ANÁLISIS DEL SECTOR

CONTRATACIÓN DE MENOR CUANTÍA

2026

OBJETO: REALIZAR PRUEBAS DE CIBERSEGURIDAD, Y EJECUTAR EL PLAN DE SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA EL INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA

1. ANÁLISIS DE MERCADO.

El sector de seguridad informática, de conformidad con el clasificador de bienes y servicios de las Naciones Unidas (UNSPSC) y la clasificación industrial internacional uniforme de todas las actividades económicas Rev. 4 A.C. (CIIU) incluye diversos servicios, los cuales responden dentro de la cadena de producción en Colombia, a un nivel de servicios, en el entendido que reúne todas aquellas actividades de pruebas de vulnerabilidad.

Para el presente proceso la clasificación Industrial Internacional Uniforme es la siguiente:

CÓDIGO CPC – DANE: 83131 – Servicios de consultoría en tecnologías de la información (TI)

CIIU Rev 4 A.C.		CPC Ver 2 A.C.
6202		83131

Incluye

Esta subclase incluye:
* Los servicios de consultoría y asesoría especializada en relación con el uso de las tecnologías de la información, como:
- La asesoría técnica para la adquisición de hardware y software y la contratación.
- La integración de sistemas.
- La seguridad informática.
- La consultoría especializada en tecnologías de la información (TI).

Por su parte, el clasificador de bienes y servicios correspondiente se encuentra en los siguientes Grupos Servicios:

Código UNSPSC	Nombre UNSPSC
81111800	Servicios de Sistemas y Administración de Componentes de Sistemas

https://operaciones.colombiacompra.gov.co/clasificador-de-bienes-y-servicios

El sector de Tecnologías de la Información y las Comunicaciones (TIC) continúa consolidándose como uno de los principales motores de crecimiento económico, innovación y transformación digital en Colombia. Las TIC son un habilitador transversal para todos los sectores productivos, permitiendo optimizar procesos, mejorar la eficiencia operativa, fortalecer la toma de decisiones basada en datos y generar nuevas oportunidades de negocio.

De acuerdo con el artículo 6 de la Ley 1978 de 2019, las Tecnologías de la Información y las Comunicaciones comprenden el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permiten la recopilación, procesamiento, almacenamiento, transmisión e intercambio de información en diferentes formatos, incluyendo voz, datos, texto, imágenes y video.

Según la Cuenta Satélite TIC del DANE, el valor agregado bruto del sector TIC en Colombia alcanzó los 58,1 billones de pesos en 2025, registrando un crecimiento del 5,5% respecto al año anterior, evidenciando su relevancia dentro de la economía nacional y su capacidad para impulsar la productividad y competitividad empresarial. Asimismo, el sector mantiene una dinámica positiva impulsada por la expansión de la conectividad, la adopción de tecnologías digitales, la inteligencia artificial, la computación en la nube y la automatización de procesos. (Fuente: DANE – Cuenta Satélite TIC 2025)

El ecosistema TIC colombiano está conformado por diversos segmentos que incluyen:

a. Infraestructura tecnológica y conectividad digital.

b. Servicios de telecomunicaciones fijas y móviles.

c. Desarrollo de software, aplicaciones y soluciones digitales.

d. Plataformas digitales y servicios basados en datos.

e. Servicios de computación en la nube y centros de datos.

f. Investigación, desarrollo e innovación tecnológica.

g. Servicios de ciberseguridad y protección de la información.

La expansión de la conectividad continúa siendo un factor clave para el crecimiento del sector. De acuerdo con cifras oficiales del Ministerio TIC, Colombia superó los 49 millones de accesos a Internet durante 2025, mientras que los accesos fijos alcanzaron aproximadamente 9,34 millones de conexiones, reflejando avances significativos en la reducción de la brecha digital y la inclusión tecnológica. (Fuente: Ministerio TIC – Boletín Trimestral Sector TIC 2025 / MinTIC – Accesos a Internet en Colombia 2025).

Paralelamente, la transformación digital ha incrementado la dependencia de las organizaciones respecto a los sistemas de información, generando nuevos desafíos relacionados con la gestión del riesgo digital y la ciberseguridad. En este contexto, una vulnerabilidad se define como una debilidad o falla en un sistema, aplicación, infraestructura o proceso que puede ser explotada por actores maliciosos para comprometer la confidencialidad, integridad o disponibilidad de la información.

Las vulnerabilidades pueden permitir, entre otras acciones:

- ✓ Acceso no autorizado a sistemas o datos.
- ✓ Suplantación de identidad de usuarios o servicios.
- ✓ Alteración o destrucción de información.
- ✓ Interrupción de servicios mediante ataques de denegación de servicio.
- ✓ Escalamiento indebido de privilegios dentro de una organización.

La protección de la información requiere un enfoque integral que combine controles tecnológicos, procesos organizacionales y cultura de seguridad. En este sentido, la norma internacional ISO/IEC 27001 continúa siendo uno de los principales referentes para la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI), proporcionando un marco estructurado para la identificación, evaluación y tratamiento de riesgos. (Fuente: ISO/IEC 27001:2022).

Actualmente, las amenazas cibernéticas evolucionan con gran rapidez debido al crecimiento de la inteligencia artificial, la digitalización de los servicios, la computación en la nube y el aumento de dispositivos conectados. Los ataques de ransomware, el phishing avanzado, la explotación de vulnerabilidades en terceros y los ataques dirigidos a infraestructuras críticas representan algunos de los principales riesgos para organizaciones públicas y privadas.

Como respuesta a este panorama, Colombia ha fortalecido su estrategia nacional de seguridad digital. Durante 2025 y 2026 se impulsaron iniciativas orientadas al fortalecimiento de capacidades institucionales, la protección de infraestructuras críticas, el desarrollo de talento especializado y la mejora de los mecanismos de respuesta ante incidentes cibernéticos. De acuerdo con información oficial del MinTIC, el ColCERT gestionó 697 incidentes de seguridad digital durante 2025, reflejando avances en los niveles de preparación y resiliencia de la infraestructura digital del país. (Fuente: MinTIC – Seguridad Digital y ColCERT 2025).

En consecuencia, las organizaciones enfrentan la necesidad de adoptar modelos de ciberseguridad basados en la gestión continua del riesgo, la protección de identidades digitales, la supervisión permanente de amenazas y el fortalecimiento de la cultura de seguridad entre colaboradores, proveedores y usuarios.

