en el CONTRATO.

En lo concerniente a los riesgos no asignados, el Contratista y El Municipio de Tocancipá se sujetarán a las normas y principios aplicables en materia de contratación estatal. Los riesgos previsibles derivados del CONTRATO han sido asignados de acuerdo con el principio según el cual: "Una asignación adecuada de los riesgos es aquella que minimiza el costo de su mitigación".

Esto se logra asignando cada riesgo a la parte que mejor lo controla criterio establecido por el Gobierno Nacional a través del Documento CONPES 3107 de 2001, en el cual también se señala: "Los principios básicos de la asignación de riesgos parten del concepto que estos deben ser asumidos: i) por la parte que esté en mejor disposición de evaluarlos, controlarlos y administrarlos, y/o; ii) por la parte que mejor disponga de los medios de acceso a los instrumentos de protección, mitigación y/o diversificación.

RIESGOS QUE ASUME EL CONTRATISTA: A partir de la fecha de suscripción del Contrato y en todas las etapas de este el Contratista asume los efectos derivados de todos y cada uno de los riesgos asociados a este Contrato, al igual que respecto a los que logre determinar, salvo los casos en que expresamente se ha determinado lo contrario. De este modo la práctica y la experiencia en la ejecución de contratos similares, ha demostrado que se debe tener en cuenta los siguientes riesgos previsibles los cuales deberán ser amparados por el Contratista, a saber, así:

TRIBUTARIO: Cuando el Estado Colombiano por motivos propios de sus decisiones y con respecto a la tributación de las entidades comerciales obligadas a ello, aumente porcentualmente el IVA.

LIQUIDEZ: Cuando por motivos la Empresa entre en un estado de iliquidez y no pueda cumplir con la totalidad del objeto del contrato.

COMERCIAL: Cuando por motivos comerciales no se pueda suministrar un elemento ya sea a nivel internacional, nacional o regional y la gestión para poder adquirirlo represente un gasto.

El Decreto 1082 de 2015 establece que el riesgo es 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"

Los artículos 2.2.1.1.1.6.1 y 2.2.1.1.1.6.2 del citado Decreto establecen la obligación para las entidades estatales de realizar, durante la etapa de planeación, el análisis de riesgo, por lo cual la entidad presenta, a continuación, la matriz de riesgos del presente proceso contractual.



La matriz de riesgos establecida tiene en cuenta los lineamientos dados en el "Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación", y que busca proteger a las entidades públicas de los eventos en el proceso de contratación, buscando reducir la probabilidad de ocurrencia del evento y de su impacto en el proceso de contratación.

De conformidad con el artículo 2.2.1.1.1.6.3 del Decreto 1082 de 2015, se identifican algunos riesgos que se pueden presentar en la ejecución del contrato que afectan el equilibrio económico del contrato, asociados con las obligaciones establecidas, contenidos en el Anexo No. 2.

Matriz de riesgos

8. GARANTIAS

De conformidad con lo reglamentado en el artículo 2.2.1.2.3.1.1. y siguientes del Decreto 1082 de 2015, con el fin de amparar los perjuicios de naturaleza contractual o extracontractual, derivados del incumplimiento total o parcial del contrato, como requisito para su ejecución, el contratista deberá constituir garantía única de cumplimiento que podrá consistir en contrato de seguro contenido en una póliza, patrimonio autónomo o garantía bancaria con los siguientes amparos:

Amparo	Vigencia
Cumplimiento	Término de duración del contrato y cuatro (4) meses más contados a partir de la fecha de expedición de la garantía y su valor debe ser del (10%) del valor del contrato.
Calidad del servicio	Término de duración del contrato y un (1) año más, contados a partir de la fecha de expedición de la garantía y su valor debe ser del (20%) del valor del contrato.
Calidad y correcto funcionamiento de los bienes	Término de duración del contrato y un (1) año más, contados a partir de la fecha de expedición de la garantía y su valor debe ser del (10%) del valor del contrato.
Pago de salarios, prestaciones sociales e indemnizaciones laborales	Término de duración del contrato y tres (3) años más, contados a partir de la fecha de expedición de la garantía y su valor debe ser del (5%) del valor del contrato.

9. ACUERDOS COMERCIALES

Para efectos del presente proceso de selección la Entidad determina la aplicabilidad del Acuerdo Comercial siguiendo las siguientes reglas en orden consecutivo:

Regla 1. La entidad debe verificar que el tratado esté vigente. Si el acuerdo comercial no lo está, este no es aplicable al proceso de contratación.

