De conformidad con lo dispuesto en el artículo 25, numerales 7 y 12 de la Ley 80 de 1993, el Decreto 1082 de 2015 y la Ley 1882 de 2018, que determinan la base jurídica para la elaboración de los estudios y documentos previos a un proceso de selección y la consecuente celebración del contrato requerido.

## 1. DESCRIPCION DE LA NECESIDAD QUE LA ENTIDAD PRETENDE SATISFACER CON EL PROCESO DE CONTRATACIÓN

El Gobierno Nacional, expidió el Decreto No. 4173 del 3 de noviembre de 2011 "Por el cual se crea la Unidad Administrativa Especial Agencia del Inspector General de Tributos, Rentas y Contribuciones Parafiscales-ITRC, se fija su estructura y se señalan sus funciones.

La U.A.E. Agencia ITRC, como entidad de vigilancia y detección de fraude, tiene la competencia para auditar y conocer los procesos disciplinarios que se adelanten contra funcionarios de la UGPP, de la DIAN y de COLJUEGOS, es decir, la Agencia realiza las investigaciones de las conductas relacionadas con las faltas disciplinarias gravísimas, adelanta auditorías y formula recomendaciones sobre los procesos, acciones y operaciones de estas tres entidades vigiladas; por lo que necesita promover de manera oportuna acciones preventivas o correctivas, frente al riesgo de fuga de recursos económicos en la administración de tributos, aduanas, control del régimen cambiario de importaciones y exportaciones a cargo de las entidades mencionadas. Asimismo, promueve las buenas prácticas y detecta las fallas en los procesos y procedimientos, en la seguridad digital y en los recaudos e ingresos que administran las entidades auditadas.

La estrategia institucional de la U.A.E. Agencia ITRC, busca articular la tecnología con los objetivos estratégicos institucionales, los objetivos sectoriales, el Plan Nacional de Desarrollo y los lineamientos de Gobierno Digital del Min Tic, teniendo como base las iniciativas de optimización tecnológica de la Entidad. El Plan Estratégico de Tecnologías de la Información de la Agencia ITRC, tiene como propósito principal alinear la gestión de TI con la misión, visión y objetivos estratégicos de la entidad, estableciendo la hoja de ruta de implementación de proyectos relacionados con las tecnologías de la información y las comunicaciones – TIC, al permitir su avance en la implementación de la Política de Gobierno Digital, articulado al modelo integrado de planeación y gestión (MIPG) y en los habilitadores de arquitectura, servicios ciudadanos digitales y seguridad y privacidad de la información, que agrega valor a los distintos grupos de interés de la entidad.

Desde el área de Tecnologías de la Información de la Agencia ITRC se contribuye directamente al cumplimiento de la labor misional del Estado, mediante el fortalecimiento de los sistemas de información y la protección del patrimonio

público frente a amenazas como el fraude y la corrupción. A través de soluciones tecnológicas integrales incluyendo infraestructura, licenciamiento, seguridad y soporte se apoya la operación institucional y se promueve la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), en cumplimiento con los lineamientos del MinTIC.

La operación de la Agencia depende de servicios tecnológicos que soportan las comunicaciones, el correo electrónico, la conectividad y el acceso a los sistemas de información. En consecuencia, una afectación de estos servicios por incidentes de ciberseguridad puede limitar la continuidad de los procesos misionales y administrativos, retrasar la atención de actuaciones institucionales, comprometer información y generar impactos operativos, jurídicos, reputacionales y económicos.

En este contexto, la seguridad informática se posiciona como un habilitador estratégico, siendo esencial para garantizar la confidencialidad, integridad y disponibilidad de los datos misionales y administrativos. La creciente sofisticación de las amenazas digitales como el ransomware, phishing y la denegación de servicio exige soluciones avanzadas que permitan una protección efectiva y adaptable.

Dado que el ciberespacio ha sido reconocido como un nuevo dominio estratégico en los conflictos globales, las entidades públicas deben fortalecer sus capacidades de defensa digital. En particular, es prioritario integrar herramientas basadas en Inteligencia Artificial (IA) en sus sistemas de seguridad perimetral, con el fin de detectar y responder en tiempo real a ciberataques, mediante algoritmos de aprendizaje automático que optimizan el análisis de datos y la toma de decisiones.

Actualmente, la Agencia ITRC dispone de una solución de seguridad basada en inteligencia artificial que opera en el entorno de correo electrónico y en la red corporativa. La herramienta apoya la identificación de comportamientos anómalos, la priorización de alertas y la respuesta frente a eventos que puedan representar amenazas para los activos de información.

La implementación de soluciones de IA contribuye al cumplimiento de lineamientos gubernamentales y estándares internacionales de ciberseguridad, como el Marco Nacional de Ciberseguridad o el NIST Cybersecurity Framework.

Actualmente, la Agencia ITRC dispone de una solución de seguridad basada en inteligencia artificial que opera en el entorno de correo electrónico y en la red corporativa. La herramienta apoya la identificación de comportamientos

anómalos, la priorización de alertas y la respuesta frente a eventos que puedan representar amenazas para los activos de información.