Principales tendencias de ciberseguridad para 2026

El panorama global de ciberseguridad continúa evolucionando rápidamente debido al crecimiento de la inteligencia artificial, la hiperconectividad, la computación en la nube y la digitalización acelerada de organizaciones públicas y privadas. En este contexto, las amenazas cibernéticas son cada vez más sofisticadas, automatizadas y difíciles de detectar.

Entre las principales tendencias de ciberseguridad identificadas para 2026 se destacan las siguientes:

Ciberataques potenciados por inteligencia artificial generativa:

Los ciberdelincuentes están utilizando herramientas de inteligencia artificial generativa para automatizar campañas de phishing, desarrollar malware adaptable y crear contenidos fraudulentos altamente convincentes, incluyendo audios, imágenes y videos falsificados (deepfakes). Esto ha incrementado la sofisticación de los ataques de ingeniería social y fraude digital. Fuente: World Economic Forum – Global Cybersecurity Outlook 2025 https://www.weforum.org/reports/global-cybersecurity-outlook-2025/

Incremento de ataques dirigidos a identidades digitales:

Las organizaciones enfrentan un aumento en ataques enfocados en el robo de credenciales, secuestro de sesiones y abuso de privilegios. Los atacantes priorizan el compromiso de identidades digitales debido a la expansión del trabajo híbrido y el uso masivo de servicios en la nube. Fuente: IBM X-Force Threat Intelligence Index 2025 https://www.ibm.com/reports/threat-intelligence.

Crecimiento del ransomware como servicio (RaaS):

Los modelos criminales de "Ransomware as a Service" continúan creciendo, permitiendo que actores con bajos conocimientos técnicos ejecuten ataques complejos mediante plataformas criminales especializadas. Fuente:ENISA Threat Landscape 2025 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

Aumento de riesgos en cadenas de suministro tecnológicas:

Los ataques a proveedores de software, plataformas cloud y terceros tecnológicos continúan siendo uno de los principales riesgos corporativos, debido a la alta dependencia de ecosistemas digitales interconectados. Fuente: CrowdStrike Global Threat Report 2025 https://www.crowdstrike.com/global-threat-report/.

Expansión de amenazas asociadas a dispositivos IoT y hogares inteligentes:

El crecimiento de dispositivos conectados, sensores inteligentes y tecnologías domésticas automatizadas ha ampliado la superficie de ataque digital, especialmente en dispositivos con configuraciones inseguras o sin actualizaciones frecuentes. Fuente:Fortinet Global Threat Landscape Report 2025. https://www.fortinet.com/resources/cyberglossary/threat-landscape.

Mayor adopción de modelos Zero Trust:

Las organizaciones están implementando modelos de seguridad "Zero Trust", basados en el principio de "nunca confiar, siempre verificar", fortaleciendo controles de acceso, autenticación multifactor y monitoreo continuo de usuarios y dispositivos. Fuente: Gartner – Cybersecurity Trends 2025. https://www.gartner.com/en/cybersecurity.

Regulaciones y exigencias de cumplimiento más estrictas:

Gobiernos y organismos internacionales están fortaleciendo normativas relacionadas con protección de datos, resiliencia digital y reporte de incidentes, aumentando las exigencias de cumplimiento para las organizaciones. Fuente: OECD Digital Security Outlook 2025. https://www.oecd.org/digital/digital-security-outlook/.

De acuerdo con la Dirección de Investigación Criminal e Interpol (DIJIN) de la Policía Nacional de Colombia, los delitos informáticos continúan aumentando significativamente en el país debido al crecimiento de servicios digitales, transacciones electrónicas y plataformas conectadas.

El número total de denuncias por delitos informáticos aumentó de 31.095 casos en 2023 a 37.409 en 2024, representando un incremento del 20,31%. Entre las modalidades con mayor crecimiento se encuentra el acceso abusivo a sistemas informáticos, que pasó de 11.406 denuncias en 2023 a 16.955 en 2024. Asimismo, la violación de datos personales aumentó de 10.155 a 11.954 denuncias durante el mismo periodo. Fuente:Policía Nacional de Colombia – DIJIN / Revista Semana. https://www.policia.gov.co.

https://www.semana.com/economia/empresas/articulo/delitos-informaticos-aumentaron-en-colombia-durante-2024/202500/.

La suplantación de sitios web también presentó un incremento importante, pasando de 4.716 denuncias en 2023 a 6.209 casos en 2024, reflejando el crecimiento de campañas de phishing y fraude digital orientadas al robo de información financiera y credenciales de acceso.

Por otra parte, aunque algunas categorías como daño informático y uso de software malicioso registraron una disminución en las denuncias reportadas, las autoridades advierten que las amenazas continúan evolucionando hacia mecanismos más sofisticados y difíciles de rastrear.

En este contexto, la ciberseguridad se ha convertido en un componente estratégico para las organizaciones, no solo desde la perspectiva tecnológica, sino también desde la gestión del riesgo empresarial, la continuidad del negocio y la protección reputacional.

2. SUBSECTOR DE PRESTACIÓN DE SERVICIOS TIC Y CIBERSEGURIDAD

En el actual contexto de transformación digital, globalización e integración tecnológica, las organizaciones públicas y privadas requieren servicios especializados que les permitan fortalecer sus capacidades tecnológicas, optimizar procesos operativos y garantizar la protección de sus activos digitales. En este escenario, el subsector de prestación de servicios TIC y ciberseguridad

ha adquirido una relevancia estratégica para la continuidad operativa, la gestión del riesgo y el cumplimiento normativo de las entidades.

La prestación de servicios especializados en tecnologías de la información comprende actividades de consultoría, implementación, soporte, aseguramiento, auditoría y fortalecimiento de infraestructuras tecnológicas, plataformas cloud, identidades digitales, servicios de seguridad informática y modelos de gestión de riesgos cibernéticos. Estos servicios permiten a las organizaciones adoptar estándares internacionales, fortalecer controles de seguridad y mejorar sus capacidades de prevención, detección y respuesta frente a amenazas digitales. Fuente: Ministerio TIC – Transformación Digital. https://www.mintic.gov.co/portal/inicio/.

Las Tecnologías de la Información y las Comunicaciones (TIC), de conformidad con la Ley 1978 de 2019, corresponden al conjunto de recursos, herramientas, redes, aplicaciones, equipos y servicios que permiten la recopilación, procesamiento, almacenamiento y transmisión de información en diferentes formatos, incluyendo voz, datos, texto, video e imágenes.

