SELECCIÓN ABREVIADA DE MENOR CUANTIA

Objeto: "ADQUIRIR E IMPLEMENTAR UN SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (Endpoint Detection and Response), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL). PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN."

Clasificación UNSPSC

Tipo	Código	Nombre Producto
Clase	43233200	Software de seguridad y protección
Clase	43222500	Equipo de seguridad de red
Clase	81111800	Servicios de sistemas y administración de componentes de sistemas
Clase	81112200	Mantenimiento y soporte de software

1. Análisis del Mercado

1.1. Aspectos generales del Mercado:

En el contexto local **SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (ENDPOINT DETECTION AND RESPONSE), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL)**

La actividad económica del presente proceso se relaciona con la actividad de Información y Comunicaciones, específicamente con "Otras actividades de tecnologías de información y actividades de servicios informáticos" y siendo la seguridad informática y seguridad de la información uno de los habilitadores transversales de la Política de Gobierno Digital de acuerdo con el Decreto 1008 de 2018, encargado de resolver los problemas de seguridad técnica de una entidad y de apoyar a través de diferentes canales a los colaboradores que normalmente trabajan en diferentes niveles o funciones, se considera que el objeto **"ADQUIRIR E IMPLEMENTAR UN SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (ENDPOINT DETECTION AND RESPONSE), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL) PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN.**", está relacionado directamente con las actividades descritas.

La actividad económica sobre la cual recae el objeto de la presente contratación se encuentra enmarcada en el sector cuaternario *"... Es la cuarta de las divisiones tradicionales del circuito productivo (o sea, de la actividad económica), y en ella se encuentran las actividades y servicios basadas en la acumulación del conocimiento y, por lo tanto, imposibles de mecanizar. En líneas generales, se le denomina como "sector de la investigación".*

El sector cuaternario es uno de los sectores clave en la innovación tecnológica e industrial, esto se debe a que la aplicación de la ciencia y la tecnología al mundo empresarial ha

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

permitido la creación de una infinidad de nuevos bienes y servicios comercializables, así como el mejoramiento de los ya existentes. Por lo tanto, este sector alberga a trabajadores profesionales hiperespecializados y a menudo requiere de grandes inversiones presupuestarias.

Por estos motivos, el sector cuaternario es probablemente el que más ha crecido en el último siglo de la historia humana, aunque sigue siendo mayoritario y predominante en las naciones del llamado "primer mundo", en las que el nivel de desarrollo industrial y tecnológico es elevado, y en las que se cuenta con los altos ingresos que requieren de este tipo de inversiones.

Algunos ejemplos de actividades económicas del sector cuaternario son:

- La industria de la informática y las TIC (tecnologías de información y telecomunicaciones).
- La industria biomédica y de edición genética con fines medicinales.
- La investigación en robótica y en inteligencia artificial.
- La industria aeroespacial y de viajes turísticos al espacio.
- La investigación farmacéutica y bioquímica."
- Tecnología de la información
- Investigación científica
- Cultura
- Educación
- Consultoría

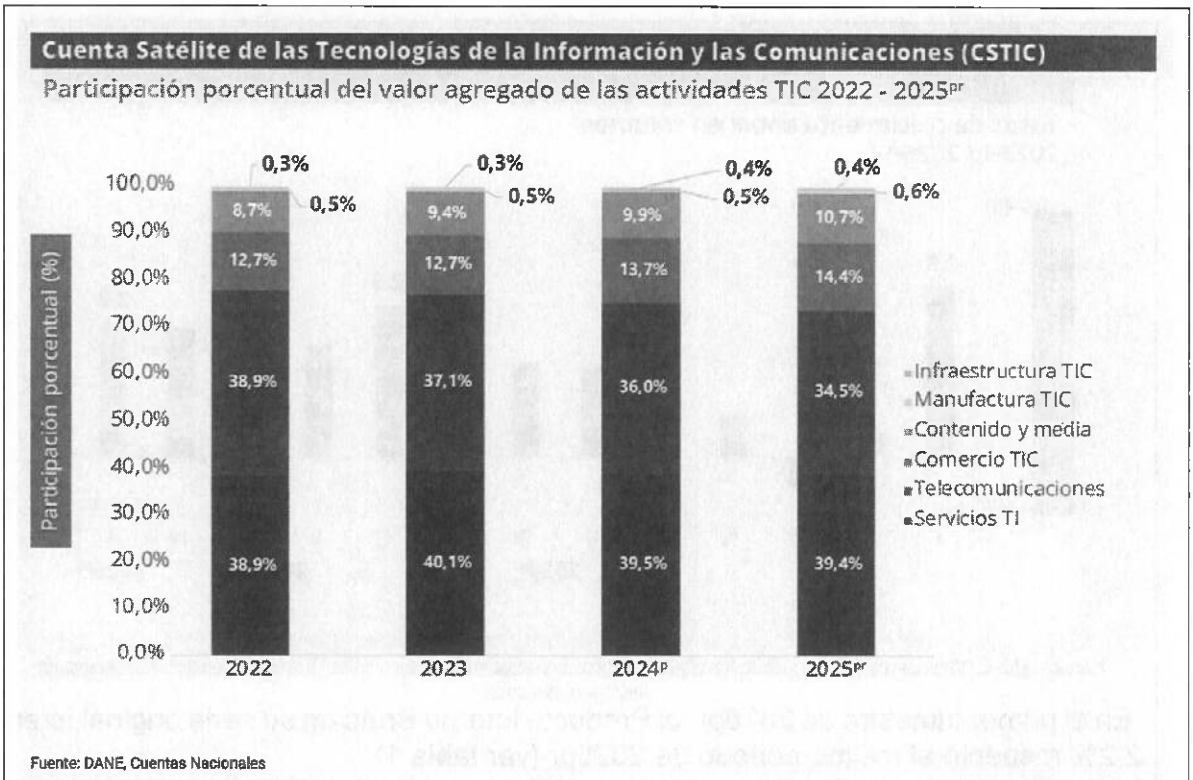
Este sector comprende las actividades económicas basadas en labores intelectuales o en la denominada economía del conocimiento. Así, su valor se obtiene a partir de ideas científicas. Este nuevo sector nace fundamentalmente en el año 2016, año de la investigación, el desarrollo y la innovación; unas actividades propias del sector secundario e industrial, pero que por su importancia estratégica y sus modos propios de producción actualmente permiten hablar de ellas como un sector diferenciado del resto.

De acuerdo con las últimas cifras publicadas por el DANE En 2025pr, el valor agregado bruto del sector TIC ascendió a 58,1 billones de pesos, presentando un crecimiento de 5,5% respecto a 2024p; mientras que en 2024p el valor agregado bruto fue de 55,1 billones de pesos, con un crecimiento de 5,3% con relación a 2023.

El excedente de explotación bruto e ingreso mixto bruto de la CSTIC presentó un crecimiento de 5,2% para 2025pr; En 2024p, este agregado presentó un crecimiento de 3,1% con respecto a 2023.

El sector TIC registró una participación de 3,47% en el valor agregado bruto nacional. En 2024p, esta participación fue de 3,55% mientras que para el período 2022 – 2025pr en promedio participó con el 3,60% del valor agregado bruto nacional.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.



Fuente: DANE, Cuentas Nacionales

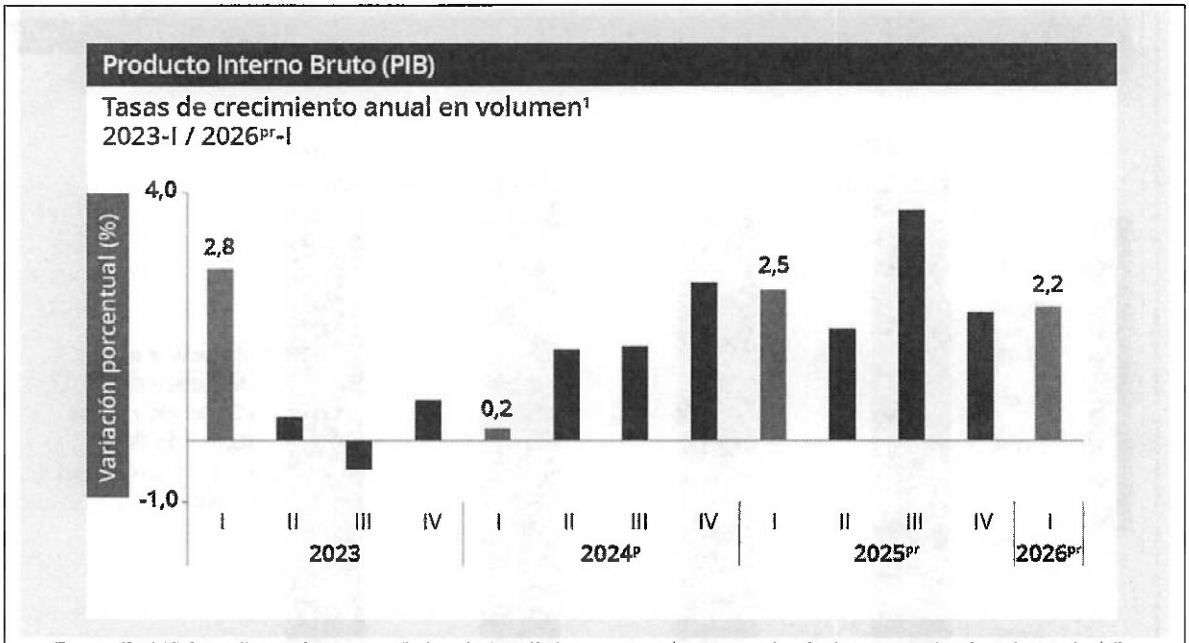
Fuente: Dane. Cuenta satélite tecnologías de la información.

Producto Interno Bruto (PIB)

De acuerdo con el Banco de la República, el PIB se define como el total de bienes y servicios producidos en un país durante un período determinado. En este sentido, constituye un indicador representativo de la dinámica productiva y del crecimiento de la economía en un periodo de tiempo.

Según el último informe técnico publicado por el DANE, correspondiente al En el primer trimestre de 2026pr, el Producto Interno Bruto en su serie original, crece 2,2% respecto al mismo periodo de 2025pr % respecto al mismo periodo de 2024p, mientras que para el total del año 2025pr la economía colombiana creció 2,5%, mostrando una mejora frente al crecimiento observado en 2024.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitaria al correo electrónico atencion.ciudadano@inder.gov.co.



Fuente: DANE. https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-nacionales-trimestrales/pib-informacion-tecnica

En el primer trimestre de 2026pr, el Producto Interno Bruto en su serie original, crece 2,2% respecto al mismo periodo de 2025pr (ver tabla 1).

Las actividades económicas que más contribuyen a la dinámica del valor agregado son:

• Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales crece 5,7% (contribuye 0,9 puntos porcentuales a la variación anual).

• Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida crece 2,9% (contribuye 0,6 puntos porcentuales a la variación anual).

• Industrias manufactureras crece 2,9% (contribuye 0,3 puntos porcentuales a la variación anual).

Respecto al trimestre inmediatamente anterior, el Producto Interno Bruto en su serie ajustada por efecto estacional y calendario crece 0,6%. Cuando se observa el comportamiento de las actividades económicas relacionadas:

• Industrias manufactureras crece 2,3%. • Actividades financieras y de seguros crece 2,2%.

• Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios; Actividades de los hogares individuales en calidad de empleadores; actividades no diferenciadas de los hogares individuales como productores de bienes y servicios para uso propio crece 1,4%.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Tabla 1. Valor agregado por actividad económica
Tasas de crecimiento en volumen[1]
Primer trimestre 2026pr

Actividad económica	Tasas de crecimiento (%)	
	Serie original	Serie ajustada por efecto estacional y calendario
	Anual	Trimestral
	2026pr-I / 2025pr-I	2026pr-I / 2025pr-IV
Agricultura, ganadería, caza, silvicultura y pesca	-1,4	-0,5
Explotación de minas y canteras	-0,1	0,8
Industrias manufactureras	2,9	2,3
Suministro de electricidad, gas, vapor y aire acondicionado[2]	2,6	0,3
Construcción	-5,4	-4,6
Comercio al por mayor y al por menor[3]	2,9	0,2
Información y comunicaciones	1,3	1,1
Actividades financieras y de seguros	2,8	2,2
Actividades inmobiliarias	2,0	0,5
Actividades profesionales, científicas y técnicas[4]	2,2	0,5
Administración pública, defensa, educación y salud[5]	5,7	1,3
Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios[6]	3,2	1,4
Valor agregado bruto	**2,2**	**0,6**
Impuestos menos subvenciones sobre los productos	2,9	0,9
Producto Interno Bruto	**2,2**	**0,6**

Fuente: DANE, PIB_T

Fuente: DANE, PIB.

En el primer trimestre de 2026pr, el valor agregado de información y comunicaciones crece 1,3% en su serie original, respecto al mismo periodo de 2025pr . Para la serie ajustada por efecto estacional y calendario, el valor agregado crece en 1,1%, respecto al trimestre inmediatamente anterior (ver tabla 8).