La vigencia del licenciamiento es temporal y su terminación puede ocasionar la pérdida de las capacidades asociadas a la detección, análisis y respuesta automatizada, así como de las actualizaciones, el soporte especializado y el mantenimiento del fabricante. Por ello, se requiere asegurar la continuidad del licenciamiento y de los servicios asociados, evitando periodos sin cobertura y preservando la configuración e integración existentes.

**Evidencia sobre exposición y dependencia digital**

Las cifras oficiales confirman que la necesidad identificada no corresponde a un riesgo hipotético. El Ministerio de Tecnologías de la Información y las Comunicaciones informó que Colombia enfrentó cerca de treinta y seis mil millones (36.000 millones) de intentos de afectación durante 2024, equivalentes al 17 % de los intentos registrados en Latinoamérica, circunstancia que ubicó al país como el segundo más atacado de la región. Este volumen evidencia un entorno de amenaza masivo y persistente, frente al cual las entidades públicas deben disponer de capacidades de detección, análisis y respuesta que operen de manera continua.

De acuerdo con el Informe de Tendencias de Amenazas Cibernéticas 2025 divulgado por el MinTIC y el ColCERT, se gestionaron 1.427 incidentes de seguridad digital en 2024 y 697 en 2025, lo que representó una reducción del 48,84 %. El propio informe aclara que esta disminución refleja una mayor preparación de la infraestructura digital y no una reducción de la actividad criminal. Asimismo, advierte el aumento de amenazas persistentes avanzadas y de ataques apoyados en inteligencia artificial contra sectores estratégicos y entidades públicas.

La información del ColCERT resulta especialmente pertinente para el alcance previsto sobre correo electrónico: el fraude representó el 79,83 % de los incidentes observados durante los dos últimos años, con 835 casos asociados a phishing y 784 casos de uso no autorizado de cuentas de correo electrónico.

Estas cifras respaldan la necesidad de mantener capacidades especializadas para analizar comportamientos anómalos, proteger buzones institucionales, priorizar alertas y responder oportunamente ante compromisos de identidad o de credenciales.

Considerando el crecimiento sostenido y la creciente complejidad de los sistemas de información y servicios tecnológicos de la Entidad, se hace indispensable complementar y reforzar estas capacidades con herramientas de detección y respuesta basadas en inteligencia artificial igualmente robustas y especializadas, que garanticen la protección integral de la información.

En este contexto, la adopción de soluciones avanzadas de IA se vuelve crítica para la operación institucional, ya que permite mitigar de forma continua los riesgos tecnológicos que podrían comprometer la disponibilidad, integridad y confidencialidad de los datos y servicios. La afectación de dichos activos no solo representa una amenaza técnica, sino que también podría impactar negativamente la misionalidad de la Agencia y el cumplimiento de sus objetivos estratégicos y tecnológicos.

**Brecha y problema que debe atenderse**

La protección basada únicamente en reglas, firmas o análisis manual resulta insuficiente frente a amenazas que cambian rápidamente, utilizan credenciales legítimas, explotan aplicaciones expuestas o adoptan técnicas de evasión. La complejidad de la infraestructura tecnológica y el volumen de eventos de seguridad demandan capacidades que permitan analizar patrones de comportamiento, correlacionar señales y advertir oportunamente desviaciones tanto en la red como en el correo electrónico.

Actualmente, la UAE Agencia ITRC cuenta con una solución de Inteligencia Artificial (IA) implementada, la cual se encuentra operativa tanto en el entorno de correo electrónico como en la red corporativa. Esta herramienta permite una gestión integral y continua de diversas amenazas cibernéticas, mediante la identificación de comportamientos anómalos y la respuesta automatizada frente a posibles incidentes de seguridad.

La necesidad no se limita a la adquisición de una licencia. Comprende la disponibilidad continua de una capacidad tecnológica integral que incluya activación, actualización, configuración, soporte, mantenimiento, garantía y acompañamiento especializado durante doce (12) meses apoyada con un conjunto de estrategias, procesos y herramientas de ciberseguridad diseñado para detectar, monitorear y bloquear la exfiltración o el uso no autorizado de información confidencial. Estos componentes son necesarios para mantener la solución operativa, atender incidentes y ajustar su funcionamiento conforme evolucionen los riesgos y el entorno tecnológico institucional.

El licenciamiento deberá conservar la interoperabilidad con el entorno tecnológico de la Agencia y contemplar actualizaciones durante toda su vigencia, soporte técnico especializado, mantenimiento preventivo y correctivo, garantía del fabricante y acompañamiento para la activación y configuración. La entrega deberá realizarse de manera que no se presenten interrupciones entre la vigencia actual y la nueva cobertura contractual.

Con la contratación se espera mantener la continuidad de las capacidades de ciberseguridad de la Agencia; mejorar la detección temprana y la priorización de eventos; reducir los tiempos de análisis y respuesta; fortalecer la protección de la red, el correo electrónico y la información institucional; y disponer de soporte y actualizaciones durante la vigencia del licenciamiento.