En Colombia, las TIC constituyen un eje transversal para el desarrollo económico, la modernización institucional y la competitividad empresarial. El Estado colombiano ha impulsado estrategias orientadas al fortalecimiento de la conectividad, la transformación digital, el gobierno digital y la ciberseguridad, especialmente en entidades públicas que administran información sensible y servicios críticos. Fuente: Ley 1978 de 2019.

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=98210.

Toda cadena de valor digital incorpora actividades de investigación, desarrollo, innovación y fortalecimiento de capacidades tecnológicas, necesarias para la evolución continua del sector TIC y la adaptación frente a nuevos riesgos cibernéticos asociados a entornos híbridos, servicios en la nube, inteligencia artificial y modelos de trabajo remoto.

Dentro de los principales componentes del sector TIC se encuentran:

a. Infraestructura tecnológica y conectividad.

b. Servicios de telecomunicaciones y redes.

c. Plataformas digitales y servicios cloud.

d. Desarrollo de software y aplicaciones.

e. Servicios de ciberseguridad y protección de la información.

f. Servicios de monitoreo, auditoría y pruebas de seguridad.

3. RELACIÓN DEL OBJETO CONTRACTUAL CON EL SECTOR

El objeto contractual denominado “REALIZAR PRUEBAS DE CIBERSEGURIDAD, Y EJECUTAR EL PLAN DE SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA EL INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA” se encuentra directamente relacionado con el sector de Tecnologías de la Información y las Comunicaciones (TIC) específicamente con el segmento de servicios especializados de ciberseguridad, seguridad de la información, evaluación de vulnerabilidades, pruebas de seguridad y fortalecimiento de la cultura de seguridad de la información

La relación del objeto con este sector se fundamenta en que las actividades a desarrollar requieren conocimientos, metodologías y capacidades técnicas especializadas para identificar vulnerabilidades y riesgos de seguridad en los activos tecnológicos de la entidad, evaluar la efectividad de los controles implementados y generar recomendaciones orientadas al fortalecimiento de la seguridad de la información. De manera complementaria, el componente de sensibilización requiere conocimientos especializados para desarrollar acciones de formación y concientización dirigidas a los usuarios de la entidad, con el propósito de fortalecer el factor humano como elemento fundamental dentro del sistema de seguridad de la información.

Fuente de consulta: Agencia Nacional de Contratación Pública – Colombia Compra Eficiente

https://www.colombiacompra.gov.co/archivos/manual/guia-para-la-elaboracion-de-estudios-del-sector?utm_source=chatgpt.com

El sector TIC en Colombia presenta una dinámica de crecimiento y transformación asociada a la incorporación de tecnologías digitales en las organizaciones públicas y privadas. De acuerdo con la Cuenta Satélite de las Tecnologías de la Información y las Comunicaciones (CSTIC) del DANE, para 2025 el valor agregado bruto del sector TIC alcanzó $58,1 billones de pesos, con un crecimiento del 5,5 % frente a 2024, evidenciando la importancia económica del sector y la creciente demanda de bienes y servicios asociados a las tecnologías de información y comunicaciones.

Fuente de consulta: DANE – Cuenta Satélite de las Tecnologías de la Información y las Comunicaciones.

https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-satelite/cuenta-satelite-de-las-tecnologias-de-la-informacion-y-las-comunicaciones-cstic?highlight=WyJxdWUiLCJxdVx1MDBlOSIsImEiXQ%3D%3D&utm_source=chatgpt.com

En este contexto de transformación digital, las entidades públicas se encuentran expuestas a riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información, así como con la seguridad de sus sistemas, aplicaciones, infraestructura tecnológica, usuarios y servicios digitales. La evolución de las amenazas cibernéticas hace necesario complementar los controles preventivos con actividades periódicas de evaluación que permitan identificar vulnerabilidades y oportunidades de mejora antes de que puedan ser aprovechadas por actores maliciosos.

El Microsoft Digital Defense Report 2025 señala que el panorama de amenazas continúa evolucionando, con un incremento en el uso de inteligencia artificial por parte de los actores maliciosos, el crecimiento de los infostealers, el ciberdelito como servicio y las amenazas dirigidas contra identidades y entornos en la nube. El informe identifica, además, la necesidad de fortalecer la resiliencia de las identidades, la nube y las capacidades de defensa de las organizaciones.

De igual manera, el IBM X-Force Threat Intelligence Index 2025 identificó que el abuso de identidades de usuarios continuó siendo uno de los principales puntos de entrada utilizados por los atacantes durante 2024, representando el 30 % de los casos analizados. Esta situación evidencia la importancia de mantener mecanismos de evaluación de seguridad y de fortalecer las capacidades de los usuarios para reconocer y prevenir situaciones que puedan comprometer las credenciales, la información y los sistemas institucionales.

En el ámbito de las entidades públicas colombianas, la seguridad de la información constituye un componente de la Política de Gobierno Digital. El Decreto 767 de 2022 establece los lineamientos generales de dicha política e incorpora la seguridad y privacidad de la información como uno de sus habilitadores, orientado al desarrollo de capacidades para preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos y activos de información.

Adicionalmente, durante 2025 el Ministerio de Tecnologías de la Información y las Comunicaciones actualizó los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) mediante la Resolución 02277 de 2025, fortaleciendo el marco aplicable a las entidades públicas en materia de seguridad de la información. Los nuevos lineamientos incorporan, entre otros aspectos, la alineación con ISO/IEC 27001:2022 y NIST CSF 2.0, así como elementos relacionados con cultura de seguridad, evaluación y gestión de controles.

En consecuencia, las actividades objeto del presente proceso se encuentran comprendidas dentro de un mercado especializado de servicios de ciberseguridad y seguridad de la información, en el cual participan empresas y profesionales con capacidades técnicas para ejecutar pruebas de seguridad, identificación y análisis de vulnerabilidades, evaluación de controles, elaboración de informes técnicos y ejecutivos, formulación de recomendaciones y actividades de sensibilización y fortalecimiento de la cultura de seguridad de la información.

Por lo anterior, la contratación de estos servicios responde a una necesidad institucional del IDEA orientada a identificar y gestionar riesgos de ciberseguridad, fortalecer los controles de seguridad de la información y mejorar el nivel de conocimiento y apropiación de las prácticas de seguridad por parte de los usuarios, contribuyendo a la protección de los activos de información, los sistemas tecnológicos y los servicios que soportan las actividades de la entidad.