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Tabla 8. Información y comunicaciones
Tasas de crecimiento en volumen[1]
Primer trimestre 2026[Pr]

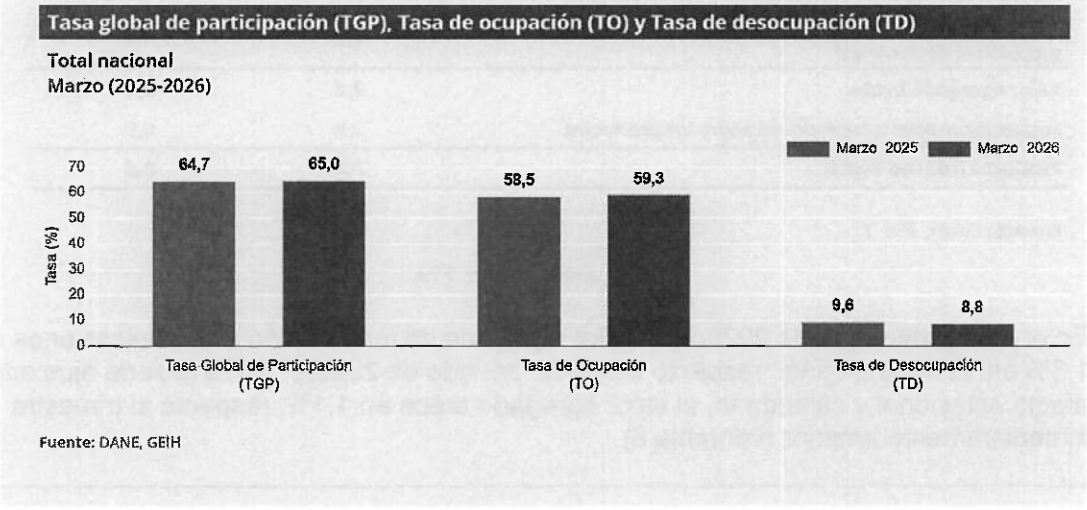
Actividad económica	Tasas de crecimiento (%)	
	Serie original	Serie ajustada por efecto estacional y calendario
	Anual	Trimestral
	2026[Pr]-I / 2025[Pr]-I	2026[Pr]-I / 2025[Pr]-IV
Información y comunicaciones	1,3	1,1

Fuente: DANE, PIB_T

Fuente: DANE, PIB

Población ocupada según rama de actividad

Para marzo de 2026, la tasa de desocupación del total nacional fue 8,8%, lo que representó una disminución de 0,8 puntos porcentuales respecto al mismo mes de 2025 (9,6%). La tasa global de participación se ubicó en 65,0% y la tasa de ocupación en 59,3%, en marzo de 2025 estas tasas fueron 64,7% y 58,5%, respectivamente.

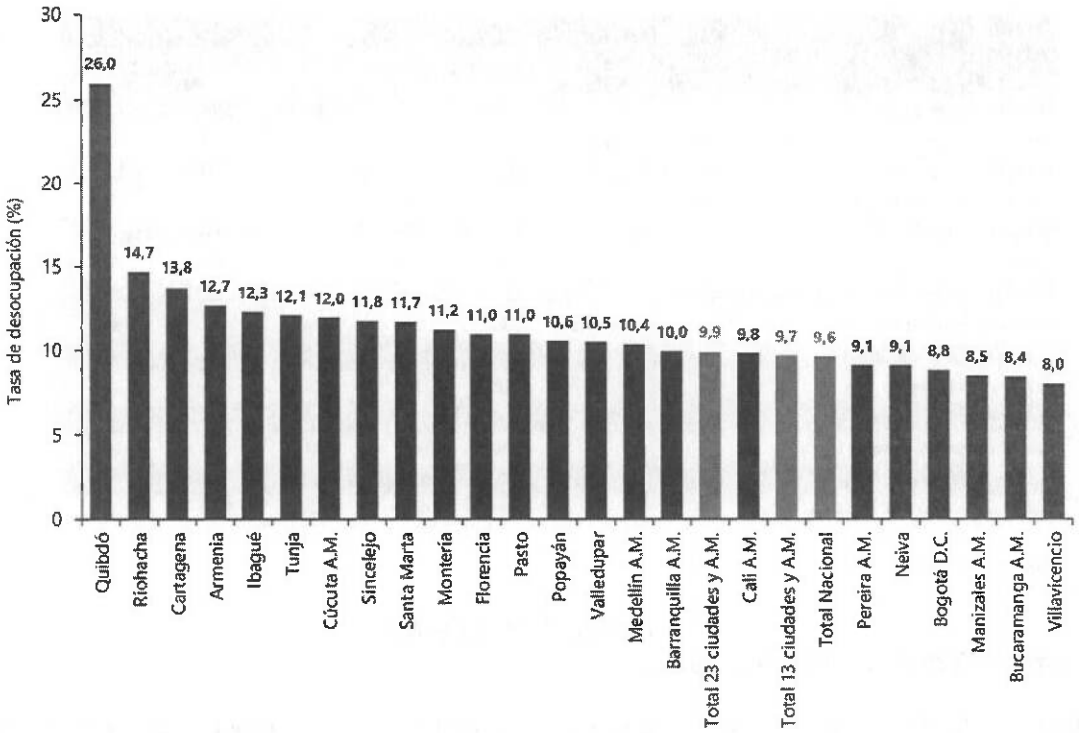


Fuente: Dane. GEIH

Para el trimestre enero - marzo 2026, de las 23 ciudades y áreas metropolitanas, las que presentaron mayores tasas de desocupación fueron: Quibdó (26,0%), Riohacha (14,7%) y Cartagena (13,8%). Las ciudades con menor tasa de desocupación fueron: Manizales A.M. (8,5%), Bucaramanga A.M. (8,4%) y Villavicencio (8,0%).

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Gráfico 6. Tasa de desocupación según ciudades
Total nacional y 23 ciudades y áreas metropolitanas
Enero - marzo 2026



Fuente: DANE, GEIH.

Fuente: Dane. GEIH

En marzo de 2026, el número de personas ocupadas en el total nacional fue 24.352 mil personas. Las ramas que más aportaron positivamente a la variación de la población ocupada fueron Administración pública y defensa, educación y atención de la salud humana (1,6 puntos porcentuales); Actividades financieras y de seguros (1,0 puntos porcentuales) y Suministro de electricidad, gas, agua y gestión de desechos^ (0,5 puntos porcentuales).

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Tabla 1. Distribución porcentual, variación absoluta y contribución a la variación de la población ocupada según rama de actividad
Total nacional
Marzo (2025 - 2026)

Rama de actividad	Total nacional				
	Marzo 2025	Marzo 2026	Distribución % 2026	Variación absoluta	Contribución en p.p.
Población ocupada	**23.702**	**24.352**	**100**	**650**	
Administración pública y defensa, educación y atención de la salud humana	2.659	3.028	12,4	369	1,6
Actividades financieras y de seguros	319	559	2,3	239	1,0
Suministro de electricidad, gas, agua y gestión de desechos^	583	708	2,9	125	0,5
Comercio y reparación de vehículos	4.179	4.284	17,6	106	0,4
Construcción	1.662	1.744	7,2	82	0,3
Actividades profesionales, científicas, técnicas y servicios administrativos	1.778	1.844	7,6	67	0,3
Actividades artísticas, entretenimiento, recreación y otras actividades de servicios	1.987	2.027	8,3	40	0,2
Alojamiento y servicios de comida	1.723	1.753	7,2	30	0,1
Actividades inmobiliarias	328	332	1,4	4	0,0
Transporte y almacenamiento	1.770	1.769	7,3	0	0,0
Información y comunicaciones	407	402	1,7	-4	0,0
Industrias manufactureras	2.623	2.457	10,1	-166	-0,7
Agricultura, ganadería, caza, silvicultura y pesca	3.685	3.443	14,1	-242	-1,0

Fuente: DANE, GEIH.

Fuente: Dane. GEIH

Gremios, Federaciones y Asociaciones

Algunas de las asociaciones y gremios relevantes en Colombia que podrían estar relacionadas con este servicio son las siguientes:

- Asociación Colombiana de Ingenieros- ACIEM.
- Asociación Nacional de Empresas de Servicios Públicos Domiciliarios y Actividades Complementarias e Inherentes - ANDESCO
- Asociación Nacional de Medios de Comunicación-ASOMEDIOS.
- Cámara Colombiana de Informática y Telecomunicaciones- CCIT.
- Centro de Investigación de las Telecomunicaciones -CINTEL-
- Federación Colombiana de la Industria de Software y Tecnologías Informativas Relacionadas –FEDESOFT.

Asociación de Operadores de Tecnologías de Información y Comunicaciones de Colombia
Asociación Colombiana de Ingenieros de Sistemas -ACIS.

1.2. Perspectiva económica:

Los factores que influyen en el poder de compra de un **SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (ENDPOINT DETECTION AND RESPONSE), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL)**

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Presupuesto gubernamental: El poder de compra de las entidades estatales está directamente relacionado con el presupuesto asignado por el gobierno. Un mayor presupuesto puede permitir la adquisición de mayor número de bienes y servicios.

- Inflación y depreciación: La inflación y la depreciación de la moneda puede afectar el poder adquisitivo de las entidades estatales y otros compradores. Una inflación alta puede reducir el poder de compra, mientras que una devaluación de la moneda incrementa el precio de las materias primas, la maquinaria, los equipos, los bienes de capital y, en especial, el de los insumos agrícolas, lo cual posteriormente se traslada al precio final.

(IPC): Indicador económico, cuyo valor numérico refleja las variaciones que experimentan los precios en un período determinado de tiempo. En abril de 2026 la variación anual del IPC fue 5,68%, es decir, 0,66 puntos porcentuales mayor que la reportada en el mismo periodo del año anterior, cuando fue de 5,16%.

IPC	Abril					
	Variación mensual		Variación año corrido		Variación anual	
	2025	2026	2025	2026	2025	2026
IPC total	0,66	**0,78**	3,30	**3,87**	5,16	**5,68**

Fuente: DANE, IPC

Fuente: DANE, Índice de Precios al Consumidor

En el mes de abril de 2026, el IPC registró una variación de 0,78% en comparación con marzo de 2026, tres divisiones se ubicaron por encima del promedio nacional (0,78%): Alimentos y bebidas no alcohólicas (1,51%), Muebles, artículos para el hogar y para la conservación ordinaria del hogar (1,06%) y por último, Transporte (0,81%). Por debajo se ubicaron: Alojamiento, agua, electricidad, gas y otros combustibles (0,70%), Salud (0,70%), Bienes y servicios diversos (0,63%), Recreación y cultura (0,58%), Bebidas alcohólicas y tabaco (0,54%), Prendas de vestir y calzado (0,45%), Restaurantes y hoteles (0,34%), Educación (0,07%) y por último, Información y comunicación (-0,05%).

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Divisiones de Gasto	Peso (%)	2025 Variación (%)	2025 Contribución Puntos Porcentuales	2026 Variación (%)	2026 Contribución Puntos Porcentuales
Alimentos y bebidas no alcohólicas	15,06	1,10	0,21	1,51	0,29
Muebles, artículos para el hogar y para la conservación ordinaria del hogar	4,19	0,53	0,02	1,06	0,04
Transporte	12,93	0,49	0,07	0,81	0,11
TOTAL	100,00	0,66	0,66	0,78	0,78
Alojamiento, agua, electricidad, gas y otros combustibles	33,12	0,74	0,23	0,70	0,22
Salud	1,71	0,38	0,01	0,70	0,01
Bienes y servicios diversos	5,36	0,61	0,03	0,63	0,03
Recreación y cultura	3,79	0,45	0,01	0,58	0,02
Bebidas alcohólicas y tabaco	1,70	0,38	0,01	0,54	0,01
Prendas de vestir y calzado	3,98	0,40	0,01	0,45	0,01
Restaurantes y hoteles	9,43	0,63	0,07	0,34	0,04
Educación	4,41	0,03	0,00	0,07	0,00
Información y comunicación	4,33	-0,19	0,00	-0,05	0,00

Fuente: DANE, IPC

Fuente: DANE, Índice de Precios al Consumidor

La depreciación (o la apreciación) del peso frente a otras monedas influye en los diferentes indicadores externos de la economía colombiana. Por ejemplo, en el caso específico de una depreciación -cuando comprar un dólar se hace más costoso-, en la cuenta corriente se puede esperar una mejora en la balanza comercial debido a que:

El valor importado puede disminuir: el encarecimiento de los productos importados influye en las decisiones de compra de los consumidores nacionales, lo que hace más probable que disminuya el consumo de productos importados y se sustituya a favor de los productos locales.

El valor exportado puede aumentar: los exportadores reciben más pesos por cada dólar que venden en los mercados internacionales. Estos mayores ingresos en pesos les pueden permitir realizar las inversiones que aumenten su capacidad productiva, y esto hace más probable que incrementen las cantidades exportadas a los mercados internacionales.

Otros índices económicos representativos: factores como el crecimiento económico, el desempleo, los niveles de inversión pública y privada, y las políticas fiscales también pueden influir en el poder de compra y los patrones de gasto de las entidades estatales y otros compradores. Un entorno económico favorable puede estimular la demanda de estos servicios, mientras que condiciones desfavorables pueden tener el efecto opuesto.

El Banco de la República define la Tasa Representativa del Mercado (TRM) como la cantidad de pesos colombianos por un dólar de los Estados Unidos. Esta tasa es calculada y certificada diariamente por la Superintendencia Financiera de Colombia, con base en las operaciones registradas en el mercado cambiario.
En este contexto, la tasa de cambio constituye una variable relevante dentro del análisis económico del sector, dado que variaciones significativas del tipo de cambio pueden impactar:

- Costos asociados a bienes y servicios transados en mercados internacionales;
- Precios de tecnología, insumos y servicios especializados;
- Presupuestos de adquisición y capacidad de compra de las entidades;
- Proyecciones de costos y condiciones generales del mercado.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los tituiares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Por lo anterior, el comportamiento de la TRM se considera un factor externo con incidencia potencial sobre la dinámica económica y las condiciones del sector analizado.