## 2. OBJETO A CONTRATAR

### 2.1. OBJETO

Adquirir un licenciamiento por (12) meses para la prevención de ciber amenazas con IA (Inteligencia Artificial) y DLP (Prevención de perdida de datos), incluido soporte y mantenimiento de la red corporativa de la agencia ITRC.

El bien o servicio objeto del presente proceso de selección está codificado en el clasificador de Bienes y Servicios UNSPSC, como se indica a continuación:

| Código Segmento | Código Familia | Código Clase | Código Producto | Nombre Producto |
|---|---|---|---|---|
| 43 | 4323 | 432330 | 43233000 | Software de entorno operativo. |
| 43 | 4323 | 432332 | 43233200 | Software de seguridad y protección. |
| 81 | 8111 | 811122 | 81112200 | Mantenimiento y soporte de software. |
| 81 | 8111 | 811118 | 81111800 | Servicios de sistemas y administración de componentes de sistemas. |

### 2.2. ALCANCE

Adquirir un licenciamiento anual de prevención de ciber amenazas con IA y DLP, incluido soporte y mantenimiento, destinado a fortalecer la seguridad digital de

la Agencia ITRC. Este licenciamiento incluirá soporte técnico especializado y mantenimiento integral durante toda su vigencia.

El alcance contempla los siguientes componentes:

- Detección y neutralización de amenazas en tiempo real, tanto a nivel de red (NDR) como de correo electrónico, mediante algoritmos de inteligencia artificial autoaprendibles.
- Prevención de perdida de datos DLP, integrado con la plataforma de correos de IA para 200 cuentas
- Servicio de actualizaciones continuas, garantizando la evolución constante frente a nuevas amenazas y vulnerabilidades.
- Soporte técnico especializado, disponible durante todo el periodo contratado.
- Mantenimiento preventivo y correctivo, asegurando la operatividad y estabilidad de la solución.
- Garantía del fabricante, válida durante la vigencia del licenciamiento, que respalde el funcionamiento adecuado de la herramienta.

Esta iniciativa busca fortalecer la postura de ciberseguridad institucional, alineándose con los estándares internacionales y las exigencias regulatorias vigentes.

| Item | Descripción | Cantidad | Tiempo |
|---|---|---|---|
| 1 | Darktrace módulo de red | 250 | 12 meses |
| 2 | Darktrace EMAIL/365 | 200 | 12 meses |
| 3 | Darktrace DLP | 200 | 12 meses |
| **Soporte** | | | |
| 4 | NDR-SPT-7x24-CT-CIB-12 | 1 | 12 meses |

## 2.3. OBLIGACIONES DEL CONTRATISTA

## A.- OBLIGACIONES GENERALES DEL CONTRATISTA:

1. Además de las establecidas en la ley, el contratista deberá cumplir con el objeto y obligaciones establecidas en el contrato de manera oportuna y eficiente con personal calificado, debidamente entrenado y con los equipos y demás especificaciones ofrecidas en la propuesta aplicando toda su experiencia e idoneidad.

2. Colaborar con la U.A.E. Agencia ITRC para que el objeto contratado se cumpla y garantizar que sea en condiciones óptimas de calidad.

3. Presentar la documentación completa requerida por la Agencia ITRC, conforme lo exige la Ley, cumpliendo con todos los requisitos.

4. Dar curso a las directrices impartidas por el Supervisor del contrato.

5. Suministrar al Supervisor toda la información requerida para el ejercicio oportuno de su gestión y proveer, al inicio y culminación de cada fase, los reportes escritos sobre la ejecución del contrato.

6. Para el desembolso de los pagos pactados se requiere la presentación de la constancia expedida por el revisor fiscal en relación con el pago de aportes a los sistemas de seguridad social a que haya lugar por parte del contratista, así como el pago de los parafiscales.

7. Realizar los actos necesarios y tomar las medidas conducentes para el debido y oportuno cumplimiento de sus obligaciones contractuales y la ejecución del presente contrato. Responder por sus actuaciones y omisiones derivadas de la ejecución del contrato, conforme lo establecido en las leyes 80 de 1993 y 1150 de 2007, Decreto 1082 de 2015 y Ley 1882 de 2018.

8. Constituir oportunamente la póliza con el amparo de los riesgos solicitados. (Si ello procede)

9. Responder por el cuidado de los bienes entregados por la Agencia para ejecutar el presente contrato. (si ello procede).

10. Entregar al vencimiento del plazo de ejecución del presente contrato los bienes y elementos que le fueron entregados (si ello procede).

11. No instalar ni utilizar en los equipos asignados por la AGENCIA para ejecutar el objeto contractual, ningún software sin la autorización previa de la AGENCIA (Si ello procede).

12. No retirar el software de la Agencia ITRC y limitar su uso a las actividades propias del presente contrato, salvo autorización previa y expresa. (Si ello procede).