4. MARCO NORMATIVO.

En cumplimiento de lo dispuesto en el artículo 2.2.1.1.1.6.1 del Decreto 1082 de 2015 y de conformidad con los lineamientos establecidos por Colombia Compra Eficiente para la elaboración de estudios y documentos previos, se realiza el presente análisis del sector correspondiente al subsector de servicios especializados en tecnologías de la información, y ciberseguridad, en atención al objeto contractual denominado:

“REALIZAR PRUEBAS DE CIBERSEGURIDAD, Y EJECUTAR EL PLAN DE SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA EL INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA”.

El sector TIC se caracteriza por su constante evolución tecnológica, innovación y adopción de estándares internacionales orientados a fortalecer la seguridad de la información, la continuidad operativa y la resiliencia digital de las organizaciones. En consecuencia, el presente proceso contractual involucra disposiciones normativas relacionadas con contratación estatal, protección

de datos personales, seguridad digital, gobierno digital, gestión de riesgos, servicios en la nube y estándares internacionales de seguridad de la información.

Normativa Constitucional y Legal

a. Constitución Política de Colombia – Artículo 15:

Consagra el derecho fundamental a la intimidad, al buen nombre y a la protección de datos personales.

b. Ley 80 de 1993. Por la cual se expide el Estatuto General de Contratación de la Administración Pública.

c. Ley 1150 de 2007:

Por medio de la cual se introducen medidas para la eficiencia y transparencia en la Ley 80 de 1993.

d. Ley 527 de 1999:

Por medio de la cual se reglamenta el acceso y uso de mensajes de datos, comercio electrónico y firmas digitales.

e. Ley 1273 de 2009:

Por medio de la cual se modifica el Código Penal y se crea el bien jurídico tutelado de la protección de la información y de los datos.

f. Ley 1341 de 2009 modificada por la Ley 1978 de 2019:

Define los principios y conceptos sobre la sociedad de la información, organización del sector TIC y transformación digital.

g. Ley 1581 de 2012:

Por la cual se dictan disposiciones generales para la protección de datos personales.

h. Ley 1712 de 2014:

Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

i. Ley 1928 de 2018:

Por medio de la cual Colombia aprueba el Convenio sobre la Ciberdelincuencia de Budapest.

j. Ley 2195 de 2022:

Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción.

k. Ley 1952 de 2019 y Ley 2094 de 2021:

Código General Disciplinario y su reforma.

l. Ley 1266 de 2008:

Por la cual se dictan disposiciones relacionadas con el hábeas data financiero y crediticio.

m. Ley 23 de 1982 y Ley 44 de 1993:

Normativa sobre derechos de autor y propiedad intelectual.

Decretos Reglamentarios

n. Decreto 1082 de 2015:

Decreto Único Reglamentario del Sector Administrativo de Planeación Nacional, aplicable a la contratación estatal.

o. Decreto 1078 de 2015:

Decreto Único Reglamentario del Sector Tecnologías de la Información y las Comunicaciones.

p. Decreto 1008 de 2018:

Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital.

q. Decreto 1499 de 2017:

Por medio del cual se actualiza el Modelo Integrado de Planeación y Gestión – MIPG.

r. Decreto 612 de 2018:

Por el cual se fijan directrices para la integración de planes institucionales y estratégicos.

s. Decreto 767 de 2022:

Por el cual se actualizan los lineamientos de Gobierno Digital y seguridad digital para entidades públicas.

Resoluciones, Circulares y Lineamientos Técnicos

t. Resolución 500 de 2021 – MinTIC:

Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información (MSPI).

u. Resolución 1519 de 2020 – MinTIC:

Por la cual se definen los estándares y directrices para publicar información señalada en la Ley 1712 de 2014.

v. Circular Externa 007 de 2018 – Superintendencia Financiera de Colombia:

Instrucciones relacionadas con requerimientos mínimos para la gestión de la seguridad de la información y ciberseguridad.

w. Circular Externa 005 de 2019 – Superintendencia Financiera de Colombia:

Reglas relativas al uso de servicios de computación en la nube.

x. Circular Externa 033 de 2020 – Superintendencia Financiera de Colombia:

Instrucciones relacionadas con la Taxonomía Única de Incidentes Cibernéticos.

y. Guía de Seguridad y Privacidad de la Información – MinTIC:

Lineamientos técnicos para la implementación de controles de seguridad y gestión de riesgos digitales en entidades públicas.

Estándares y Buenas Prácticas Internacionales

z. ISO/IEC 27001:2022:

Norma internacional para Sistemas de Gestión de Seguridad de la Información (SGSI).

aa. ISO/IEC 27002:2022:

Buenas prácticas y controles para la seguridad de la información.

ab. NIST Cybersecurity Framework (CSF) 2.0:

Marco de referencia para la gestión y fortalecimiento de capacidades de ciberseguridad.

ac. Microsoft Security Benchmark / Zero Trust Framework:

Normativa y Actos Administrativos Internos

ad. Políticas internas de seguridad de la información, gobierno digital, tratamiento de datos personales y gestión de activos tecnológicos adoptadas por el IDEA.

El marco normativo anteriormente relacionado resulta aplicable al presente proceso contractual, considerando que el objeto comprende la implementación de controles de seguridad, fortalecimiento de identidades digitales, aseguramiento de plataformas cloud y on-premise, así como actividades relacionadas con la gestión integral de riesgos de seguridad de la información dentro de la infraestructura tecnológica institucional del IDEA.

5. CARACTERIZACIÓN DEL SECTOR

Crecimiento del sector TIC y generación de empleo

El sector de Tecnologías de la Información y las Comunicaciones (TIC) continúa consolidándose como uno de los principales dinamizadores de la economía colombiana, impulsado por la transformación digital, la migración a servicios en la nube, la automatización de procesos, la

inteligencia artificial y el fortalecimiento de la ciberseguridad en organizaciones públicas y privadas.

De acuerdo con la Cuenta Satélite TIC (CSTIC) del DANE, durante 2025 el sector mantuvo una dinámica positiva tanto en generación de valor agregado como en empleo especializado, especialmente en actividades relacionadas con servicios TI, desarrollo de software, servicios cloud, ciberseguridad y plataformas digitales.

Los segmentos con mayor crecimiento continúan siendo:

- ✓ Servicios de tecnologías de la información y desarrollo de software.
- ✓ Servicios de computación en la nube y transformación digital.
- ✓ Ciberseguridad y protección de identidades digitales.
- ✓ Plataformas digitales y servicios basados en datos.
- ✓ Servicios de soporte, consultoría y administración tecnológica.

Fuente DANE – Cuenta Satélite TIC 2025

https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-satelite/cuenta-satelite-de-las-tecnologias-de-la-informacion-y-las-comunicaciones-cstic.