TRM: En los últimos dos años, la Tasa Representativa del Mercado (TRM) en Colombia ha experimentado fluctuaciones significativas. En octubre de 2023, la TRM se ubicó alrededor de $4,200 pesos por dólar, mientras que en octubre de 2024, alcanzó un valor de $4,404.92 pesos por dólar, lo que representa un aumento del 4.88% en comparación con el mismo período del año anterior. Sin embargo, en lo que va de 2026, la TRM ha mostrado una tendencia a la baja, con un valor cercano a los 3.103,28 pesos por dólar en febrero de 2026.

La TRM ha estado influenciada por factores económicos internos y externos, como la política monetaria del Banco de la República, la situación económica global y los precios del petróleo. En 2024, la TRM alcanzó un máximo de $4,504.55 pesos por dólar en marzo, mientras que en 2025, el máximo fue de $4,441 pesos por dólar en enero. La tendencia actual sugiere que la TRM podría seguir fluctuando en torno a los $3,650-$4,000 pesos por dólar en los próximos meses, dependiendo de la evolución de la economía colombiana y global.

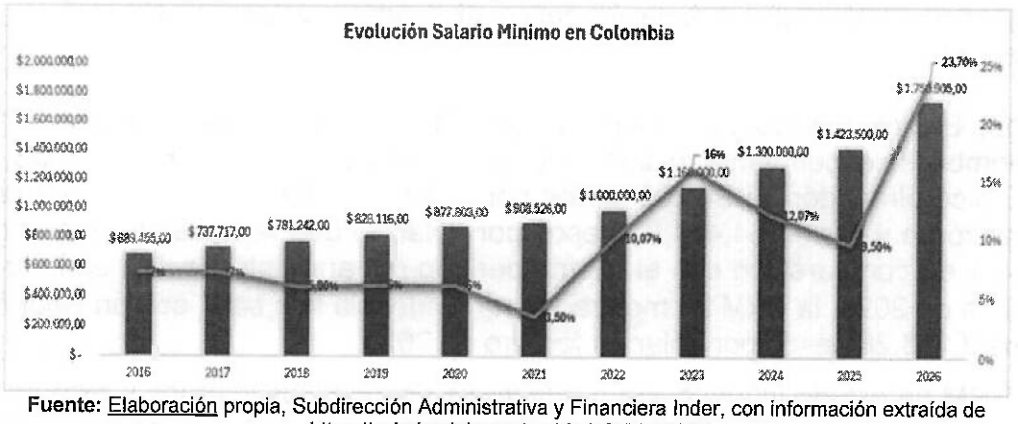


https://www.banrep.gov.co/es/estadisticas/trm

- ***Salario Mínimo Legal Vigente en Colombia***

Se trae a colación en el presente estudio el salario mínimo legal, pues este puede tener un impacto significativo en el comercio al afectar tanto a los consumidores como a las empresas en términos de demanda, costos laborales, competitividad y distribución del ingreso.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.



Fuente: Elaboración propia, Subdirección Administrativa y Financiera Inder, con información extraída de https://salariominimocolombia.info/historico

De forma particular el incremento para el salario mínimo que regirá en 2026 estuvo sin acuerdos durante el mes diciembre, en medio de una negociación llena de tensiones en la mesa tripartita de concertación. Por esta razón el lunes 29 de diciembre, vísperas a la celebración de Fin de año, el presidente Gustavo Petro firmó el decreto que fijó la subida del salario mínimo en 23,78% cifra histórica que promete grandes impactos en la economía local.

- **Salario mínimo y los costos que implica para las empresas**

Es importante tener en cuenta que contratar un trabajador no se limita al salario recibido por el trabajador. Para las empresas, el costo real incluye una serie de pagos adicionales que muchas veces pasan desapercibidos para el empleado, entre esos rubros están los aportes a salud, pensión, riesgos laborales y cajas de compensación, además de las prestaciones sociales: prima, cesantías, intereses a las cesantías y vacaciones. Es por esto por lo que cuando se gesta un incremento en el salario mínimo, todos estos valores también aumentan de forma automática. Con el nuevo Salario Mínimo el costo mensual de un empleado corresponde aproximadamente a la suma de 2.975.000 pesos.

- **Tasa Interbancaria (TIB)**

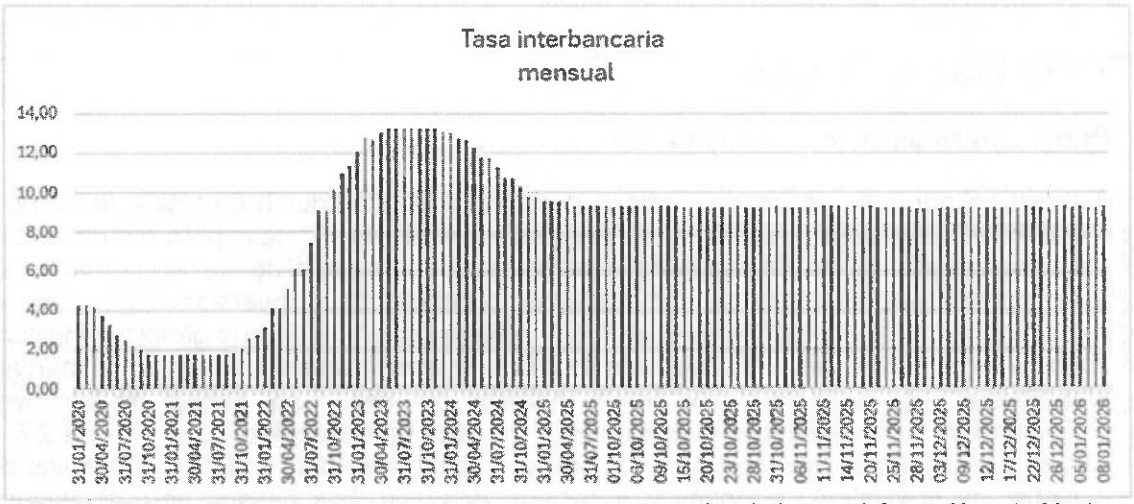
La tasa de interés interbancaria puede ser definida como el termómetro del mercado financiero. Este indicador, refleja el riesgo crediticio asociado con las contrapartes involucradas en las operaciones y las condiciones de liquidez en el mercado monetario local. La TIB es calculada por el Banco de la República y la fórmula utilizada para su cálculo corresponde al promedio ponderado por monto de estos préstamos interbancarios.

En los últimos 12 meses, la tasa de interés interbancaria en Colombia ha experimentado variaciones significativas. Según datos del Banco de la República, la tasa interbancaria se ubicó en 9,21% en octubre de 2025, lo que representa una disminución en comparación con los meses anteriores. En octubre de 2024, la tasa

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

estaba en 9,248%, mientras que en julio de 2025 se mantuvo estable en 9,25%. A lo largo del año pasado, la tasa ha fluctuado entre 9,21% y 9,52%, reflejando las condiciones cambiantes del mercado monetario y la política monetaria del Banco Central.

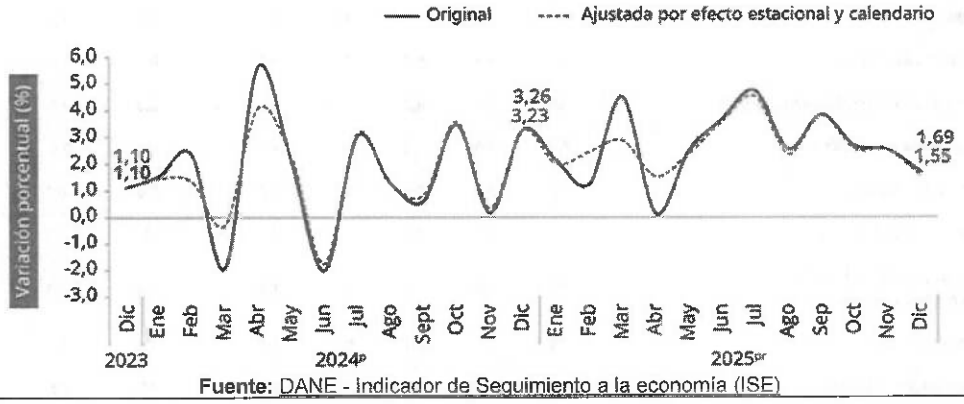
La disminución de la tasa interbancaria en los últimos meses puede atribuirse a la política monetaria expansionista implementada por el Banco de la República para estimular la economía. Sin embargo, la tasa sigue siendo relativamente alta en comparación con el promedio histórico, lo que sugiere que el banco central sigue siendo cauteloso con la inflación y las condiciones económicas globales.



Fuente: Elaboración propia, Subdirección Administrativa y Financiera Inder, con información extraída de Banrepublica.

Indicador de seguimiento a la economía (ISE)

De acuerdo con el Boletín actualizado por el DANE, el 16 de febrero de 2026, para el mes de diciembre de 2025pr el ISE en su serie original, se ubicó en 141,19, lo que representó un crecimiento de 1,69% respecto al mes de diciembre de 2024p (138,85).



Fuente: DANE - Indicador de Seguimiento a la economía (ISE)

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Otros índices económicos representativos:

Factores como el crecimiento económico, el comportamiento del empleo, los niveles de inversión pública y privada, la inflación, la tasa de cambio y las políticas fiscales pueden influir en el poder de compra y en los patrones de gasto de las entidades estatales y demás agentes del mercado. Un entorno económico favorable puede estimular la demanda de bienes y servicios, fortalecer la inversión y mejorar las condiciones del mercado; mientras que condiciones económicas menos favorables pueden generar restricciones presupuestales, mayores costos y ajustes en las decisiones de adquisición.

1.3. Perspectiva internacional:

Perspectivas de la economía mundial

A pesar del aumento de las tensiones comerciales y la incertidumbre política, la economía mundial se ha mantenido resiliente. El crecimiento del último año se explica por un aumento del comercio exterior en anticipación del aumento de aranceles al comercio internacional, la adaptación de las cadenas de suministro, un aumento de la inversión relacionada con proyectos de inteligencia artificial y un fuerte apetito por el riesgo que genera condiciones financieras holgadas. Sin embargo, más de una cuarta parte de las economías de mercados emergentes y en desarrollo aún tienen ingresos per cápita por debajo de los niveles prepandemia. Se espera que el crecimiento mundial se desacelere este año en 2,6 por ciento. Los países de ingreso bajo y los países frágiles enfrentan desafíos crecientes para sostener su crecimiento económico y generar empleos. Los riesgos para el escenario internacional continúan sesgados a la baja, incluyendo el aumento de las barreras comerciales y el estrés en los mercados financieros. La cooperación global y las reformas domésticas siguen siendo fundamentales para apoyar el crecimiento a largo plazo y la generación de empleo.

	PIB real (%)					Revisión*		
	2023	2024	2025e	2026f	2027f	2025e	2026f	2027f
Mundo	2.8	2.8	2.7	2.6	2.7	0.4	0.2	0.1
Economías avanzadas	1.6	1.7	1.7	1.6	1.6	0.5	0.2	0.0
Economías emergentes y en desarrollo	4.4	4.3	4.2	4.0	4.1	0.3	0.2	0.2
Asia oriental y el Pacífico	5.2	5.0	4.8	4.4	4.3	0.3	0.4	0.3
Europa y Asia central	3.6	3.6	2.4	2.4	2.7	0.0	-0.1	0.0
América Latina y el Caribe	2.4	2.4	2.2	2.3	2.6	-0.1	-0.1	0.0
Oriente Medio y Norte de África, Afganistán y Pakistán	2.1	2.6	3.1	3.6	3.9	0.4	-0.1	-0.1
Asia meridional	8.0	6.3	7.1	6.2	6.5	1.0	-0.2	0.0
África al sur del Sahara	3.0	3.7	4.0	4.3	4.5	0.3	0.2	0.2

Fuente: https://www.bancomundial.org/es/publication/global-economic-prospects

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

En cuanto a la economía colombiana, "las tensiones comerciales y la incertidumbre que estas conllevan siguen siendo elevadas. Además, la demanda interna permanece en niveles bajos en algunos países, lo que contrarrestará en parte el efecto positivo de la flexibilización de las condiciones financieras", asegura el Banco Mundial.

Para el caso específico de Colombia, el Banco Mundial proyecta que la economía se expandirá un 2,6 por ciento en este 2026 y otro 2,8 por ciento de cara al 2027, lo que significa un ajuste respecto a su proyección anterior de 2,7 y 2,9 por ciento, respectivamente. "Este crecimiento se apoyará de un consumo resiliente y de la recuperación gradual de la inversión privada".

1.4. Perspectiva técnica:

SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (ENDPOINT DETECTION AND RESPONSE), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL)

Desde la perspectiva técnica, el mercado de soluciones de seguridad ha evolucionado de forma significativa en los últimos años, migrando desde herramientas aisladas y reactivas hacia soluciones especializadas, inteligentes y orientadas a la prevención, detección y respuesta. Las tecnologías tradicionales basadas exclusivamente en firmas han sido complementadas y, en determinados escenarios, superadas por soluciones de nueva generación que incorporan inteligencia artificial, aprendizaje automático, análisis de comportamiento, detección basada en anomalías y mecanismos automatizados de protección. En este escenario, las soluciones de EDR (Endpoint Detection and Response) han adquirido especial relevancia al proporcionar capacidades avanzadas de monitoreo, detección, investigación y respuesta sobre los dispositivos y servidores que hacen parte de la infraestructura tecnológica.