13. No introducir modificación alguna al software instalado, sin la autorización previa y escrita de la Agencia ITRC (si ello procede).

14. Implementar acciones de gestión ambiental que garanticen primordialmente el cumplimiento de los objetivos de ecoeficiencia, de acuerdo con la normatividad ambiental vigente (si ello procede); así mismo y de acuerdo con el Decreto 1072 de 2015, deberán contar un Sistema de Gestión de la Seguridad y Salud en el Trabajo en su entidad.

15. Las demás necesarias para el cumplimiento del objeto, que se desprendan de la naturaleza de este.

**B.- OBLIGACIONES ESPECÍFICAS**

1. Cumplir integralmente las especificaciones, cantidades, coberturas, vigencias, entregables y condiciones de aceptación establecidas en el estudio previo y el anexo técnico.

2. Hacer entrega del certificado de la licencia IA y DLP objeto del presente contrato conforme a las especificaciones técnicas, en un término de tiempo máximo de treinta (30) días calendario.

3. Realizar la actualización y configuración del software (IA) que se requieran dentro del proceso de actualización.

4. Prestar el servicio de soporte técnico para las herramientas adquiridas dentro del período definido en las especificaciones técnicas.

5. Efectuar los mantenimientos y actualizaciones, según lo acordado entre el contratista y el supervisor del contrato, conforme a lo establecido en las especificaciones técnicas.

6. Prestar el soporte en modalidad remota y, cuando la naturaleza del incidente lo requiera y exista coordinación previa con el supervisor, de manera presencial en la ciudad de Bogotá.

7. Mantener la garantía de los nuevos componentes entregados por el período definido en las especificaciones técnicas.

8. Garantizar la vigencia y operatividad del licenciamiento de IA de acuerdo con lo indicado en el anexo técnico, contados a partir de la fecha de activación indicada por la Agencia ITRC. Es importante resaltar, que la Entidad cuenta actualmente con el licenciamiento vigente hasta el mes de agosto, por lo que el proveedor debe apoyar y habilitar estos componentes tan pronto terminen las vigencias mencionadas.

9. Entregar al supervisor un inventario de las licencias y coberturas activadas, que identifique como mínimo el componente, cantidad, fecha de inicio, fecha de terminación, número de contrato o certificado y canal de soporte.

10. Garantizar que todo el personal empleado para el desarrollo del objeto del contrato cuenta con el conocimiento suficiente para llevar a cabo las actividades contratadas.

11. Cumplir las políticas de seguridad y privacidad de la información de la Agencia, las disposiciones sobre protección de datos personales y los lineamientos de seguridad digital aplicables durante toda la ejecución.

12. Al finalizar la ejecución, entregar un informe de cierre con el estado de las licencias, casos de soporte atendidos, asuntos pendientes y recomendaciones de continuidad; igualmente, devolver o eliminar de forma segura la información y los accesos temporales proporcionados por la Agencia.

## 2.4. LUGAR DE EJECUCIÓN

Se tendrá como lugar de ejecución del presente contrato las oficinas de la Unidad Administrativa Especial Agencia del Inspector General de Tributos, Rentas y Contribuciones Parafiscales-ITRC, en la ciudad de Bogotá.

## 2.5. PLAZO

El plazo de ejecución del contrato será de treinta (30) días calendario, contados a partir de la fecha de suscripción del acta de inicio, una vez se hayan cumplido

los requisitos de perfeccionamiento y ejecución establecidos. Sin exceder de 30 de diciembre de 2026.

Durante dicho periodo, se realizará la entrega del certificado y las credenciales de acceso correspondientes, mediante acta en la que se dejará constancia de la fecha de activación del licenciamiento, el cual tendrá una vigencia de doce (12) meses para los componentes aplicables. Esta activación permitirá a la Agencia acceder a los servicios tecnológicos contratados, con el respaldo y validación del personal técnico de la Oficina de Administración de Tecnologías de la Información – OATI.

### 2.6. SUPERVISOR

El seguimiento y control del presente contrato será ejercido por el jefe de la Oficina Asesora de Tecnología de la Información – OATI, quien será el encargado de coordinar, disponer e informar todo lo inherente al contrato y vigilar el estricto cumplimiento de su objeto.

## 3. MODALIDAD DE SELECCIÓN DEL CONTRATISTA Y SU JUSTIFICACIÓN, INCLUYENDO LOS FUNDAMENTOS JURIDICOS

El procedimiento de selección del contratista está sometido a los principios de transparencia, selección objetiva e igualdad de derechos y oportunidades de los que se deriva la obligación de someter a todos los oferentes a las mismas condiciones definidas en la ley y en el pliego de condiciones. Cabe recordar que los pliegos de condiciones forman parte esencial del contrato; son la fuente de derechos y obligaciones de las partes y elemento fundamental para su interpretación e integración, pues contienen la voluntad de la administración a la que se someten los proponentes durante el proceso de selección y el oferente favorecido durante el mismo lapso y, más allá, durante la vigencia del contrato.