El crecimiento de los servicios tecnológicos especializados ha incrementado la demanda de talento humano en áreas como ciberseguridad, seguridad de la información, arquitectura cloud, análisis de riesgos y operación de centros de seguridad (SOC).

De acuerdo con el Ministerio TIC, Colombia continúa fortaleciendo programas de formación en habilidades digitales, ciberseguridad e inteligencia artificial, con el objetivo de reducir la brecha de talento tecnológico y fortalecer la competitividad del ecosistema digital nacional. FuenteMinisterio TIC – Talento Digital. https://talentodigital.mintic.gov.co/

Fortalecimiento de la industria TI y transformación digital

El Gobierno Nacional continúa impulsando estrategias para fortalecer la industria TI y acelerar la transformación digital de entidades públicas y privadas, promoviendo la adopción de tecnologías emergentes, servicios digitales y modelos de seguridad basados en gestión del riesgo.

Entre las principales líneas estratégicas del sector se destacan:

- ✓ Modernización de infraestructuras tecnológicas.
- ✓ Implementación de modelos de Gobierno Digital.
- ✓ Fortalecimiento de capacidades de ciberseguridad.
- ✓ Adopción de servicios cloud y arquitecturas híbridas.
- ✓ Protección de datos e identidades digitales.
- ✓ Implementación de modelos Zero Trust.
- ✓ Automatización y analítica basada en inteligencia artificial.

Fuente: Política de Gobierno Digital – MinTIC. https://gobiernodigital.mintic.gov.co/

La transformación digital de las organizaciones ha generado un aumento significativo en la necesidad de servicios especializados orientados a asegurar plataformas colaborativas, sistemas de autenticación centralizada y entornos híbridos de infraestructura tecnológica.

En consecuencia, las soluciones de seguridad de la información y protección de infraestructura crítica se han convertido en componentes estratégicos y transversales dentro de la arquitectura tecnológica del Instituto para el Desarrollo de Antioquia – IDEA. Lo anterior obedece a que estas soluciones concentran y blindan los procesos de autenticación robusta, control de acceso perimetral y lógico a datos sensibles, administración del ciclo de vida de usuarios y monitoreo de servicios corporativos, garantizando la continuidad del negocio financiero y de fomento de la entidad frente a vectores de amenaza actuales."

5.1 Caracterización del mercado relacionado con el objeto contractual

El objeto del presente proceso de selección se encuentra directamente relacionado con el mercado de servicios especializados en tecnologías de la información, seguridad de la infraestructura y ciberseguridad, un sector maduro y altamente competitivo que cuenta con una pluralidad de oferentes, integradores y fabricantes a nivel nacional e internacional. Específicamente, las líneas de servicio requeridas por el Instituto para el Desarrollo de Antioquia – IDEA se enmarcan en los siguientes nichos especializados del mercado decantados por la oferta tecnológica actual

El crecimiento de ataques dirigidos a credenciales e identidades digitales ha convertido este segmento en uno de los más relevantes dentro del sector TIC. Según IBM X-Force Threat Intelligence Index 2025, el abuso de cuentas válidas y robo de credenciales continúa siendo uno de los principales vectores de ataque utilizados por ciberdelincuentes. FuenteIBM X-Force Threat Intelligence Index 2025. https://www.ibm.com/reports/threat-intelligence

Variables económicas para considerar en el presente proceso

Las principales variables económicas que impactan el presente proceso contractual corresponden al comportamiento del Producto Interno Bruto (PIB), inflación, mercado laboral especializado, variación del salario mínimo y crecimiento del sector TIC.

Producto Interno Bruto (PIB)

De acuerdo con cifras preliminares del DANE, durante 2025 la economía colombiana mantuvo una recuperación gradual impulsada principalmente por sectores relacionados con servicios, comercio, actividades profesionales, transformación digital y administración pública.

El crecimiento económico estuvo soportado principalmente por:

- ✓ Actividades profesionales, científicas y técnicas.
- ✓ Servicios tecnológicos y transformación digital.
- ✓ Comercio y servicios empresariales.
- ✓ Administración pública y servicios asociados.
- ✓ Agricultura y actividades logísticas.

Fuente DANE – Producto Interno Bruto (PIB) 2025.

https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/producto-interno-bruto-pib

El sector TIC continúa siendo uno de los principales habilitadores de productividad empresarial y modernización institucional, especialmente por el crecimiento sostenido de servicios cloud, inteligencia artificial, automatización y ciberseguridad.

Actividades profesionales, científicas y técnicas

Las actividades profesionales, científicas y técnicas continúan teniendo una participación estratégica dentro de la economía nacional, debido a que integran servicios especializados relacionados con consultoría, ingeniería, tecnologías de la información, seguridad digital y soporte técnico especializado.

Estas actividades son fundamentales para el desarrollo de proyectos de modernización tecnológica y fortalecimiento institucional, particularmente en entidades públicas que requieren mejorar sus capacidades digitales y fortalecer sus controles de seguridad de la información.

El mercado de servicios especializados en ciberseguridad presenta actualmente una alta demanda debido al crecimiento de amenazas digitales, requerimientos regulatorios y procesos de transformación digital acelerada.

En consecuencia, las organizaciones demandan proveedores con capacidades técnicas especializadas, experiencia certificada y conocimientos avanzados en plataformas cloud, gestión de identidades, seguridad híbrida y estándares internacionales de seguridad de la información.

6. ANÁLISIS DEL ENTORNO INTERNO.

El análisis del entorno interno comprende la identificación de las fortalezas, debilidades y riesgos asociados al subsector de servicios especializados en seguridad de la información, ciberseguridad y gestión de la identidad digital. Particularmente, se centra en aquellos factores relacionados con los servicios de implementación, aseguramiento, mitigación de vulnerabilidades y fortalecimiento de las arquitecturas tecnológicas híbridas (On-Premise y Cloud), plataformas de productividad, herramientas de gobierno de identidades y sistemas de directorio corporativo que soportan la operación del Instituto para el Desarrollo de Antioquia – IDEA.

Este análisis permite identificar los factores internos que pueden favorecer o impactar la adecuada ejecución del objeto contractual, considerando aspectos técnicos, organizacionales, económicos, operativos y de talento humano asociados al sector TIC, el cumplimiento de las directrices del Gobierno Digital y los estándares de seguridad digital del Estado colombiano.

Riesgos

De conformidad con lo establecido en el artículo 4 de la Ley 1150 de 2007, el Decreto 1082 de 2015 y los lineamientos definidos por Colombia Compra Eficiente en el Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación, la Entidad elaborará la matriz de riesgos del proceso contractual, la cual contendrá la tipificación, estimación, asignación y tratamiento de los riesgos previsibles que puedan afectar el equilibrio económico y la adecuada ejecución del contrato.