Uno de los principales avances tecnológicos en este mercado es la consolidación de capacidades de seguridad que permiten proteger de manera coordinada los diferentes componentes utilizados por las organizaciones, donde EDR, protección de correo electrónico, herramientas colaborativas y WAF contribuyen a establecer diferentes capas de protección. Estas tecnologías operan principalmente mediante plataformas centralizadas y modelos SaaS o servicios en la nube, facilitando la administración, actualización y aplicación uniforme de políticas de seguridad. Este enfoque permite a las entidades mejorar la visibilidad sobre los dispositivos, usuarios, comunicaciones y aplicaciones web, reducir los tiempos de detección y respuesta, fortalecer la prevención frente a amenazas y disponer de mecanismos de administración centralizada más eficientes. Así mismo, contribuye a establecer controles de seguridad que consideran de manera continua el comportamiento de los dispositivos, usuarios y servicios tecnológicos.

La integración de estas capacidades amplía de manera significativa la cobertura de seguridad institucional, al incorporar la protección de los dispositivos, el correo

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

electrónico, las herramientas utilizadas para la colaboración y las aplicaciones y servicios web expuestos a Internet. El EDR permite identificar comportamientos sospechosos y actividades maliciosas en endpoints y servidores; la protección de correo electrónico permite prevenir amenazas como phishing, malware, suplantación y archivos maliciosos; las herramientas colaborativas incorporan controles para proteger la información y las comunicaciones realizadas mediante plataformas de productividad; y el WAF proporciona protección especializada para aplicaciones web y servicios digitales. La utilización coordinada de estos controles permite establecer diferentes barreras de protección frente a campañas que pueden involucrar simultáneamente usuarios, dispositivos, correo electrónico, archivos, aplicaciones y servicios publicados en Internet.

Actualmente, el mercado ofrece una amplia disponibilidad de soluciones maduras y especializadas que integran estas capacidades, con fabricantes como Microsoft, Sophos, Fortinet, Palo Alto Networks, Trend Micro, CrowdStrike y SentinelOne, entre otros, cuyas plataformas permiten implementar funciones de protección, detección, monitoreo y respuesta de acuerdo con las necesidades de cada organización. Estas soluciones, disponibles principalmente bajo esquemas de suscripción y servicios en la nube, facilitan su adopción por parte de entidades públicas al reducir la necesidad de infraestructura local, acelerar los tiempos de implementación y permitir la actualización continua de los mecanismos de seguridad frente a nuevas amenazas. Adicionalmente, estos modelos facilitan la administración de ambientes tecnológicos con diferentes tipos de dispositivos, usuarios, servicios de correo, herramientas colaborativas y aplicaciones expuestas a Internet.

Importancia de contar con EDR, protección de correo electrónico, herramientas colaborativas y WAF

Para una entidad pública como el INDER Medellín, contar con capacidades integradas de protección para endpoints, correo electrónico, herramientas colaborativas y aplicaciones web no constituye únicamente una necesidad técnica, sino un componente estratégico para la protección de sus activos digitales, la continuidad operativa y la confianza institucional. En un entorno donde las amenazas cibernéticas evolucionan de forma constante y se vuelven cada vez más sofisticadas, la protección aislada de los activos tecnológicos resulta insuficiente; por ello, se requiere un modelo de seguridad por capas que permita prevenir, detectar, analizar y responder oportunamente a eventos que puedan comprometer los dispositivos, las comunicaciones, la información institucional y los servicios digitales expuestos a Internet.

El EDR constituye un control fundamental para la protección de los equipos de usuario y servidores, al proporcionar capacidades avanzadas para identificar comportamientos anómalos, actividades maliciosas y técnicas utilizadas por los atacantes, así como para facilitar acciones de contención y respuesta. Estas capacidades permiten complementar la protección tradicional contra malware con mecanismos basados en comportamiento, aprendizaje automático y análisis de actividades ejecutadas en los dispositivos. Por su

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

parte, la protección de correo electrónico constituye una barrera esencial frente a una de las principales vías de ingreso de amenazas a las organizaciones, mediante la identificación y bloqueo de campañas de phishing, malware, ransomware, archivos y enlaces maliciosos, suplantación de identidad y mensajes no deseados, reduciendo el riesgo de compromiso de las cuentas y dispositivos institucionales.

Las herramientas colaborativas cumplen igualmente un papel relevante en la protección de la información institucional, debido a que permiten el intercambio de archivos, documentos, mensajes y demás contenidos entre usuarios internos y externos. En este contexto, resulta necesario disponer de mecanismos que permitan aplicar controles de seguridad sobre la información compartida, identificar actividades potencialmente riesgosas y proteger los contenidos frente a accesos, archivos o comportamientos que puedan representar una amenaza. De manera complementaria, el WAF (Web Application Firewall) cumple un rol crítico en la protección de portales web, aplicaciones institucionales, APIs y servicios expuestos a Internet, mitigando amenazas dirigidas a la capa de aplicación como inyecciones SQL, cross-site scripting (XSS), explotación de vulnerabilidades, ataques automatizados, abuso de servicios web y otras técnicas utilizadas para comprometer aplicaciones.

En este contexto, la adecuada implementación de estas tecnologías permite establecer controles específicos para cada uno de los principales vectores de ataque asociados al uso de dispositivos, correo electrónico, plataformas colaborativas y servicios web. El EDR proporciona visibilidad y capacidades de detección y respuesta sobre endpoints y servidores; la protección de correo electrónico permite analizar y bloquear contenidos y comunicaciones potencialmente maliciosas; las herramientas colaborativas permiten fortalecer la protección de la información compartida y de los mecanismos de colaboración; y el WAF protege las aplicaciones y servicios publicados frente a ataques dirigidos a la capa web. La aplicación coordinada de estos controles permite fortalecer la prevención, facilitar la identificación de eventos de seguridad y establecer mecanismos oportunos de contención y protección de acuerdo con la naturaleza de cada amenaza.

En consecuencia, para el INDER Medellín, la adopción de soluciones especializadas de EDR, protección de correo electrónico, herramientas colaborativas y WAF representa una decisión técnicamente sólida, alineada con las tendencias actuales de ciberseguridad y con las necesidades de protección de las entidades públicas. Este enfoque permite fortalecer las capacidades institucionales de prevención, detección y respuesta frente a incidentes que puedan afectar los dispositivos, servidores, usuarios, comunicaciones, información y servicios digitales, contribuyendo además a la continuidad de las operaciones, la protección de los datos institucionales y el mantenimiento de la integridad, disponibilidad y confidencialidad de la información.

ALCANCE DE LA CAPACIDAD OPERATIVA DEL SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR, PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Las soluciones deberán proporcionar de manera coherente y completamente interoperable capacidades de protección para Endpoints y servidores mediante EDR, correo electrónico, espacios de trabajo colaborativo, y sitios web, permitiendo la prevención, detección y respuesta ante amenazas de seguridad, así como el análisis y gestión de eventos e incidentes de seguridad, garantizando la trazabilidad de las acciones de protección y respuesta.

La solución deberá disponer de mecanismos de gestión centralizada que faciliten la operación, monitoreo y administración de los componentes de seguridad desde una interfaz unificada o integrada. Asimismo, deberá contar con garantía y soporte del fabricante y cumplir con las siguientes capacidades técnicas:

2.1.1. DIMENSIONAMIENTO DE LA SOLUCIÓN: A continuación, se realiza una discriminación de las especificaciones técnicas requeridas para satisfacer el objeto contractual:

I. **WAF (WEB APPLICATION FIREWALL):**

La plataforma deberá ser desplegadas y administrada en nube. Soportar la protección de aplicaciones institucionales expuestas a internet en entornos de computación en la nube, garantizando operación continua, escalabilidad automática, alta disponibilidad y balanceo de carga, bajo arquitectura de capa siete (HTTP/HTTPS). Estas capacidades deberán permitir la inspección, prevención y mitigación de ataques contra aplicaciones, la aplicación de políticas de seguridad administradas, así como la capacidad para auditoría, análisis forense y trazabilidad del tráfico. Para este propósito, la plataforma deberá soportar, como mínimo, una capacidad equivalente a la siguiente.

Con el fin de que los Proponentes tengan un panorama claro acerca del estado actual del consumo del WAF, se procede a brindar la siguiente información:

- **Datos actuales:**

- throughput promedio últimos 6 meses: 3.1 MB/s
- RPS promedio últimos 6 meses: 100
- Crecimiento últimos dos años 2 MB/s
- Sitios Web protegidos: 10.
- Transferencia total mensual: 8 TB
- Pico máximo últimos 6 meses 12.42 MB/s

Con la finalidad de que el Contratista que resulte adjudicado pueda solventar los picos de consumo, se recomienda presupuestar el consumo diario descrito a continuación:

- Se solicita un throughput promedio de 14.3 MB/s. Este se calcula de la siguiente manera: redondeamos el actual throughput a 3,5 MB/s en promedio y sumamos un crecimiento proyectado de 2 MB/s para los próximos 12 meses, esta suma da como

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

resultado 5.5 MB/s al cual le sumamos 160 % de holgura para atender variaciones o picos de consumo durante la vigencia del servicio.

Pormenorización de los Datos de Requerimiento Mínimo Exigido:

- throughput promedio = (3.5+2) x 2.6) = 14.3MB/s
- Sitios Web a proteger: 10 sitos.
- Transferencia mensual mínima: 15 TB
- Conexiones persistentes requeridas 12.500 (si aplica)
- Validación del servicio: La solución debe estar en capacidad en realizar chequeos de salud (health checks) a servicios y/o aplicaciones, con el fin de detectar de forma proactiva el estado de los diferentes componentes de los servicios, para reaccionar de forma proactiva a una posible falla o indisponibilidad.

El INDER protegerá máximo 10 sitios web de su propiedad. Esta es una cantidad fija que ya incorpora el crecimiento máximo proyectado por la Entidad para el periodo de ejecución de las licencias, por lo que no se presentará incremento superior a 10 sitios durante la vigencia de contrato.

El Contratista deberá prever, presupuestar y garantizar la capacidad mínima requerida y antes referenciada. De esta manera podrá atender eventuales incrementos en el consumo del WAF durante la ejecución del contrato y vigencia de las licencias, asegurando la continuidad de la protección de seguridad sin generar costos adicionales para el INDER Medellín por encima del presupuesto adjudicado. Para tal efecto, se recomienda considerar en su propuesta económica el consumo total diario estimado descrito.

El contratista también podrá proponer estrategias, mecanismos, políticas de usabilidad de los datos con la finalidad de disminuir los riesgos de picos en las transferencias.

II. PROTECCIÓN ENDPOINTS Y SERVIDORES.

Para el dimensionamiento de esta solución, la Entidad suministra como referencia los siguientes parámetros:

- Número de EndPoints existentes, número de servidores existentes y número de licencias endpoints de reserva.

El licenciamiento para 1.020 EndPoints y servidores no tendrá crecimiento durante la vigencia de las licencias, esta cantidad es fija y ya contempla el incremento máximo proyectado de equipos para el periodo de la vigencia de las licencias. La cantidad comprende 900 EndPoints, 20 servidores on premise y 100 licencias para respaldar el posible crecimiento proyectado de los EndPoints.

III. PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS.

Para el dimensionamiento de esta solución, la Entidad suministra los siguientes parámetros:

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

El INDER Medellín cuenta con M365, Se debe tener presente que el INDER actualmente cuenta con 2.300 cuentas de usuario de correo electrónico, que corresponden a una cantidad fija que no tendrá crecimiento durante la ejecución del contrato y la vigencia de las licencias, toda vez que este número ya considera el margen máximo de usuarios previsto por la Entidad.

Importante: Se aceptarán soluciones de cualquier fabricante, siempre que la totalidad de los componentes, funcionalidades y módulos que conformen la solución ofertada sean provistos por un único fabricante.

INICIO DE LA VIGENCIA DE LAS LICENCIAS

El Contratista deberá realizar, con anterioridad al 1 de noviembre de 2026, todas las actividades necesarias para la configuración, instalación, puesta en funcionamiento y verificación del sistema de ciberseguridad, incluyendo las respectivas pruebas de funcionamiento y la entrega del informe de instalación. Lo anterior deberá revisado y ser recibido a satisfacción por parte del supervisor y del apoyo técnico antes de dicha fecha, con el fin de garantizar que las licencias puedan iniciar su vigencia el 1 de noviembre de 2026.

IV. IMPLEMENTACIÓN Y SOPORTE TÉCNICO.

La Entidad requiere Soporte Técnico durante 12 meses de la Plataforma de Ciberseguridad, la cual deberá contar como mínimo con las siguientes características:

1- Actualizaciones y mantenimiento de producto o Compatibilidad con nuevos sistemas operativos, acceso a versiones nuevas sin costo adicional dentro de la vigencia.
2- Deberá incluir atención remota telefónica 24/7, asistencia para configuración y despliegue, guías técnicas, manuales y base de conocimientos y SLA (acuerdo de nivel de servicio).
3- Deberá contar con medios de escalamiento que deberá corresponder como mínimo a una Plataforma helpdesk con usuario y contraseña.
4- Transferencia de Conocimiento: La actividad de transferencia de conocimiento inicial sobre uso del producto deberá ser como mínimo de 20 horas que será prestado a mínimo tres Contratista que forman parte del Equipo Técnico del INDER.
   La capacitación o actividad de transferencia del conocimiento deberá contar dentro de sus temáticas con las siguientes: a) laboratorios de aprendizaje de uso de la solución para administradores o equipos técnicos, documentación de mejores prácticas; b) Interfaz de administración
5- Recuperación, restablecimiento o migración sin costo adicional, en caso de que aplique.