El contrato por suscribir estará sometido a la legislación y jurisdicción colombiana y se rige por las normas de la Ley 80 de 1993, Ley 1150 de 2007, y Decreto 1082 de 2015 y las demás normas que la complementen, modifiquen o reglamenten y por las normas civiles y comerciales que regulen el objeto del contrato.

Ley 1150 de 2007 Literal g), numeral 4 del artículo 2, determina: "Contratación directa. La modalidad de selección de contratación directa solamente procederá en los siguientes casos: (...) g) Cuando no exista pluralidad de oferentes en el mercado".

1) Decreto 1082 de 2015: Artículo 2.2.1.2.1.4.8. Contratación directa cuando no exista pluralidad de oferentes. Se considera que no existe pluralidad de oferentes cuando existe solamente una persona que puede proveer el bien o el servicio por ser titular de los derechos de propiedad industrial o de los derechos de autor, o por ser proveedor exclusivo en el territorio nacional

De acuerdo con lo anterior y en cumplimiento de las disposiciones de la ley 1150 de 2007 y el Decreto 1082 de 2015, así como la cuantía de contratación, se establece que este proceso de selección corresponde a **SELECCIÓN ABREVIADA- SUBASTA INVERSA**.

## 4. VALOR ESTIMADO DEL CONTRATO Y JUSTIFICACIÓN.

De conformidad con el Título I, Subsección 6 "Análisis del Sector Económico y de los oferentes por parte de las Entidades Estatales", Artículo 2.2.1.1.1.6.1 "Deber de análisis de las Entidades Estatales", y la Sección II, Subsección 1 "Planeación", Artículo 2.2.1.1.2.1.1 "Estudios y documentos previos" en el numeral 4, del Decreto 1082 de 2015, la U.A.E. Agencia ITRC realiza el siguiente análisis del sector, identificando que el sector del cual hace parte el objeto contractual es el de Tecnologías de la Información (TI) y el subsector es Software y Servicios Asociados.

### 4.1. ANALISIS DEL SECTOR, EL CUAL SOPORTA EL VALOR ESTIMADO DEL CONTRATO.

El alcance del estudio de sector debe ser proporcional al valor del proceso de contratación, la naturaleza del objeto a contratar, el tipo de contrato y a los riesgos identificados para el proceso de contratación.

El análisis del sector cubre tres áreas:

**A. Aspectos Generales**

La presente contratación se enmarca en el sector terciario de la economía, más conocido como el sector servicios, específicamente en el subsector de desarrollo de sistemas informáticos, consultoría informática y actividades relacionadas. La industria del software en Colombia es fundamental para el desarrollo económico y tecnológico del país, requiriendo una alta inversión en investigación, desarrollo y formación de profesionales.

Actualmente, Colombia se encuentra posicionado como el cuarto mercado de TI más grande en Latinoamérica, con segmentos destacados como aplicaciones e infraestructura TI. El país ha avanzado significativamente en políticas de inteligencia artificial, impulsando un notable crecimiento en las ventas de software de seguridad y plataformas de IA.

Según el IBM X-Force Threat Intelligence Index 2024, los países más atacados en América Latina durante 2023 fueron: Brasil: 68% de los incidentes, Colombia: 17% y Chile: 8%.

En América Latina, las tácticas más comunes de los ciberdelincuentes incluyeron el uso de credenciales válidas para acceder a sistemas, explotación de aplicaciones públicas y campañas de phishing. Los sectores más afectados fueron retail, finanzas y seguros.

En el entorno global, los sistemas de Inteligencia Artificial (IA) en ciberseguridad, se han diseñado para colaborar, categorizando los ataques según el nivel de amenaza; los encargados de ciberseguridad, por su parte, asignan la prioridad con que se debe atender cada uno, iniciando por los más peligrosos para la información de la empresa. Los ataques de tipo malware y otros que puedan surgir, también evolucionan, lo que hace que las amenazas sean más rápidas y sofisticadas. Es por esto por lo que el "Machine learning" se convierte en actor fundamental para estar al mismo nivel del delito y a preparación institucional.

En la actualidad, la mayoría de las investigaciones y avances importantes en la industria de ciberseguridad, provienen de la subdisciplina IA denominada Machine Learning, que se centra en la aplicación de algoritmos derivados de los datos. De esta premisa, se derivan dos esquemas asociados a la relación de la IA y la ciberseguridad como son: los definidos por los analistas (ingenieros de seguridad o infraestructura) y los definidos por las máquinas.

Los analistas crean protocolos y reglas según su experiencia, sin embargo, se pueden encontrar con problemas cuando aparece una amenaza nueva o desconocida, conllevando más esfuerzo, tiempo, riesgos, implicaciones jurídicas, económicas, etc. De otra parte, las máquinas aplican sus protocolos de seguridad según la información adquirida por el "Machine Learning" y "Deep Learning", en los cuales tienen influencia directa los patrones de comportamiento en redes para predecir movimientos y ataques a futuro, sistemas operativos utilizados, servidores, estructuras de seguridad, las acciones de los usuarios y las tácticas de respuesta.