Tratándose de un proceso relacionado con servicios especializados de ciberseguridad y aseguramiento de plataformas tecnológicas críticas, se identifican principalmente riesgos asociados a:

- ✓ Cambios tecnológicos y actualización permanente de plataformas cloud.
- ✓ Escasez de talento humano especializado en ciberseguridad.
- ✓ Riesgos operativos derivados de configuraciones incorrectas o incompatibilidades técnicas.
- ✓ Riesgos asociados a disponibilidad de servicios tecnológicos y continuidad operativa.
- ✓ Riesgos de seguridad de la información y acceso no autorizado.
- ✓ Dependencia de servicios cloud y actualizaciones de fabricantes tecnológicos.
- ✓ Riesgos de retraso en actividades técnicas por complejidad de integración entre entornos híbridos y on-premise.
- ✓ Riesgos asociados a la gestión de identidades, privilegios y accesos administrativos.

La matriz de riesgos correspondiente hará parte integral del presente proceso contractual.

Fortalezas

El sector TIC y de ciberseguridad en Colombia presenta múltiples fortalezas que favorecen el desarrollo de proyectos tecnológicos especializados y la implementación de servicios avanzados de seguridad digital en entidades públicas y privadas.

Entre las principales fortalezas del sector se destacan:

- ✓ Crecimiento sostenido del sector TIC como impulsor de la transformación digital y modernización institucional.
- ✓ Incremento de la demanda de servicios especializados en ciberseguridad, nube e identidades digitales.
- ✓ Existencia de proveedores especializados con experiencia ciberseguridad y seguridad de la información.
- ✓ Mayor adopción de estándares internacionales de seguridad de la información y buenas prácticas de ciberseguridad.
- ✓ Fortalecimiento de políticas públicas orientadas a Gobierno Digital y seguridad digital.
- ✓ Disponibilidad de soluciones tecnológicas avanzadas para protección de identidades, accesos y entornos híbridos.
- ✓ Consolidación de servicios cloud como componente estratégico para entidades públicas y privadas.

- ✓ Crecimiento de programas de formación y certificación en tecnologías ciberseguridad y administración cloud.
- ✓ Mayor madurez institucional frente a la gestión del riesgo digital y protección de la información.
- ✓ Integración de herramientas de automatización, monitoreo y respuesta ante incidentes de seguridad.

El sector cuenta además con proveedores capaces de implementar modelos de seguridad alineados con estándares internacionales y arquitecturas modernas de protección basadas en Zero Trust, autenticación multifactor, acceso condicional y protección de identidades digitales.

Debilidades

A pesar del crecimiento y fortalecimiento del sector TIC y de ciberseguridad, persisten algunas limitaciones y desafíos que pueden impactar la ejecución de proyectos especializados relacionados con seguridad digital y administración de plataformas tecnológicas.

Entre las principales debilidades identificadas se encuentran:

- ✓ Escasez de profesionales altamente especializados en ciberseguridad y seguridad de la información.
- ✓ Alta rotación del talento humano especializado debido a la elevada demanda del mercado tecnológico.
- ✓ Brechas de conocimiento técnico en tecnologías emergentes y modelos avanzados de seguridad.
- ✓ Dependencia de fabricantes y proveedores internacionales para soporte, licenciamiento y actualización tecnológica.
- ✓ Diferencias en niveles de madurez digital entre organizaciones públicas y privadas.
- ✓ Incremento constante de amenazas cibernéticas y evolución acelerada de técnicas de ataque.
- ✓ Limitaciones presupuestales en algunas entidades para mantener procesos continuos de actualización tecnológica y fortalecimiento de seguridad.
- ✓ Complejidad técnica asociada a la integración de entornos híbridos entre plataformas cloud y sistemas on-premise.
- ✓ Necesidad permanente de capacitación y actualización técnica del personal encargado de la administración tecnológica.
- ✓ Persistencia de riesgos derivados de errores de configuración, privilegios excesivos y malas prácticas de seguridad.

No obstante, el mercado presenta actualmente una oferta creciente de empresas especializadas y profesionales certificados que permiten atender las necesidades de fortalecimiento de ciberseguridad, modernización tecnológica y protección de infraestructuras digitales críticas en el sector público y privado.

7. ANÁLISIS DEL ENTORNO EXTERNO

El análisis del entorno externo tiene como finalidad identificar factores, tendencias y condiciones del mercado que puedan generar impactos positivos o negativos sobre el sector TIC y de ciberseguridad, así como sobre la adecuada ejecución del objeto contractual.

El entorno tecnológico actual se caracteriza por una rápida evolución digital, un incremento exponencial en la sofisticación de las amenazas cibernéticas (especialmente aquellas dirigidas al sector público y financiero), la transformación acelerada de los modelos operativos y la creciente adopción de arquitecturas integradas de nube. Estos factores generan oportunidades de optimización y crecimiento tecnológico, pero también imponen desafíos críticos de resiliencia para la entidad y exigen un alto nivel de especialización por parte de los proveedores del sector.

Oportunidades

Las oportunidades corresponden a situaciones favorables del entorno que pueden fortalecer el desarrollo del sector TIC y de ciberseguridad, así como mejorar las capacidades tecnológicas y de protección digital de las organizaciones.

Entre las principales oportunidades identificadas se encuentran:

- ✓ Crecimiento sostenido de la transformación digital en entidades públicas y privadas, aumentando la demanda de servicios especializados en ciberseguridad y protección de entornos cloud.
- ✓ Mayor adopción de plataformas y modelos híbridos de infraestructura tecnológica, impulsando la necesidad de implementación de controles de ciberseguridad.
- ✓ Incremento de inversiones en seguridad digital, protección de identidades y fortalecimiento de capacidades de respuesta ante incidentes cibernéticos.
- ✓ Fortalecimiento de políticas públicas relacionadas con Gobierno Digital, protección de datos personales y seguridad de la información.
- ✓ Desarrollo de programas de formación y certificación en tecnologías cloud, ciberseguridad y administración de plataformas.

- ✓ Consolidación de modelos de trabajo híbrido y remoto, que incrementan la necesidad de controles de acceso seguro, autenticación multifactor y gestión de identidades digitales.
- ✓ Crecimiento del mercado de servicios especializados en ciberseguridad, y administración segura de entornos híbridos.
- ✓ Mayor integración entre sector público, academia y empresas tecnológicas para fortalecer capacidades de innovación, investigación y desarrollo tecnológico.
- ✓ Evolución de soluciones de inteligencia artificial aplicadas a monitoreo, detección de amenazas y automatización de controles de seguridad.
- ✓ Incremento de estándares regulatorios y exigencias de cumplimiento que impulsan la adopción de mejores prácticas de seguridad de la información.