En materia de implementación deberá realizar todas las actividades necesarias para la configuración, instalación, puesta en funcionamiento y verificación del sistema de ciberseguridad, incluyendo las respectivas pruebas de funcionamiento y la entrega del informe de instalación con el protocolo y resultados de pruebas realizadas. Lo anterior deberá ser recibido a satisfacción por parte del supervisor y del apoyo técnico.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

DETALLES TÉCNICOS DE LOS SERVICIOS A CONTRATAR POR PARTE DEL INSTITUTO DE DEPORTS Y RECREACIÓN:

La solución deberá disponer de mecanismos de gestión centralizada que faciliten la operación, monitoreo y administración de los componentes de seguridad desde una sola interfaz unificada o integrada. Asimismo, deberá contar con garantía y soporte del fabricante y cumplir con las siguientes capacidades técnicas:

Todas las características descritas a continuación son referencia al resultado esperado al implementar toda la solución mas no a una marca en específico, y sin restringir a una única forma de obtener el resultado final esperado, por lo cual se informa que sin importar el mecanismo que cada fabricante utiliza, la solución deberá permitir implementar todos los controles descritos.

1. PROTECCIÓN ENDPOINTS Y SERVIDORES	
La Entidad solicita una solución que provea la seguridad de las estaciones de trabajo y servidores mediante prevención, detección y respuesta ante amenazas en el EndPoint, que incluya protección contra malware, ransomware, amenazas sin archivo residentes en memoria, explotación de vulnerabilidades, robo de credenciales y uso malicioso de herramientas legítimas del sistema operativo, gestionada desde una sola interfaz.	
Cantidad	1020
Vigencia	12 Meses
Medida	Unidad
#	Requerimiento Técnico Mínimo (de obligatorio cumplimiento)
	GENERALIDADES
1.1	La Entidad requiere del licenciamiento de la solución EDR para 1020 dispositivos. **SERVIDORES ON-PREMISES (20)** Protección de servidores de centro de datos con diferentes sistemas operativos en cualquier versión: • Windows server 2008 • Windows server 2012 • Windows server 2016 • Windows server 2022 • Windows server 2025 • Linux Ubuntu 22.04 • CentOS 8 **ENDPOINTS (900)** • Debe tener compatibilidad Multiplataforma principalmente Windows, macOS en cualquier versión. **RESERVA ENDPOINTS (100)** • Debe tener compatibilidad Multiplataforma principalmente Windows, macOS en cualquier versión.
1.2	La solución de EDR debe proporcionar a la Entidad un conjunto de protecciones tanto en pre-ejecución —antes de que la amenaza tenga capacidad de comprometer el sistema— como en post-ejecución —cuando la amenaza ya interactúa con el servidor o la estación de trabajo—, con capacidad de respuesta en tiempo real. La capa de pre-ejecución debe incorporar un motor de prevención basado en aprendizaje automático, capaz de emitir un veredicto sobre archivos no vistos previamente sin depender exclusivamente de firmas, operando de forma local en el agente para mantener la protección en equipos desconectados de la red. La capa de post-ejecución debe operar mediante análisis de comportamiento en tiempo de ejecución, con capacidad de bloquear comunicaciones salientes a nivel de proceso, impedir el acceso malicioso al sistema de archivos y al registro, y detener el cifrado por ransomware, incluso en equipos sin conectividad con la consola de gestión.
2	**FUNCIONALIDADES DE PREVENCIÓN**
2.1	El EDR debe utilizar un motor antivirus de aprendizaje automático para detener la ejecución previa de malware. Esta capacidad NGAV viene integrada en un agente único y ligero, lo que permite a los usuarios asignar protección antimalware a cualquier grupo de terminales sin necesidad de ninguna solución adicional.
2.2	Disponer de aprendizaje automático, NGAV basado en kernel y Machine learning (ML)
2.3	Enriquecer los eventos de seguridad con información de inteligencia de amenazas proveniente de una base de datos en la nube actualizada de forma continua, incluyendo reputación de archivos, dominios y direcciones IP.
2.4	Mantener la capacidad de prevención y detección en equipos sin conectividad con la consola de gestión o con los servicios en la nube del fabricante, conservando la telemetría localmente y sincronizándola al restablecerse la conexión.
2.5	Proporcionar un control de dispositivos de almacenamiento extraíble (**Almacenamiento USB, Pendrive, Periféricos externos**), sobre estaciones de trabajo Windows, con políticas asignables de forma diferenciada por grupo de equipos. La solución debe permitir el bloqueo del uso de dispositivos por categoría (**Almacenamiento USB, Dispositivos móviles, Unidades ópticas, impresoras escáner, Dispositivos de interfaz HID, dongles, y los que pertenezcan en esta categorías**), y disponer de un mecanismo de autorización granular que habilite dispositivos específicos mediante su fabricante, descripción o número de serie, o una combinación de estos criterios. Todo intento de uso de dispositivo extraíble debe generar un evento registrado y consultable en la consola de gestión.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

2.6	La solución debe reducir el ruido operativo mediante: clasificación automática del veredicto de cada evento, con historial y reclasificación posterior; agrupación de eventos relacionados en un incidente único; y excepciones granulares —acotables por proceso, ruta y grupo de equipos— que supriman detecciones equivalentes sin recurrir a exclusiones amplias.
2.7	La solución deberá evaluar vulnerabilidades en sistemas operativos y aplicaciones de EndPoints Windows, Windows Server y Linux, identificando CVE/CVSS, activos afectados y nivel de riesgo, y proporcionando mecanismos de mitigación como virtual patching mientras se realiza el parcheo definitivo.
3	**FUNCIONALIDADES DE DESCUBRIMIENTO**
3.1	El EDR debe contar con un sistema automatizado de control de políticas de superficie de ataques, con evaluaciones y descubrimiento de vulnerabilidades que permiten al personal encargado de la seguridad dar gestión.
3.2	Descubrir y controlar dispositivos no autorizados (por ejemplo, dispositivos no protegidos o no administrados) y detectar dispositivos IoT.
3.3	Realizar un seguimiento de aplicaciones ejecutadas, y su clasificación de seguridad.
3.4	Descubrir y mitigar las vulnerabilidades del sistema y las aplicaciones con parches virtuales, mediante el análisis de sus comunicaciones e inhabilitando el acceso a su comunicación con el exterior.
3.5	Al descubrir las vulnerabilidades debe mostrar la clasificación de reputación y el detalle de los códigos CVE aplicables
3.6	Reducir la superficie de ataque con políticas proactivas basadas en niveles de riesgo.
4	**FUNCIONALIDADES DE DETECCIÓN Y PROTECCIÓN**
4.1	El EDR debe detectar y desactivar el malware así sean amenazas del tipo sin archivos o file-less y otros ataques avanzados en tiempo real para proteger los datos y evitar brechas en la seguridad en la entidad. Tan pronto como el EDR detecte flujos y comportamientos sospechosos, inmediatamente debe desactivar las amenazas potenciales, bloquear las comunicaciones salientes y el acceso al sistema de archivos desde esos procesos sospechosos, por otro lado debe evitar la exfiltración de datos, las comunicaciones de comando y control (C&C), la manipulación de archivos y el cifrado de ransomware. Al mismo tiempo, el backend del EDR debe continuar recopilando evidencias adicionales, enriqueciendo los datos de eventos y clasificando los incidentes para aplicar de forma automatizada una estrategia de respuesta a incidentes, permitiendo así automáticamente la continuidad del negocio incluso en dispositivos ya comprometidos cumpliendo como mínimo con los siguientes ítems:
4.2	Detección basada en el análisis del comportamiento en tiempo de ejecución con visibilidad a nivel de kernel sobre los procesos y actividades del EndPoint, capaz de identificar técnicas de infiltración sigilosa, ataques residentes en memoria, ataques basados en scripts y uso malicioso de herramientas y binarios legítimos del sistema operativo (living off the land).
4.3	Debe Proporcionar protección en los procesos en ejecución, el inicio y parada de procesos, y en las interacciones entre procesos, así como frente a actividades sospechosas asociadas a librerías (archivos DLL en el caso de sistemas operativos Windows).
4.4	Debe poder Detener las amenazas en tiempo real y eliminar el tiempo de permanencia de dichas amenazas en la organización, incluso en los endpoints desconectados de la red corporativa.
4.5	Debe Bloquear las comunicaciones de forma granular a nivel de proceso, evitando exfiltraciones de datos, movimientos laterales y conexión con redes de comando y control.
4.6	Debe Impedir a los procesos maliciosos el acceso a los sistemas de ficheros, protegiendo frente a cifrados de ransomware, y la creación/modificación/eliminación maliciosa de archivos y/o registros.
4.7	Debe permitir definir listas de permitidos y denegados mediante criterios de identificación de archivos y aplicaciones que incluyan, como mínimo: hash del archivo, nombre y ruta de ubicación, y firma digital del editor, admitiendo para este último criterio la identificación por certificado, por huella digital del certificado o por nombre del firmante.
4.8	Debe Proporcionar la capacidad para marcar, tanto manual como automáticamente, determinada actividad como falso positivo, evitando además que ocurran detecciones similares.
4.9	La solución deberá conservar los eventos de seguridad y la telemetría de actividad del endpoint durante un período mínimo de noventa (90) días, disponibles para análisis retrospectivo mediante consultas estructuradas sobre la totalidad del período retenido.
4.10	La solución debe revalidar el veredicto de los eventos de seguridad mediante un análisis posterior en el servicio en la nube del fabricante, que incorpore inteligencia de amenazas. Cada reclasificación debe registrarse en un historial auditable, y las acciones de respuesta automatizada deben basarse en el veredicto final.
5	**FUNCIONALIDADES DE PROTECCIÓN CONTRA RANSOMWARE**
5.1	La solución de EDR debe contar con políticas predefinidas y exclusivas para la prevención de secuestro de información por ataques de ransomware, por lo cual debe incluir más de 30 estrategias de protección diferentes. Dichas estrategias deben incluir como mínimo:
5.2	1. Debug de Procesos.
5.3	2. Código dinámico.
5.4	3. Formato de archivo ejecutable incorrecto
5.5	4. Una pila con código ejecutable
5.6	5. El programa ejecutado no tiene instalador
5.7	6. Programa crítico falso.
5.8	7. Empaquetador falso.
5.9	8. File Encryptor.
5.10	9. Proceso oculto.
5.11	10. Ejecutable inyectado.
5.12	11. Proceso inyectado.
5.13	12. Hilo inyectado.
5.14	13. Suma de comprobación no válida.
5.15	14. Ejecución no válida.
5.16	15. Puntero no válido.
5.17	16. Inyección de kernel.
5.18	17. Empaquetador conocido.
5.19	18. Archivo malicioso detectado.
5.20	19. Proceso malicioso.
5.21	20. Ejecutable modificado.
5.22	21. Stack Parcialmente asignado.
5.23	22. Exploit de escalamiento de privilegios.
5.24	23. Proceso vacío.
5.25	24. Manipulación de pilas.
5.26	25. Aplicación sospechosa.
5.27	26. Empaquetador sospechoso.
5.28	27. Ejecutable manipulado.
5.29	28. Ejecutable no confirmado.
5.30	29. Ejecutable sin asignar.
5.31	30. Código grabable.
6	**FUNCIONALIDADES DE REMEDIACIÓN**