Regla 2. Si la entidad debe verificar si está incluida en el Acuerdo Comercial. Si la entidad lo está, el proceso de contratación, en principio, está cubierto por este y en consecuencia, es necesario continuar con la siguiente regla. En el evento de que la entidad no esté cubierta por el Acuerdo Comercial, en



principio, el proceso de contratación no estará cobijado por el mismo y, por tanto, no es necesario continuar con análisis adicional alguno.

En todo caso debe tenerse en cuenta que algunos Acuerdos comerciales incorporan obligaciones de trato nacional para entidades que en principio no están obligadas a todas las disposiciones del Acuerdo Comercial.

Regla 3. Si la entidad está incluida en el Acuerdo Comercial, debe verificar que el presupuesto oficial estimado del proceso de contratación sea igual o superior al valor a partir del cual el Acuerdo Comercial es aplicable; en dicho caso, el proceso de contratación, en principio estará cubierto por el Acuerdo Comercial y en consecuencia, la entidad deberá observarlo.

Regla 4. Si la entidad estatal está incluida en el Acuerdo Comercial y el valor estimado del proceso de contratación es igual o superior al valor a partir del cual el Acuerdo Comercial es aplicable, la entidad estatal debe determinar si hay excepciones que cobijen al proceso de contratación.

De conformidad con el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015 y siguiendo los lineamientos de la última versión del Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación expedido por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente, la Entidad determinó la aplicabilidad de los tratados internacionales vigentes para el presente proceso de selección.

Para las Entidades Estatales del nivel municipal (como la Alcaldía de Tocancipá), la aplicabilidad está restringida a los acuerdos donde las entidades subcentrales o territoriales fueron expresamente incluidas en las listas de cobertura y cuyos presupuestos oficiales superen los umbrales expresados en Derechos Especiales de Giro (DEG) o dólares (USD) liquidados para la vigencia.

Realizado el análisis consecutivo de las Reglas 1 a 4, se consolida la aplicabilidad en la siguiente matriz institucional:

ACUERDO COMERCIAL	ENTIDAD ESTATAL INCLUIDA (Regla 2)	PRESUPUESTO SUPERIOR AL UMBRAL (Regla 3)	EXCEPCIÓN APLICABLE (Regla 4)	PROCESO CUBIERTO POR EL ACUERDO
Comunidad Andina (CAN)	SI	N/A (Aplica sin umbral)	N/A	SI
Alianza Pacífico (Chile y Perú)	SI	NO (Presupuesto inferior)	NO	NO
Alianza Pacífico (México)	NO	NO	NO	NO
Canadá	NO	NO	NO	NO



ACUERDO COMERCIAL	ENTIDAD ESTATAL INCLUIDA (Regla 2)	PRESUPUESTO SUPERIOR AL UMBRAL (Regla 3)	EXCEPCIÓN APLICABLE (Regla 4)	PROCESO CUBIERTO POR EL ACUERDO
Chile (TLC Bilateral)	si	NO (Presupuesto inferior)	NO	NO
Corea	NO	NO	NO	NO
Costa Rica	SI	NO	NO	NO
Estados AELC (EFTA: Suiza, Noruega, Liechtenstein e Islandia)	si	NO (Presupuesto inferior)	NO	NO
Estados Unidos	NO	NO	NO	NO
México (TLC Bilateral)	NO	NO	NO	NO
Triángulo Norte (El Salvador y Honduras)	NO	NO	NO	NO
Triángulo Norte (Guatemala)	si	si	NO *Salvo que la convocatoria sea limitada a Mipyme	NO *Salvo que la convocatoria sea limitada a Mipyme
Unión Europea	si	NO (Presupuesto inferior)	NO	NO
Reino Unido de Gran Bretaña e Irlanda del Norte	si	NO (Presupuesto inferior)	NO	NO



ACUERDO COMERCIAL	ENTIDAD ESTATAL INCLUIDA (Regla 2)	PRESUPUESTO SUPERIOR AL UMBRAL (Regla 3)	EXCEPCIÓN APLICABLE (Regla 4)	PROCESO CUBIERTO POR EL ACUERDO
Israel	NO	NO	NO	NO

Para el presente análisis, y considerando que las plataformas de ciberseguridad de la Alcaldía corresponden a la adquisición de bienes y servicios tecnológicos de una entidad subcentral, se constata que el presupuesto oficial estimado del proceso no supera los umbrales mínimos obligatorios fijados para la vigencia por el Ministerio de Comercio Industria y Turismo – MINCIT y la agencia Nacional de Contratación Pública - Colombia Compra Eficiente, en consecuencia, el presente Proceso de Contratación está cobijado única y exclusivamente por los acuerdos comerciales de la Comunidad Andina de Naciones (CAN) (Decisión 439 de 1998) y Triángulo Norte (únicamente Guatemala, Salvo que la convocatoria sea limitada a Mipyme), el cual otorga trato nacional de manera automática sin umbral mínimo de cuantía. Las ofertas de bienes y servicios de los países miembros de la CAN (Bolivia, Ecuador y Perú) serán tratadas como ofertas de bienes y servicios colombianos para efectos de numeral 4.2 del Manual para el Manejo de los Acuerdos Comerciales en Procesos de Contratación¹.