Como se observa, estos dos esquemas refuerzan el concepto de complementariedad entre ambos: el hombre y la máquina.

**B. Estudio de la oferta**

Los proveedores de este sector que aplican para este proyecto se caracterizan por las siguientes condiciones debido a que estos bienes y/o servicios son importados:

- Empresas que tienen líneas exclusivas de productos con un fabricante internacional. (Resellers/Partners).
- Empresas que venden estos productos indistintamente de la marca en particular.

Estos proveedores generalmente también ofrecen a la venta bienes, servicios y/o componentes, software, configuraciones, consultorías, soporte, servicios especializados entre otros, los cuales son complementarios a las implementaciones de las soluciones tecnológicas y que en la mayoría de las veces son necesarios para las entidades que lo requieren.

Estos proveedores tienen una dinámica de producción, distribución y entrega de bienes y servicios, basada en que:

- No producen estos bienes tecnológicos ya que son importados.
- Son distribuidores de estos bienes, razón por la cual debe pasar previamente por un proceso de nacionalización.
-

Con respecto a la entrega de bienes y servicios, estos proveedores se caracterizan por disponer de una serie de recursos que, adicionalmente a la venta de equipos y componentes, pueden contribuir con las configuraciones necesarias para cada organización o establecer proyectos para análisis, diseño/rediseño, definición de arquitecturas relacionadas a la infraestructura de transmisión de datos y servicios, y profesionales especializados.

## Gamma Ingenieros

| COTIZACION GAMMA INGENIEROS SAS | | |
|---|---|---|
| HARDWARE | | |
| **Item** | **Especificaciones** | **Valor (12 meses)** |
| **Darktrace Modulo Red** | Renovación Darktrace 250 usuarios | $ 105.584.620,68 |
| **CLOUD** | | |
| **Darktrace Mail** | Renovación Darktrace Email/office365 - 200 cuentas | $ 124.902.828,00 |
| | Darktrace/DLP - 200 cuentas | |
| **SERVICIOS** | | |
| **NDR-SPT-7x24-CT-CIB-12** | Soporte 7x24 por 12 meses para la plataforma de detección y respuesta de red NDR | $ 19.524.758,40 |
| | **TOTAL** | **$ 250.012.207,08** |

## E&C Ingenieros

| COTIZACION E&C Ingenieros | | |
|---|---|---|
| HARDWARE | | |
| **Item** | **Especificaciones** | **Valor (12 meses)** |
| **Darktrace Modulo Red** | Renovación Darktrace 250 usuarios | $ 107.907.482,33 |
| **CLOUD** | | |
| **Darktrace Mail** | Renovación Darktrace Email/office365 - 200 cuentas | $ 127.650.690,22 |
| | Darktrace/DLP - 200 cuentas | |
| **SERVICIOS** | | |
| **NDR-SPT-7x24-CT-CIB-12** | Soporte 7x24 por 12 meses para la plataforma de detección y respuesta de red NDR | $ 19.954.303,08 |
| | **TOTAL** | **$ 255.512.475,63** |

## WEXLER

| COTIZACION WEXLER | | |
|---|---|---|
| HARDWARE | | |
| **Item** | **Especificaciones** | **Valor (12 meses)** |
| **Darktrace Modulo Red** | Renovación Darktrace 250 usuarios | $ 107.379.559,23 |
| **CLOUD** | | |
| **Darktrace Mail** | Renovación Darktrace Email/office365 - 200 cuentas | $ 127.026.176,08 |
| | Darktrace/DLP - 200 cuentas | |
| **SERVICIOS** | | |
| **NDR-SPT-7x24-CT-CIB-12** | Soporte 7x24 por 12 meses para la plataforma de detección y respuesta de red NDR | $ 19.856.679,29 |
| | **TOTAL** | **$ 254.262.414,60** |

## C. Estudio de la demanda

La entidad ha considerado las condiciones en las cuales ha adquirido anteriormente, el bien o servicio objeto del proceso de contratación y como lo han hecho otras entidades estatales. Igualmente, se tienen en cuenta otras variables como los precios del dólar con respecto a los años anteriores, necesidades y desarrollos actuales sobre la herramienta.

Con respecto a la entrega de servicios, estos proveedores se caracterizan por disponer de recursos especializados que contribuyen a optimizar las configuraciones necesarias o establecer proyectos de análisis, diseño/rediseño y definición de arquitecturas relacionadas con la infraestructura tecnológica que soporta los datos y servicios.

La entidad ha adquirido en los últimos 3 años, el servicio objeto del proceso de contratación, así:

Agencia ITRC
**Proceso estimado total:** $319.994.570.
**Numero de proceso:** CTO 067 de 2024
**Objeto:** Renovación del licenciamiento de la solución de seguridad Perimetral – FORTINET de la Agencia ITRC, incluyendo detección de amenazas con inteligencia artificial, servicio de actualización, soporte técnico y mantenimiento, durante el tiempo de vigencia del licenciamiento, con cambio de partes (si se requiere) y garantía por parte del fabricante durante su vigencia.