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

6.1	La Solución de EDR propuesta debe orquestar operaciones de respuesta a incidentes utilizando playbooks predefinidos en la solución, optimizando sí la respuesta a incidentes y los procesos de remediación, revirtiendo de modo automático los cambios maliciosos realizados por amenazas ya contenidas, en un único dispositivo o en dispositivos distribuidos a lo largo del entorno de la entidad, las características de remediación deben cumplir como mínimo con los siguientes requerimientos:
6.2	Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta.
6.3	La solución debe permitir definir playbooks de respuesta configurables por clasificación de evento y por grupo de dispositivos, con acciones ejecutables de forma automática o previa aprobación del analista.
6.4	Debe optimizar los recursos de seguridad, automatizando las acciones de respuesta a incidentes, como la eliminación de archivos, la finalización de procesos maliciosos, la reversión de cambios persistentes, la notificación a los usuarios, el aislamiento de aplicaciones y dispositivos, y la integración con una plataforma de ITMS para apertura de tickets.
6.5	Debe permitir la respuesta a incidentes basada en el contexto utilizando la clasificación de incidentes y los sujetos de los ataques (como por ejemplo, grupos de estaciones de trabajo).
6.6	Visibilidad completa de la cadena de ataque y de los cambios realizados en el sistema, con representación gráfica de la secuencia de procesos involucrados desde el origen.
6.7	Reversión automatizada de cambios de persistencia introducidos por la amenaza, incluyendo entradas de registro, tareas programadas y servicios creados o modificados.
6.8	Debe realizar la contención y respuesta de forma automática
6.9	Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta.
7	**FUNCIONALIDADES DE INVESTIGACIÓN**
7.1	La solución de EDR debe enriquecer automáticamente los registros de los eventos con información detallada sobre el malware antes y después de la infección, para realizar análisis forenses en los endpoints infiltrados. Su interfaz guiada debe proporcionar una guía útil, mejores prácticas y sugerir los próximos pasos lógicos a los analistas de seguridad, estas características de investigación deben cumplir como mínimo con los siguientes requerimientos:
7.2	Debe tener la capacidad de contención automática de la amenaza debe permitir que el análisis forense posterior se realice sin presión de tiempo, manteniendo el equipo operativo.
7.3	Debe contar con la capacidad de visualización de la cadena de ataque completa con identificación del origen de la infección (paciente cero), disponible incluso cuando el dispositivo se encuentre fuera de línea.
7.4	Debe conservar instantáneas de memoria, de los ataques sin archivo o file-less para la búsqueda de amenazas basada en memoria.
7.5	La interfaz grafica debe mostrar explicaciones claras por qué el evento está marcado como sospechoso o malicioso, enumera el marco de ataque MITRE correspondiente, así como el siguiente paso lógico para la investigación forense.
8	**FUNCIONALIDADES DE EDR**
8.1	La solución de EDR debe disponer de capacidades de integración con otras plataformas de seguridad del ecosistema de la Entidad, ya sea mediante conectores nativos preconfigurados por el fabricante o mediante interfaces de programación de aplicaciones (API) documentadas públicamente. La integración deberá permitir, como mínimo, el intercambio bidireccional de información de eventos e indicadores de compromiso, y la ejecución de acciones de respuesta coordinada. El proponente deberá acreditar, mediante documentación técnica oficial del fabricante, la disponibilidad de la integración para cada una de las siguientes categorías de solución:
8.2	1. Next Generation Firewall de la Entidad
8.3	2. Control de Acceso a la Red.
8.4	3. Análisis dinámico de archivos en entorno aislado SandBoxing.
8.5	4. Plataformas de engaño (deception) o honeypots
8.6	5. Correlacionador de Eventos, SIEM.
8.7	6. Plataforma de Orquestación, automatización y respuesta a incidentes, SOAR.
8.8	7. Plataforma de Análisis de comportamiento de usuario UEBA
8.9	8. Plataforma de Manejo de Identidades, IAM
8.10	Debe contar con la funcionalidad de INVESTIGACIÓN IMPULSADA POR INTELIGENCIA ARTIFICIAL
8.11	Debe contar con la funcionalidad de RESPUESTA AUTOMATIZADA
9	**COMPONENTES DE LA SOLUCIÓN DE EDR**
9.1	La plataforma de seguridad del endpoint EDR debe ser una arquitectura distribuida, la cual debe constar de una agente en software el cual debe ser compatible con los siguientes sistemas operativos y entornos, en versiones de 32 y 64 bits:
9.2	Windows: XP SP2/SP3, 7, 8, 8.1 y 10.
9.3	Windows Server: 2003 R2 SP2, 2008 R2 SP2, 2012, 2012 R2, 2016 y 2019.
9.4	MacOS: Yosemite (10.10), El Captain (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15).
9.5	Linux: Redhat Enterprise Linux and CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 and 7.7, y Ubuntu LTS 16.04.5, 16.04.6, 18.04.2 server, en 64-bit.
9.6	Entornos VDI: VMware Horizons 6 y 7, y Citrix Desktop 7.
9.7	En cuanto al hardware, se debe ser un agente muy ligero; el cual no debe requerir más de 100MB de memoria RAM, y 20MB de espacio en disco.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

9.8	Adicional la solución debe permitir ser desplegada de cualquiera de las siguientes maneras:
9.9	Nube: En la Nube del Fabricante.
9.10	On-Premise: En el Datacenter de la entidad.
9.11	Hibrida: En Nube y On-premise.
9.12	AirGapped o Sistemas Cerrados.
9.13	El producto debe incluir servicios de mejores prácticas implementadas por personal de servicios de Fabrica o un partner de servicios autorizado por Fabrica
10	**Servicios Profesionales**
10.1	La solución debe ofrecer transferencia de conocimiento en la fase de implementación sin cargo adicional.
10.2	El servicio de atención al cliente deberá estar disponible las 24 horas del día, los 7 días de la semana por correo electrónico, chat y teléfono.
10.3	El soporte del servicio debe entregarse por 12 meses

2. PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS		
La Entidad solicita una solución que provea la seguridad del sitio de trabajo a través de protección del correo electrónico, plataformas de colaboración, que incluya protección contra phishing, ransomware, ataques de día cero y apropiaciones de cuentas en una sola consola.		
Cantidad		2300
Vigencia		12 Meses
Medida		Unidad
#	**Categoria**	**Requerimiento Técnico Mínimo (de obligatorio cumplimiento)**
1		**Protección de correo electrónico.**
1.1	**Escaneo de correo electrónico**	La solución debe analizar dinámicamente el 100% de los correos electrónicos
1.2		La solución debe analizar todas las URL y archivos adjuntos de los correos electrónicos entrantes
1.3		La solución debe escanear dinámicamente los correos electrónicos a una velocidad media de 15 segundos
1.4		El administrador de la solución debe estar en capacidad de acceder automáticamente a los detalles del análisis para ver las razones exactas por las que se marca un correo electrónico como malicioso
1.5		La solución debe proteger activamente contra el spam
1.6		La solución debe identificar amenazas después de la entrega de correo. Debe estar en capacidad de notificar a los usuarios y recuperar correos electrónicos maliciosos de sus bandejas de entrada para ponerlos en cuarentena automáticamente
1.7		La solución debe utilizar fuentes de inteligencia sobre amenazas para identificar amenazas conocidas
1.8	**Identificación de amenazas**	La solución debe utilizar capacidades internas de búsqueda de amenazas asistidas por humanos
1.9		La solución debe escanear los correos electrónicos de forma estática utilizando motores Antivirus
1.10		La solución debe utilizar herramientas para identificar firmas muy complejas
1.11		La solución debe proteger contra los ataques de phishing a través del reconocimiento de imágenes, el análisis de texto y los evaluadores de reputación
1.12		La solución debe proteger contra los ataques BEC cuando se realizan comprobaciones SPF, DKIM y DMARC
1.13	**Amenazas avanzadas**	La solución debe proteger contra los ataques de suplantación de identidad mediante el uso de técnicas para descubrir la suplantación de nombres de visualización y la suplantación de VIP
1.14		La solución debe proteger contra ataques de día cero y día N al inspeccionar datos a nivel de CPU
1.15		La solución debe detectar ATO mediante la observación de anomalías en el comportamiento del usuario
1.16	**Manejo de URL**	La solución debe hacer clic y escanear activamente las direcciones URL para identificar enlaces maliciosos antes de que lleguen al buzón del usuario final
1.17	**Sandbox**	La solución contar con la tecnología Sandbox para identificar archivos maliciosos
1.18		La solución debe utilizar datos de nivel de CPU para inspeccionar el flujo de ejecución de archivos
1.19		La solución debe mantener la integridad de los archivos durante los análisis, evitando alterar la estructura de los archivos
1.20		La solución debe identificar vulnerabilidades de daño en la memoria
1.21		La solución debe detectar errores lógicos y macros dentro de los documentos
1.22		La solución debe escanear cientos de tipos de archivos diferentes

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

1.23	Gestión de archivos	La solución debe descomprimir el contenido de forma recursiva, buscando enlaces y archivos incrustados para escanear
1.24		La tecnología de la solución para escanear enlaces y archivos incrustados debe tener al menos 7 capas de profundidad
1.25		La solución debe analizar contenido protegido con contraseña al entregarse el password
1.26		La solución debe analizar archivos comprimidos/comprimidos
1.27	Situación del mercado	La solución debe estar en la Guía de mercado de Gartner para la seguridad del correo electrónico
1.28		La solución debe estar catalogada en los tres primeros lugares en la evaluación de SE Labs.
2	**Protección de herramientas de colaboración**	
2.1	Protección de Herramientas de colaboración	La solución debe ser compatible con Slack, Microsoft 365 (Teams, One Drive, SharePoint), Google Drive, Box, Salesforce, Dropbox, Zendesk, AWS S3 Buckets y otras aplicaciones usando APIs.
2.2		La solución debe detectar y bloquear archivos maliciosos, URLs, y ataques avanzados en las soluciones protegidas
2.3		La solución debe tener la capacidad de integrarse a un servicio de Incident&Response (IR) para evaluar casos particulares o solicitados por el usuario final.
2.4		Debe escanear el 100% de los datos
2.5		La solución debe evaluar los correos y URLs que se envíen por las plataformas evaluadas
2.6		El servicio debe tener un Objetivo de nivel de servicio de mínimo 99.98%
2.7		Debe proveer servicios de Análisis de amenazas, Análisis dinámico y estático de archivos, protección de toma de cuenta (mínimo MS365)
3	**Uso**	
3.1	Duración	La solución debe ser nativa de la nube y está totalmente alojada en la nube
3.2		La solución debe actualizarse automáticamente
3.3		La solución debe satisfacer las necesidades de escalamiento de licenciamiento de un cliente sin afectar la experiencia del usuario ni requerir la compra de equipos adicionales
3.4	Instalación	La solución debe permitir la implementación en modo de prevención de amenazas, evitando las amenazas antes de que lleguen a los usuarios finales
3.5		La solución debe permitir ser implementada en modo CCO/Journaling, así como en línea para una protección completa en M365 como mínimo
3.6		La solución debe permitir la implementación para los usuarios a través de una invitación por correo electrónico
3.7		La solución debe ser implementada automáticamente con la integración de Office 365
3.8	Integración	La solución debe tener la posibilidad de conectarse a través de API a otras aplicaciones
3.9		La solución debe integrarse con Office 365 a través de API sin necesidad de cambiar el registro MX
3.10		La solución debe poderse ajustar a las políticas e integrarse a un SIEM, y no requiere cambios en la infraestructura e integración vía REST APIs
3.11		La solución debe estar en capacidad de exportar registros en tiempo real a un SIEM
3.12		La solución debe estar en capacidad de integrarse con gestores de Identidades a través de SAML
3.13	Gestión de datos	Los usuarios se deben asignan automáticamente permisos a roles y grupos en función de un esquema RBAC
3.14		La solución debe estar en capacidad mediante licencias adicionales de proteger el uso del cliente del almacenamiento compartido, las herramientas de colaboración y el navegador
3.15		La solución debe cifrar los datos en reposo con AES-256 y en tránsito con TLS 1.2+
3.16		Las claves de cifrado deben estar protegidas con soluciones como AWS KMS
3.17		La solución debe cumplir con: SOC2, GDPR, HIPAA, ISO 27001
3.18		La solución debe estar alojada en servidores separados ubicados en Europa, EE. UU. y APAC para garantizar resiliencia del servicio
3.19	Gestión	La solución debe proporcionar un panel de administración informativo que muestre datos de incidentes, informes y políticas
3.20		la solución debe tener la opción de incluir en las listas negras o blancas en función de la IP, las URL, los dominios, los remitentes, los tipos de archivos, etc.
3.21		La solución debe registrar las acciones del usuario, como los intentos de inicio de sesión, los cambios en el veredicto, la publicación de correos electrónicos y las solicitudes de investigación
3.22		El cliente debe estar en capacidad de personalizar los banners y las alertas de advertencia y traducirlos a otros idiomas como español, inglés y portugués

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

3.23		La solución debe tener una forma que el usuario reporte un presunto falso positivo o falso negativo para que la solución la revise y de su veredicto
3.24		La solución debe enviar informes y resúmenes de acciones a los usuarios
4		**Servicio**
4.1	**Soporte al cliente**	La solución debe ofrecer transferencia de conocimiento en la fase de implementación sin cargo adicional.
4.2		El servicio de atención al cliente deberá estar disponible las 24 horas del día, los 7 días de la semana por correo electrónico, chat y teléfono.
4.4	**Duración**	El soporte del servicio debe entregarse por 12 meses.