En cumplimiento a los artículos 2.2.1.2.4.2.2 y 2.2.1.2.4.2.3 del Decreto 1082 de 2015 y teniendo en cuenta que según el Ministerio de Comercio Industria y Turismo – MINCIT y la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente el valor de los umbrales para la limitación de los procesos contractuales a MiPymes será el previsto por la norma equivalente a ciento veinticinco mil dólares de los Estados Unidos de América (US\$125.000) equivalente a \$511.708.497 y tendrá vigencia del 1 de enero del 2026 hasta el 31 de diciembre de 2026.²

Es por ello por lo que el proceso es susceptible de ser limitado a MIPYMES teniendo en cuenta que el presupuesto oficial estimado es de: **NOVENTA Y NUEVE MILLONES SETECIENTOS CUARENTA MIL CIENTO VENTIOCHO PESOS M/CTE. (\$ 99.740.128).**

10. DATOS GENERALES DEL PROCESO

El análisis del sector para la adquisición de plataformas de EDR/XDR, protección de email y protección de endpoints indica que las empresas buscan simplificar la defensa de su ecosistema digital. La principal conclusión es que el mercado valora las soluciones que ofrecen una visibilidad completa a través de una única interfaz. Esto significa que las organizaciones prefieren un proveedor que pueda unificar la detección y respuesta avanzada (EDR/XDR), el filtro de correo electrónico y la seguridad de los dispositivos finales en un solo sistema integrado. Este enfoque no solo facilita la operación diaria del equipo de seguridad, sino que también permite una correlación de eventos más rápida y precisa, teniendo en cuenta que las funcionalidades de automatización para la contención de amenazas y las capacidades predictivas son aspectos altamente considerados.

¹ Manual para el manejo de los Acuerdos Comerciales en Procesos de Contratación, numeral 4.2 https://www.colombiacompra.gov.co/wp-content/uploads/2024/08/manual_para_el_manejo_de_acuerdos_comerciales_vf.pdf

² Umbrales-2026.pdf. Colombia compra eficiente <https://www.colombiacompra.gov.co/wp-content/uploads/2024/10/Umbrales-2026.pdf>





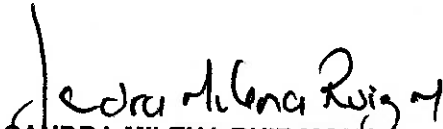
ALCALDÍA DE TOCANCIPÁ

El análisis sugiere, por lo tanto, que el éxito en este proceso recae en elegir una solución que maximice la cobertura de seguridad de forma eficiente, sin sobrecargar al equipo técnico con la gestión de herramientas desconectadas.

En este orden de ideas se determina que el valor del proceso debe estar justificado por la reducción de la superficie de ataque lograda a través de la unificación de EDR/XDR, protección de email y endpoints, y la capacidad de la solución para automatizar las tareas de respuesta, minimizando así el esfuerzo manual y el riesgo inherente a las herramientas fragmentadas. El valor, entonces, se basa más en el retorno de la inversión en eficiencia y mitigación de riesgos que en la suma simple de los componentes licenciados así:

PRESUPUESTO OFICIAL	NOVENTA Y NUEVE MILLONES SETECIENTOS CUARENTA MIL CIENTO VENTIOCHO PESOS M/CTE. (\$ 99.740.128).
PLAZO DE EJECUCIÓN	MAXIMO HASTA EL 31 DE DICIEMBRE
TIPO DE CONTRATO	COMPRAVENTA
MODALIDAD DE SELECCIÓN	PROCESO DE SELECCIÓN ABREVIADA POR EL PROCEDIMIENTO DE SUBASTA INVERSA ELECTRONICA
CÓDIGO UNSPC	43233200. Software de seguridad y protección 81111500. Ingeniería de software o hardware

De esta manera se ha elaborado el Análisis del Sector, acatando lo indicado por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente.


SANDRA MILENA RUIZ MONGADA
Secretaria Administrativa

Proyectó: Ing. Waldo Gómez Manrique - Profesional Universitario /SA 