De conformidad con Sección II, Subsección 1 "Planeación", Artículo 2.2.1.1.2.1.1 "Estudios y documentos previos" en el numeral 4, del Decreto 1082 de 2015 y haciendo uso del SECOP II, para verificar otras contrataciones con el mismo objeto contractual y estudios efectuados, se encontraron los siguientes procesos:

**Consultas en SECOP:**

| | |
|---|---|
| **No. PROCESO SECOP II** | MC-080-CENACTELEMATICA-2025 |
| **CONTRATANTE** | CENTRAL ADMINISTRATIVA Y CONTABLE TELEMATICA (EJERCITO NACIONAL) |
| **OBJETO** | MANTENIMIENTO Y SOPORTE TECNICO DE LA PLATAFORMA DARKTRACE DEL BATALLON DE CIBERDEFENSA Y CIBERSEGURIDAD DEL EJERCITO NACIONAL" A EJECUTAR EN LA VIGENCIA 2025. |
| **TOTAL** | $116.752.580,00 |

| | |
|---|---|
| **No. PROCESO SECOP II** | MJD-SAMC-001-2025 |
| **CONTRATANTE** | Ministerio de Justicia y del Derecho |
| **OBJETO** | Implementación de soluciones de ciberseguridad basadas en inteligencia artificial, enfocadas en la protección de datos y sistemas institucionales. |

| | |
|---|---|
| **TOTAL** | $126.126.403,00 |

| | |
|---|---|
| **No. PROCESO SECOP II** | IPR-008-26 |
| **CONTRATANTE** | FONDO NACIONAL DE GARANTIAS S.A. - FNG |
| **OBJETO** | Prestar el servicio de renovación, soporte y mantenimiento de la plataforma de contención de eventos de ciberseguridad basada en inteligencia artificial Darktrace |
| **TOTAL** | $ 672.805.103 |

### 4.2. VALOR

El presupuesto para el contrato que se derive del presente procedimiento de selección, se estima en la suma de **DOCIENTOS CINCUENTA MILLONES DE PESOS M/CTE (250.000.000,00)**, y todos los costos directos e indirectos y los impuestos, tasas y contribuciones que conlleven la celebración y ejecución total del contrato que resulte del presente proceso de selección el cual se encuentra amparado por el Certificado de Disponibilidad Presupuestal No.9826 de 2026, rubro presupuestal **A-02-01-01-006-002**.

| Rubro Presupuestal | Descripción del Gasto | Valor |
|---|---|---|
| **A-02-01-01-006-002** | **PRODUCTOS DE LA PROPIEDAD INTELECTUAL** | |
| A-02-01-01-006-002-03-1-01 | **Paquete de Software** (Licenciamiento prevención de ciberamenzas con IA (vigencia 1 año). | $250.000.000,00 |
| **VALOR TOTAL DE LA SOLICITUD** | | **$250.000.000,00** |

### 4.3. FORMA DE PAGO

El valor del contrato se realizará UN UNICO PAGO, pagadero dentro de los treinta (30) días calendario siguientes, de acuerdo a la disponibilidad del P.A.C. (Plan Anual Mensualizado de Caja), previa presentación de a) La factura correspondiente con el lleno de los requisitos legales señalados en el Artículo 617 del Estatuto Tributario, b) La certificación del cumplimiento del pago de aportes parafiscales relativos al sistema de seguridad social integral así como, los propios del SENA, ICBF y CAJA DE COMPENSACIÓN FAMILIAR, cuando corresponda en los términos del art. 23 de la Ley 1150 de 2007, c) LA ENTREGA

DE LOS CÓDIGOS DE ACTIVACIÓN, d) la certificación de cumplimiento a satisfacción expedida por el supervisor, y e) debe realizarse el ingreso a almacén.

## 5. CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE

### 5.1. CRITERIOS DE EVALUACIÓN

El procedimiento de selección del contratista está sometido a los principios de transparencia, selección objetiva e igualdad de derechos y oportunidades de los que se deriva la obligación de someter a todos los oferentes a las mismas condiciones definidas en la ley y en el pliego de condiciones.

Cabe recordar que los pliegos de condiciones forman parte esencial del contrato; son la fuente de derechos y obligaciones de las partes y elemento fundamental para su interpretación e integración, pues contienen la voluntad de la administración a la que se someten los proponentes durante el proceso de selección y el oferente favorecido durante el mismo lapso y, más allá, durante la vigencia del contrato.

El numeral 2º del artículo 5º de la Ley 1150 de 2007 estipula que: "La oferta más favorable será aquella que, teniendo en cuenta los factores técnicos y económicos de escogencia y la ponderación precisa y detallada de los mismos, contenida en los pliegos de condiciones o sus equivalentes, resulte ser la más ventajosa para la entidad, sin que la favorabilidad la constituyan factores diferentes a los contenidos en dichos documentos. (…)".