3. WAF (WEB APPLICATION FIREWALL)		
La entidad requiere una solución unificada para proteger aplicaciones web (**10 sitios máximo**) y debe permitir APIs, optimizar el rendimiento y simplificar la gestión en entornos híbridos y multi-nube, que cumpla con los siguientes requerimientos		
Cantidad		1
Vigencia		12 Meses
Medida		Unidad
#	Categoría	Requerimiento Técnico Mínimo (de obligatorio cumplimiento)
1		CARACTERÍSTICA/FUNCIONALIDAD
1.1	**Seguridad de Aplicaciones Web y API (WAF y API Security):**	Protección contra ataques de día cero mediante aprendizaje automático dual.
1.2		Eliminación de falsos positivos analizando y filtrando tráfico antes de llegar a las aplicaciones.
1.3		Protección contra los riesgos principales de OWASP Top 10.
1.4		Actualizaciones automáticas con inteligencia de amenazas en tiempo real.
1.5		Configuración simplificada a través de una interfaz intuitiva.
1.6		Protección basada en firmas.
1.7		Inteligencia de amenazas IP.
1.8		Inteligencia GEO-IP.
1.9		Reglas de seguridad personalizadas.
1.10		Cumplimiento de HTTP.
1.11		Protección de URL, parámetros y CORS.
1.12		Protección de cookies.
1.13		Prevención de fugas de información.
1.14		Antivirus para cargas de archivos.
1.15		Sandbox para cargas de archivos.
1.16		Protección contra ataques de día cero basada en aprendizaje automático.
1.17		Cumplimiento de esquemas (Open API, XML, JSON).
1.18		API Gateway.
1.19		Protección de API móviles.
1.20		Descubrimiento, catálogo de PII y protección basada en aprendizaje automático.
1.21		Protección de encabezados HTTP.
1.22		Protección contra CSRF y ataques Man-in-the-Browser (MiTB).
1.23	**Protección Avanzada contra Bots:**	Detección basada en comportamiento mediante análisis biométrico y de comportamiento.
1.24		Perfilado avanzado de dispositivos para bloquear ataques de bots.
1.25		Identificación y bloqueo de rastreadores web no deseados y amenazas automatizadas.
1.26		Análisis en tiempo real e histórico del tráfico y actividades de bots.
1.27		Protección avanzada contra bots (detección biométrica, firma y engaño).
1.28	**Balanceo de Carga Global de Servidores (GSLB):**	Balanceo de carga basado en DNS para distribuir tráfico entre múltiples centros de datos.
1.29		Distribución geográfica del tráfico según métricas de salud y ubicación.
1.30		Integración sencilla con la plataforma de Protección Web.
1.31		Alta disponibilidad incluso durante interrupciones regionales.
1.32		Capacidad para realizar chequeos de salud (health checks) sobre servicios y aplicaciones, permitiendo identificar el estado operativo de sus componentes, detectar de manera anticipada posibles fallas o indisponibilidades y generar acciones de respuesta proactiva.
1.33	**Análisis de Amenazas:**	Identificación de patrones de ataque ocultos mediante correlación de eventos basada en IA.
1.34		Visibilidad en tiempo real de eventos de seguridad en toda la infraestructura.
1.35		Respuesta proactiva a incidentes con inteligencia de amenazas y flujos de trabajo automatizados.
1.36		Reducción de la fatiga de alertas consolidando múltiples alertas en incidentes significativos.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

1.37	Automatización	Automatización de tareas de seguridad como actualizaciones de políticas y correcciones de configuración.
1.38		Priorización de amenazas de alto riesgo y caza adaptativa de amenazas.
1.39		Enriquecimiento de inteligencia de amenazas para mejorar la defensa proactiva.
1.40	Protección contra Toma de Cuentas:	Seguimiento de usuarios.
1.41		Protección contra fijación de sesiones.
1.42		Defensa contra relleno de credenciales.
1.43	Protección contra DDoS:	Mitigación de DDoS en capas 3-4.
1.44		Mitigación de DDoS en capa 7.
1.45	Entrega de Aplicaciones:	Certificados SSL automáticos y personalizados.
1.46		Autenticación de clientes/Mutual TLS.
1.47		Red de entrega de contenido (CDN).
1.48		CDN GEO limitado.
1.49		Balanceo de carga y monitoreo de salud de servidores.
1.50		Enrutamiento de contenido del servidor de origen.
1.51		Sala de espera.
1.52	Escaneo DAST:	Evaluación de vulnerabilidades.
1.53		Escaneo de API.
1.54	Reportes y Análisis:	Registros de ataques.
1.55		Notificaciones de alertas.
1.56		Integración con SIEM.
1.57		Enmascaramiento de datos sensibles en registros.
1.58		Análisis de registros en tiempo real e históricos.
1.59		Dashboards e informes.
1.60		Registros de tráfico.
1.61		Análisis de amenazas con IA.
1.62	Gestión:	Control de acceso basado en roles.
1.63		Soporte para inicio de sesión único (SSO).
1.64		Soporte API.
1.65	Servicios:	La solución debe ofrecer transferencia de conocimiento en la fase de implementación sin cargo adicional.
1.66		El servicio de atención al cliente deberá estar disponible las 24 horas del día, los 7 días de la semana por correo electrónico, chat y teléfono.
1.67		El servicio soporte debe entregarse por 12 meses

4. IMPLEMENTACIÓN Y SOPORTE TÉCNICO	
4.1	• Soporte Técnico durante 12 meses de la plataforma seguridad deberá contar como mínimo con las siguientes características: o Actualizaciones y mantenimiento de producto o Compatibilidad con nuevos sistemas operativos, acceso a versiones nuevas sin costo adicional dentro de la vigencia. o Soporte técnico: Deberá incluir, atención remota telefónica 24/7, asistencia para configuración y despliegue, guías técnicas, manuales y base de conocimientos, SLA (acuerdo de nivel de servicio). Medios de escalamiento mínimo helpdesk con usuario y contraseña o Transferencia de Conocimiento: Actividad de transferencia de conocimiento inicial sobre uso del producto 20 horas; laboratorios de aprendizaje de uso de la solución para administradores o equipos técnicos, documentación de mejores prácticas. o Interfaz de administración: Recuperación, restablecimiento o migración sin costo adicional, en caso de que aplique.
4.2	• Realizar todas las actividades necesarias para la configuración, instalación, puesta en funcionamiento y verificación del sistema de ciberseguridad, incluyendo las respectivas pruebas de funcionamiento y la entrega del informe de instalación con el protocolo y resultados de pruebas realizadas. Lo anterior deberá ser recibido a satisfacción por parte del supervisor y del apoyo técnico.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

- Todas las actividades, comunicaciones y documentos relacionados con el proceso de contratación y la ejecución del contrato deberán realizarse y presentarse en idioma castellano.
- Todos los componentes deber ser del mismo fabricante.
- La vigencia de la solución de seguridad debe iniciar a partir del 1 de noviembre de 2026 por 12 meses.
- Las licencias de la plataforma de seguridad deben ser en la última versión publicada por el fabricante y deben quedar a nombre del INDER Medellín.
- La plataforma de seguridad debe contar con acceso a actualizaciones periódicas para la protección contra nuevas amenazas.
- La garantía comercial del fabricante:

  El licenciamiento de los productos tendrá una vigencia de doce (12) meses, durante los cuales deberá mantenerse vigente el soporte del fabricante. El fabricante deberá garantizar la disponibilidad de soporte técnico 24x7, permitiendo la apertura y atención de casos de soporte durante todo el periodo de vigencia del licenciamiento.

ACTIVIDADES A EJECUTAR POR EL CONTRATISTA:

Estas actividades son transversales durante la vigencia del contrato y de las licencias.

Prestación de servicios profesionales especializados para la implementación, configuración, puesta en operación, transferencia de conocimiento y soporte técnico de las soluciones de ciberseguridad adquiridas, durante la vigencia del contratoy de las licencias, de la siguiente forma:

1. Una vez suscrita el Acta de Inicio por las partes, el Contratista deberá realizar un análisis del nivel de seguridad actual del INDER Medellín y presentar los resultados de dicho examen al Instituto, el cual deberá ser entregado mediante un informe por escrito a más tardar 15 días calendario contados a partir de la suscripción del Acta de Inicio.
2. Con anterioridad al 15 de noviembre de 2026, el Contratista deberá proceder con la Instalación, configuración y puesta en marcha de las soluciones definidas (EDR, PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS Y WAF) en el presente alcance:
   a. Despliegue del 40% de los 1020 agentes en los EndPoint.
   b. Despliegue de agentes en 5 de los 20 para servidores.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

c. Despliegue de la solución WAF con la configuración de las políticas de protección para 10 sitios Web.

d. Despliegue y configuración de la protección para 2300 buzones de correo y herramientas colaborativas.

e. Configuración de la interfaz de administración e integración de los servicios.

3. Con anterioridad al 15 de noviembre de 2026, deberá alinear la solución de seguridad según las políticas de ciberseguridad del INDER Medellín.
4. Transferencia de conocimiento a 3 integrantes del personal técnico del INDER Medellín sobre la administración del SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR, PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF.
5. Envió de Campañas de entrenamiento para usuarios finales en la identificación de situaciones de riesgo, "Boletines de sensibilización de Ciberseguridad" a través de correo electrónico, a los usuarios del instituto (gestionado y coordinado entre el oferente y la coordinación de TI.).
6. Capacitación virtual (dos al año), sobre concienciación en ciberseguridad para usuarios finales durante la vigencia del contrato y de las licencias, entregar evidencia documentada que incluya el contenido o protocolo de la actividad una vez sea realizada.
7. Durante la vigencia de las licencias y a solicitud del apoyo técnico del instituto, realizar una evaluación de ciberseguridad basado en algún framework cómo: NIST, ISO 27001 o CIS Controls. Entregar evidencia documentada que incluya alcance, criterios de severidad, protocolo y demás contenido de la actividad una vez sea realizada.

OBLIGACIONES ESPECÍFICAS

1. Dentro de los primeros 5 días hábiles posteriores a la fecha de inicio del contrato, el contratista deberá asistir a una reunión presencial o virtual para socializar requisitos exigidos por INDER Medellín, obligaciones establecidas por INDER Medellín y dudas del contratista.
2. Cumplir con los requisitos técnicos y actividades descritas en el anexo técnico y ESPECIFICACIONES TÉCNICAS del Estudio Previo. Entregable: Informe técnico de entrega final, el cual debe contener cada ítem indicar actividad realizada o licencia entregada.
3. Mediante carta firmada por el Representante Legal, Informar detalladamente el alcance de la garantía del fabricante y soporte técnico adquirido para los servicios contratados, la cual debe coincidir con las características mencionadas en las especificaciones técnicas.
   Entregable: Carta firmada por el representante legal.
4. El contrista deberá brindar el soporte técnico, de conformidad con las condiciones y alcance establecidos en la carta de garantía, cuando sea requerido por la supervisión durante la vigencia de la plataforma adquirida.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

5. El contratista deberá presentar un informe cuantitativo del desempeño de toda la solución de seguridad con periodicidad mensual durante la vigencia de la plataforma adquirida.
   Entregable: Carta firmada por el representante legal con este compromiso.
6. El contratista deberá entregar de forma digital, la evidencia de las licencias(s) de la plataforma a nombre del INDER Medellín.
7. Deberá contar con un sistema de escalamiento de solicitudes, medios de contacto y SLA. Entregable: Incluir esta información en el informe técnico de entrega final.
8. El contratista deberá desarrollar cronogramas, planes de trabajo e implementación, procedimientos y contenidos que sean necesarios para la correcta ejecución de todas las actividades que conlleve el proyecto.
9. Durante la vigencia de las licencias, realizar dos (2) pruebas de penetración, en las fechas que sean determinadas y solicitadas por el apoyo técnico designado por la Entidad, quien comunicará oportunamente al contratista los momentos en los cuales deberán ejecutarse dichas pruebas, una vez realizada cada prueba deberá entregar el informe al instituto con todo el protocolo realizado.

PLAZO: Hasta el 31 de diciembre de 2026

PARÁGRAFO: Aclaración, explicación sobre el plazo del contrato y vigencias de licencias.

Se aclara que, a más tardar el 15 de noviembre de 2026, el contratista deberá haber culminado las actividades de diagnóstico, instalación, configuración y parametrización, de manera que la solución se encuentre completamente implementada y en operación.

El plazo comprendido entre el 15 de noviembre y el 31 de diciembre de 2026 estará destinado a la ejecución de actividades posteriores a la implementación, tales como la elaboración de informes, actividades derivadas de la puesta en funcionamiento de la solución y verificaciones necesarias para la autorización de pago.

A partir del 31 de diciembre de 2026 y hasta el la finalización de la vigencia de las licencias, el contratista deberá continuar prestando de forma ininterrumpida, todos los servicios contratados y previstos en las especificaciones técnicas como garantía, soporte, mantenimiento, disponibilidad, actividades con alcance dentro de la vigencia de las licencias y las demás obligaciones detalladas en las especificaciones técnicas, obligaciones específicas y garantizando el correcto funcionamiento de la solución durante todo el período de prestación del servicio, 1 año.

LUGAR DE EJECUCIÓN: Será la ciudad de Medellín, en las instalaciones del INDER Medellín.

OBLIGACIONES ALMBIENTALES:

Atendiendo al objeto y los requerimientos técnicos establecidos, no aplican obligaciones ambientales.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

1.5. Perspectiva legal: Atendiendo la naturaleza del objeto a contratar el procedimiento de selección a seguir es el de SELECCIÓN ABREVIADA DE MENOR CUANTIA.

7.1. FUNDAMENTOS JURIDICOS: Con fundamento en el literal B del numeral 2 del artículo 2° de la Ley 1150 de 2007 en armonía con el artículo 2.2.1.2.1.2.20 del Decreto 1082 de 2015, se establecen las causales de contratación en materia de selección abreviada, entre las cuales se encuentra la de menor cuantía, causal a la cual se acude, entre otras, y para el proceso objeto de análisis, en eventos en los cuales los bienes o servicios que precisa la Entidad no revisten las características técnicas uniformes y de común utilización a la que alude el literal a) de la norma antes citada. Ello es así, en el entendido que el servicio que pretende contratar la Entidad a través del presente proceso de contratación no es ofrecido bajo un mismo estándar para quienes los demandan, o lo que es lo mismo, su oferta en el mercado no ocurre en condiciones equivalentes para todo interesado en adquirirlos. Así mismo, dadas las connotaciones técnicas específicas requeridas por la Entidad, no nos encontramos ante un servicio susceptible de homogeneidad, esto es, fácilmente descriptible por características mínimas comunes a los de su tipo.

Lo anterior permite entrever con claridad la imposibilidad de acudir a la modalidad de subasta inversa, consignada en el literal a) del numeral 2 del artículo 2 de la Ley 1150 de 2007, siendo entonces dable jurídicamente acudir a la vía de procedimiento de menor cuantía.