La creciente sofisticación de las amenazas cibernéticas ha convertido la seguridad digital en una prioridad estratégica para las organizaciones, favoreciendo la demanda de servicios especializados orientados al fortalecimiento de plataformas tecnológicas críticas y protección de activos digitales.

Amenazas

Las amenazas corresponden a factores externos que pueden afectar el desempeño del sector TIC y de ciberseguridad, así como impactar la ejecución de proyectos tecnológicos especializados.

Entre las principales amenazas identificadas se destacan:

- ✓ Evolución constante y sofisticación de amenazas cibernéticas como ransomware, phishing avanzado, secuestro de identidades digitales y ataques dirigidos a infraestructuras críticas.
- ✓ Escasez global de talento humano especializado en ciberseguridad y seguridad de la información.
- ✓ Alta rotación de profesionales especializados debido a la creciente demanda internacional de perfiles técnicos avanzados.
- ✓ Dependencia tecnológica de fabricantes internacionales y cambios permanentes en licenciamiento, actualizaciones y modelos de servicios cloud.
- ✓ Incremento de ataques dirigidos a servicios en la nube, cuentas privilegiadas y entornos híbridos.
- ✓ Riesgos asociados a configuraciones inseguras, errores humanos y malas prácticas de administración tecnológica.
- ✓ Crecimiento de ataques de ingeniería social potenciados mediante inteligencia artificial

generativa y automatización criminal.

- ✓ Competencia creciente entre proveedores nacionales e internacionales de servicios especializados en ciberseguridad y transformación digital.
- ✓ Cambios regulatorios y mayores exigencias de cumplimiento en protección de datos, seguridad digital y gobierno digital.
- ✓ Dependencia operativa de plataformas tecnológicas críticas que pueden generar impactos significativos ante incidentes de seguridad o indisponibilidad de servicios.

Adicionalmente, la rápida evolución tecnológica obliga a las organizaciones y proveedores del sector a mantener procesos permanentes de actualización técnica, capacitación y adopción de buenas prácticas de seguridad para responder adecuadamente a un entorno digital cada vez más dinámico y complejo.

8. OBJETO.

La necesidad del presente proceso de selección obedece a “REALIZAR PRUEBAS DE CIBERSEGURIDAD, Y EJECUTAR EL PLAN DE SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA EL INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA.”.

9. CAPACIDAD FINANCIERA Y ORGANIZACIONAL.

El IDEA establece las condiciones mínimas que deben cumplir los proponentes de los procesos de contratación para reflejar la respectiva salud financiera y organizacional, permitiendo evaluar la aptitud del proponente para cumplir oportuna y cabalmente el objeto del contrato. De igual manera, para establecer las condiciones mencionadas, se realizó un análisis del comportamiento del sector de acuerdo con la naturaleza del proceso de contratación, su valor, plazo y forma de pago.

El pilar fundamental del análisis financiero está contemplado en la información que proporcionan los estados financieros de la empresa, entre los más conocidos y usados se encuentran el Balance General y el estado de resultados, que son elaborados generalmente, al finalizar cada periodo fiscal.

Uno de los instrumentos más usados para realizar el análisis financiero de las empresas es el uso de indicadores financieros, ya que estos pueden medir el comportamiento de las mismas,

presentando una perspectiva de la situación financiera, mostrando el grado de liquidez, el apalancamiento financiero, su patrimonio y en general lo que tenga que ver con su actividad.

El proponente deberá cumplir con los indicadores financieros exigidos en el presente proceso de selección, los cuales se evaluarán teniendo en cuenta el Registro Único de Proponentes-RUP en firme del último año fiscal, donde conste la información de los Estados Financieros debidamente aprobados.

INDICADORES FINANCIEROS

- ✓ La razón de cobertura de interés: Nos sirve para medir el apalancamiento financiero del proponente, informando sobre el grado en que los intereses son absorbidos por los beneficiarios antes de intereses e impuestos más la amortización.
- ✓ El endeudamiento**:** Nos indica el monto del dinero de terceros que se utilizan para generar utilidades, dichas obligaciones son de gran importancia ya que estas comprometen al proponente en el transcurso del tiempo.
- ✓ La liquidez: Es considerada como la capacidad que se tiene para pagar las obligaciones a corto plazo que se han adquirido a medida que éstas se vencen. Se refiere no solamente a las finanzas del proponente, sino a su habilidad para convertir en efectivo determinados activos.

INDICADORES DE CAPACIDAD ORGANIZACIONAL

- ✓ Rentabilidad sobre el patrimonio: Determina la rentabilidad del patrimonio del proponente, es decir, la capacidad de generación de utilidad operacional por cada peso invertido en el patrimonio.
- ✓ Rentabilidad sobre activos: Determinar la rentabilidad de los activos del proponente, es decir, la capacidad de generación de utilidad operacional por cada peso invertido en el activo:

10. ANÁLISIS DE LA DEMANDA.

Al realizar el proceso por medio de la modalidad de menor cuantía, la entidad pretende que la empresa a la que se le adjudique el contrato sea estable financieramente y reconocida en el mercado; adicional deberá ofrecer algunos servicios en la ciudad de Medellín, para tener una respuesta pronta a los requerimientos que se puedan presentar en el desarrollo del objeto contractual.

Por otra parte, la vigencia y el presupuesto oficial del contrato de ejecución de los insumos objeto de análisis se estableció de acuerdo con la necesidad del Instituto. En el caso de solicitud de garantías, estas se determinarán atendiendo la naturaleza del objeto y actividades a realizar, así como la vigencia de las mismas.

Las demás variables que se tienen establecidas en el presente proceso de selección obedecen expresamente a la contratación del servicio que se está adelantando actualmente, las cuales cumplen con las mismas condiciones establecidas en adquisiciones previas realizadas por el Instituto, lo que demuestra que la condiciones técnicas y presupuestales del presente proceso garantizan pluralidad de oferentes y equilibrio en las utilidades a percibir por el contratista favorecido con la adjudicación del contrato.

Adicional al análisis realizado a las adquisiciones previas que se han adelantado en el Instituto, se identificó y analizó los procesos realizados por otra Entidades Públicas, como se evidencia a continuación.