Los pliegos de condiciones establecen como criterios de habilitación los aspectos de experiencia, capacidad financiera y jurídica, a través de los cuales se busca que la Entidad escoja un proponente que cumpla con las condiciones técnicas, financieras y jurídicas que garanticen el cumplimiento del objeto contractual.

De conformidad con lo expuesto, cabe concluir que los principios de transparencia, igualdad y selección objetiva, a que está sometida la selección del contratista, se desarrollan mediante la sujeción de la escogencia del contratista a la ley y al pliego de condiciones.

Habilitados los proponentes de acuerdo con los criterios anteriores, se procederá a escoger el adjudicatario de acuerdo con el procedimiento para la selección por Subasta Inversa, una vez cumpla con los requisitos habilitantes y se realice el proceso en la plataforma de SECOP II.

Para el Certificado de Inscripción Calificación y Clasificación en el Registro Único de Proponentes (RUP). De acuerdo con lo establecido en el artículo 6 de la Ley 1150 de 2007 y los artículos 2.2.1.1.1.5.1 y subsiguientes del Decreto 1082 de 2015, el oferente deberá anexar a su propuesta el documento correspondiente expedido por la Cámara de Comercio de su jurisdicción, en el cual conste su inscripción y clasificación en los bienes, obras o servicios a ofrecer.

### 5.2. CRITERIOS TECNICOS

El oferente deberá anexar certificación de Darktrace, en donde conste que es partner autorizado para la venta, suministro de productos, servicios, licencias y garantías de la solución Darktrace (Nivel Premier) para Colombia.

## 6. EL ANÁLISIS DEL RIESGO Y LA FORMA DE MITIGARLO

Para una mejor determinación de los riesgos existentes es importante tener claro el concepto de riesgos como aquel daño potencial que puede surgir por un suceso presente o futuro y puede generarse en el desarrollo de un contrato en cualquiera de sus etapas (precontractual, contractual y postcontractual) diariamente, en ocasiones se refiere al riesgo como sinónimo de probabilidad, pero en el asesoramiento profesional de riesgo, el riesgo combina la probabilidad de que ocurra un evento negativo. Es decir, en palabras claras, el riesgo es la posibilidad de que un peligro pueda llegar a materializarse dentro de un período determinado, como también es la probabilidad de que un resultado esperado no ocurra, en el periodo de tiempo de ejecución del contrato y con las obligaciones de este.

Se anexa la MATRIZ DE RIESGOS del proceso de contratación.

## 7. ANALISIS QUE SUSTENTA LA EXIGENCIA DE GARANTIAS

Para la ejecución del contrato que llegare a adjudicarse como resultado del presente proceso de selección se hace necesario, de acuerdo con las actividades a desarrollar y con la importancia del proceso para la Entidad, exigir al futuro contratista la constitución de una garantía de cumplimiento dentro de los tres (3) días hábiles siguientes a la suscripción del contrato a favor de la **Unidad Administrativa Especial Agencia del Inspector General de Tributos, Rentas y Contribuciones Parafiscales - ITRC** con NIT No. 900.528.648-4, que ampare:

| AMPARO | % | SOBRE EL VALOR TOTAL | VIGENCIA |
|---|---|---|---|
| *Calidad del Bien o Servicio* | *10%* | *Del contrato* | *Calidad del servicio suministrado por una vigencia igual al plazo del contrato y 18 meses más.* |
| *Cumplimiento del Contrato* | *10%* | *Del contrato* | *El cumplimiento general del contrato, el pago de multas, de la cláusula penal pecuniaria y demás sanciones con una vigencia igual al plazo del contrato y 18 meses más, contados a partir de la fecha de expedición de la garantía.* |

Al monto de esta garantía se imputará el valor de las multas y la cláusula penal, y se repondrá si por este motivo se disminuyere o agotare. El garante podrá subrogarse en las obligaciones del CONTRATISTA ante la Agencia. La garantía deberá estar vigente hasta la liquidación del contrato.

En caso de que haya necesidad de adicionar, prorrogar o suspender la ejecución del contrato resultante, o en cualquier otro evento, el CONTRATISTA se obliga a modificarla de acuerdo con las normas legales vigentes.

El CONTRATISTA deberá mantenerla vigente y será de su cargo el pago de todas las primas y demás erogaciones de constitución.

## 8. INDICACIÓN DE SI LA CONTRATACIÓN RESPECTIVA ESTÁ COBIJADA POR UN ACUERDO COMERCIAL

El presente Proceso de Contratación **NO** está cobijado por ningún Acuerdo Comercial.

Atentamente,

RODRIGUEZ ROA JAVIER RAUL

Firmado digitalmente por RODRIGUEZ ROA JAVIER RAUL
Fecha: 2026.10.23 12:02:13 -05'00'

**Javier Raúl Rodriguez Roa**
**Jefe Oficina Asesora de Tecnología de la Información - OATI (E)**