ADQUISICIONES DE OTRAS ENTIDADES		
ITEM	**ANÁLISIS 1:** INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA	**ANÁLISIS 2**: INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA
Modalidad de Selección del Contratista	Selección abreviada de menor cuantía	Selección abreviada de menor cuantía
Objeto del contrato	Realizar Pruebas de Seguridad y Ciberseguridad, y Ejecutar Plan de Sensibilización Para el Instituto para el Desarrollo de Antioquia – IDEA	Realización de pruebas seguridad a la plataforma tecnológica del Instituto para el Desarrollo de Antioquia
Presupuesto Oficial	$186.294.999 IVA incluido	$ 123.321.867 IVA incluido
Forma de pago	Un primer pago correspondiente al cincuenta por ciento 50% del valor del contrato, una vez se completen las actividades definidas en el alcance del ítem “Pruebas de hackeo ético”, así como la entrega de los informes y registros solicitados, la presentación de las actividades realizadas y previa verificación, aprobación y visto bueno del supervisor designado.	Un primer pago del veinte por ciento (20%) del valor del contrato, cuando se realice la primera prueba de vulnerabilidad, la prueba de hackeo ético y la prueba de hardening. Un segundo pago del veinte por ciento (20%) del valor del contrato cuando se realice la segunda prueba de vulnerabilidad. Un tercer pago del veinte por ciento (20%) del valor del contrato

	Un segundo pago correspondiente al cincuenta por ciento 50% del valor del contrato, una vez se realicé y ejecute el Plan de Sensibilización, la campaña de sensibilización, el taller gamificado, las pruebas de ingeniería social, la entrega de los informes y registros solicitados y la presentación de las actividades realizadas, previa verificación, aprobación y visto bueno del supervisor designado.	cuando se realice el análisis de footprinting. Un cuarto pago del veinte por ciento (20%) del valor del contrato cuando se realice las pruebas de ingeniería social acompañada del informe respectivo. El quinto pago del veinte por ciento (20%) del valor del contrato cuando se realice la actividad de sensibilización en ciberseguridad.
Vigencia del contrato	Desde el inicio de ejecución en la plataforma SECOP II. Hasta el 31 de diciembre de 2025.	Desde la suscripción del acta de inicio hasta el 31 de diciembre de 2023
Comportamiento de los contratistas (imposición de multas)	No reportan.	No reportan.
Garantías exigidas en el proceso.	Garantía de cumplimiento (cumplimiento del contrato, calidad del servicio,	Cumplimiento, calidad del servicio, pago de salarios y prestaciones sociales, otros.

ANÁLISIS: De la información analizada se evidencia que en el Instituto se han adelantado este tipo de procesos contractuales en la modalidad de selección abreviada de menor cuantía, teniendo en cuenta la naturaleza, complejidad técnica y cuantía del servicio requerido.

El presente contrato se adelantará bajo la modalidad de Selección Abreviada de Menor Cuantía, teniendo en cuenta las características técnicas, el alcance especializado de los servicios requeridos y el presupuesto estimado para la contratación.

Las condiciones comúnmente observadas en los procesos de contratación analizados se describen a continuación:

(a) forma de pago: En los contratos revisados se identificó que se establecieron pagos distribuidos según el cumplimiento de las obligaciones contractuales, expedición del recibo a satisfacción por parte del supervisor y verificación de los requisitos legales exigidos para el pago.

Para el presente proceso contractual del IDEA, se realizará en 2 pagos del 50% del valor del contrato cada uno, una vez se hayan ejecutado y recibido a satisfacción las actividades contempladas dentro del alcance contractual.

(b) valor: Se evidencia adicionalmente que el valor del presupuesto oficial varía de acuerdo con la cantidad de insumos requeridos, en razón a los plazos de ejecución, y necesidades.

Las demás condiciones y variables que se tienen establecidas para el presente proceso de contratación obedecen expresamente a la contratación de servicios, los cuales cumplen con las mismas condiciones establecidas en adquisiciones previas realizadas por otras entidades, lo que demuestra que las condiciones técnicas y presupuestales del presente proceso garantizan pluralidad de oferentes y participación activa para su efectiva adjudicación.

11. ANÁLISIS DE LA OFERTA

PROVEEDORES

El sector tecnológico es altamente dinámico y las organizaciones requieren para cumplir con sus objetivos apalancar su estrategia en el uso de las TIC, es por lo que los bienes y servicios que se adquieren se ven impactados directamente por esos cambios tecnológicos, permitiendo así garantizar la seguridad e información que cuenta el IDEA. A continuación, se indican las características del sector y su impacto, que pueden afectar el presente proceso de contratación:

PRESTADORES DEL SERVICIO OBJETO DE CONTRATACIÓN: Consultadas las bases de datos e información registrada en el RUES “Registro único empresarial y social Cámaras de Comercio”, administrado por CONFECÁMARAS, se identificó los siguientes posibles proveedores que se describen a continuación:

- SOFTWARE ONE
- CONTROLES EMPRESARIALES
- WHITE HAT
- WEXLER
- GAMMA INGENIEROS
- SOFISTIC

Con respecto a la prestación de servicios pruebas de seguridad, se puede decir que en el mercado existen varias empresas con la experiencia y competencia suficiente, estas a su vez están representadas en los diferentes países donde operan.

Precio Artificialmente Bajo

Para el presente proceso de selección se tiene un presupuesto oficial estimado en la suma de hasta ciento noventa y seis millones cuatrocientos ochenta y un mil novecientos treinta y dos pesos M/L ($196.481.932) IVA Incluido

Cuando el valor de la oferta sea considerado artificialmente bajo, de conformidad con el precio analizado por el Comité Asesor y Evaluador y el procedimiento establecido en la GUÍA PARA EL MANEJO DE OFERTAS ARTIFICIALMENTE BAJAS EN PROCESOS DE CONTRATACIÓN expedida por Colombia Compra Eficiente. El IDEA requerirá al oferente para que explique las razones que sustenten el valor por él ofertado. Analizadas las explicaciones, el Comité Asesor y Evaluador recomendará al ordenador del gasto del IDEA o su delegado, el rechazo o la continuidad de la oferta en el proceso.

Procederá la recomendación de continuidad de la oferta en el proceso de selección, cuando el valor de la misma responde a circunstancias objetivas del proponente y su oferta, que no ponen en riesgo el proceso, ni el cumplimiento de las obligaciones contractuales en caso de que se adjudique el contrato a dicho proponente, de conformidad con el artículo 2.2.1.1.2.2.4 del Decreto 1082 de 2015.