El procedimiento para la selección abreviada de menor cuantía se encuentra consignado en el artículo 2.2.1.2.1.2.20, el cual establece las siguientes reglas en la materia referenciada:

ARTÍCULO 2.2.1.2.1.2.20. Procedimiento para la selección abreviada de menor cuantía. *Además de las normas generales establecidas en el presente título, las siguientes reglas son aplicables a la selección abreviada de menor cuantía:*

1. En un término no mayor a tres (3) días hábiles contados a partir de la fecha de apertura del Proceso de Contratación los interesados deben manifestar su intención de participar, a través del mecanismo establecido para el efecto en los pliegos de condiciones.

2. Si la Entidad Estatal recibe más de diez (10) manifestaciones de interés puede continuar el proceso o hacer un sorteo para seleccionar máximo diez (10) interesados con quienes continuará el Proceso de Contratación. La Entidad Estatal debe establecer en los pliegos de condiciones si hay lugar a sorteo y la forma en la cual lo hará.

3. Si hay lugar a sorteo, el plazo para la presentación de las ofertas empezará a correr el día hábil siguiente a la fecha en la cual la Entidad Estatal informe a los interesados el resultado del sorteo.

4. La Entidad Estatal debe publicar el informe de evaluación de ofertas durante tres (3) días hábiles

Art. 2.2.1.2.1.2.20 del Decreto 1082 de 2015

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

2. Análisis de la demanda

2.1. Adquisiciones previas del Inder

Las adquisiciones anteriores de **SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (ENDPOINT DETECTION AND RESPONSE), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL)**

Modalidad	Vigencia	Presupuesto Oficial	Objeto	Contrato
LICITACIÓN PÚBLICA	2018	$148.393.000	Renovación de licenciamiento, soporte y garantía de antimalware – antispam y el dispositivo web aplication firewall (waf)	6700003748
SELECCIÓN ABREVIADA DE MENOR CUANTÍA	2019	$180.282.200	Renovación de licenciamiento, soporte y garantía de antimalware – antispam y el dispositivo web aplication firewall (waf)	6700008260
CONTRATACIÓN INTERADMINISTRATIVA DIRECTA	2021	$361.924.956	Adquirir, implementar y actualizar el licenciamiento de las herramientas antivirus trend micro, el radware appwall, vmware y veeam backup	6700018230
LICITACIÓN PÚBLICA	2022	$346.467.611	Renovación del licenciamiento: antivirus y antispam - trend micro, waf-radware, vmware y veeam backup	6700024475
SELECCIÓN ABREVIADA DE MÍNIMA CUANTÍA	2022	$678.300	Adquisición de certificado ssl de sitio seguro y certificado de firma digital almacenado en medio criptográfico o token	6700025875
SELECCIÓN ABREVIADA DE MÍNIMA CUANTÍA	2023	$318.342.400	Renovación del licenciamiento: antivirus y antispam –trend micro, waf-radware, veeam backup y adquisición de certificado digital ssl de sitio seguro y certificado de firma digital almacenado en medio criptografico o token	6700030103
ADMINISTRACIÓN DELEGADA	2024	$2.554.162.038	CONTRATO INTERADMINISTRATIVO DE MANDATO SIN REPRESENTACIÓN PARA ADQUIRIR LOS SERVICIOS DE INFRAESTRUCTURA TECNOLÓGICA EN MODALIDAD HÍBRIDA (NUBE PÚBLICA Y ON-PREMISE) QUE PERMITAN ALOJAR LOS SERVICIOS DIGITALES Y LA IMPLEMENTACIÓN, PUESTA EN MARCHA DE UNA SOLUCIÓN DE RED INALÁMBRICA PARA LA SEDE ADMINISTRATIVA, LICENCIAMIENTO ANTIVIRUS, ANTISPAM Y WAF CON EL OBJETIVO DE FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN.	6700038898
SUBASTA INVERSA	2025	$591.6610.100	ADQUIRIR COMO SERVICIO LAS SOLUCIONES DE ANTIVIRUS, ANTISPAM Y FIREWALL DE APLICACIONES WEB (WAF) PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN.	6700045132

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Se puede observar que, a lo largo de su existencia, que la Entidad ha contratado servicios similares o idénticos en diversas ocasiones, de acuerdo con su objeto y funciones. Es posible afirmar, que la modalidad de contratación depende de las necesidades puntuales de la Entidad y por lo tanto del monto del proceso

Entre 2018 y 2025, el INDER Medellín ha realizado una inversión creciente en infraestructura y seguridad tecnológica, pasando de contratos por aproximadamente **$148 millones** en 2018 a más de $591.6610.100 en 2025.

La mayor inversión se presentó en 2024 con un presupuesto de **$2.554 millones**, destinado a modernización tecnológica, infraestructura híbrida, antivirus, antispam y firewall WAF.

En general, se evidencia una continuidad en la contratación de servicios de ciberseguridad, licenciamiento y protección de infraestructura digital, reflejando un fortalecimiento progresivo de la capacidad tecnológica y de seguridad informática de la entidad.

2.2. Histórico de compras o adquisiciones de otras Entidades Estatales y otros consumidores del bien o servicios

Las adquisiciones o compras de otras Entidades Estatales **SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (ENDPOINT DETECTION AND RESPONSE), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL)**

Antivirus y Antispam

Proceso	Año	Modalidad	Entidad	Objeto	Valor
CMI-ISABU-001-2024	2024	MINIMA CUANTIA	E.S.E. INSTITUTO DE SALUD DE BUCARAMANGA	suministro de licencias antivirus para la ese isabu	77.060.484
MC-DAL-041-2023	2023	MINIMA CUANTIA	GOBERNACIÓN DE BOLÍVAR	Contratar la renovación de licencia de software antivirus bitdefender, con actualización, soporte, capacitación y asistencia técnica por el término de un año, para las estaciones de trabajo y servidor	95.000.000

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitaria al correo electrónico atencion.ciudadano@inder.gov.co.

IDU-SASI-DTAF-001-2022	2022	SELECCIÓN ABREVIADA	IDU- INSTITUTO DE DESARROLLO URBANO	Adquirir para el IDU el servicio de renovación y actualización del licenciamiento de antivirus	$362.311.444
CM-SAMC-089-2026	2026	SELECCIÓN ABREVIADA MENOR CUANTÍA	CLUB MILITAR	SERVICIO DE RENOVACIÓN DE LICENCIAS PARA ANTIVIRUS SOPHOS Y SOPORTE PARA EL SISTEMA DE SEGURIDAD PERIMETRAL PALO ALTO DEL CLUB MILITAR	$ 249.022.332

WAF

Proceso	Año	Modalidad	Entidad	Objeto	Valor
SSPD-SA-008-2023	2023	MINIMA CUANTIA	FONPRECON	Renovación del servicio de firewall de Aplicaciones en Web (WAF) y el content delivery de red (CDN) con el que cuenta la Superservicios (Manifestación de interés (Menor Cuantía)) (Presentación de oferta)	299.785.306,75
LP-075-CENACTELEMATICA-2023 (Presentación de oferta)	2023	Licitación Publica	CENTRAL ADMINISTRATIVA Y CONTABLE TELEMATICA	Adquisición, instalación y configuración de una herramienta de seguridad para la protección y balanceo a las aplicaciones web (waf) para el fortalecimiento de los medios cibernéticos del ejército nacional	1.573.615.520
SGA-SASI-10-2023	2023	MINIMA CUANTIA	IDU-INSTITUTO DE DESARROLLO URBANO	extensión de garantías firewall y waf (presentación de oferta)	542.636.750
DAFP-CD-124-2025	2025	Contratación directa	DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA	Adquisición, Instalación, configuración, puesta en operación y prestar servicios de soporte de una solución de Web Application Firewall (WAF) para la protección de los servicios y aplicaciones web del	$ 579.087.000

De los procesos consultados, se puede concluir que para las vigencias entre 2022 y 2026 se adelantaron por parte de varias entidades procesos con objetos similares, estos adjudicados mediante la modalidad aplicable de acuerdo con la cuantía y objeto específico.

Gasto a nivel nacional durante las vigencias 2021 al 2025

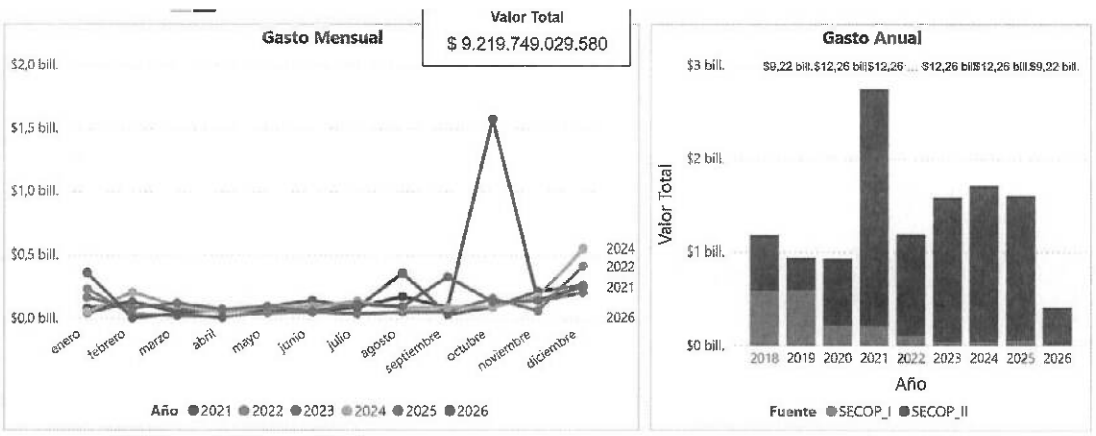
AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

A través de la herramienta MAE - Modelo de Abastecimiento Estratégico para el Análisis de la Demanda, se logró identificar la dinámica de contratación por parte de las diferentes entidades estatales en lo que refiere a la "**ADQUIRIR E IMPLEMENTAR UN SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (ENDPOINT DETECTION AND RESPONSE), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL) PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN.**", con el fin de identificar los aspectos más característicos y relevantes que componen el mercado objeto de contratación, por lo que se filtró la información considerando los siguientes parámetros:

Vigencias: 01/01/2021 al 30/04/2026
Códigos UNSPCS: los códigos señalados al inicio del documento
Ubicación: Todo el territorio nacional.
Plataforma: SECOP I y SECOP II
Modalidad: Competitiva –Directa - Especial.

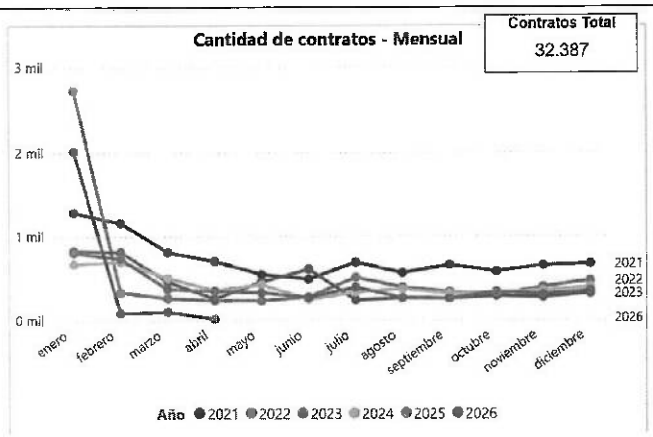
De acuerdo con los datos obtenidos se puede concluir que durante el periodo comprendido entre el 01/01/2021 y 30/04/2026, las Entidades Estatales a nivel nacional han llevado a cabo contrataciones cuyo código UNSPSC corresponde a los contenidos en el proceso analizado.

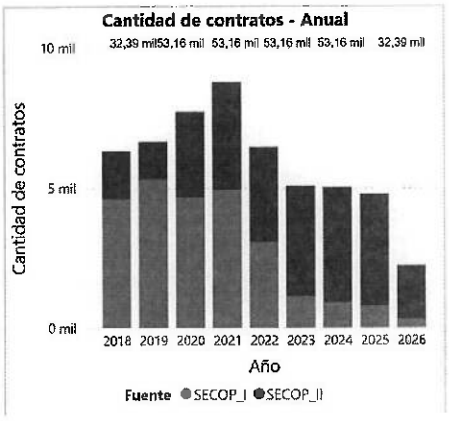
El valor total contratado en las vigencias tomadas como referencia corresponde aproximadamente a $ 9.219.749.029.580:



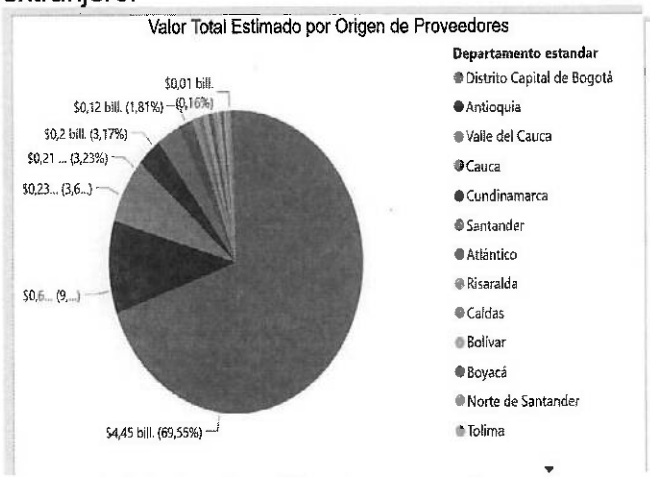
Adicional a lo anterior, si se consideran la cantidad de contratos celebrados, es posible observar que se han acreditado un total de 32.387 contratos:

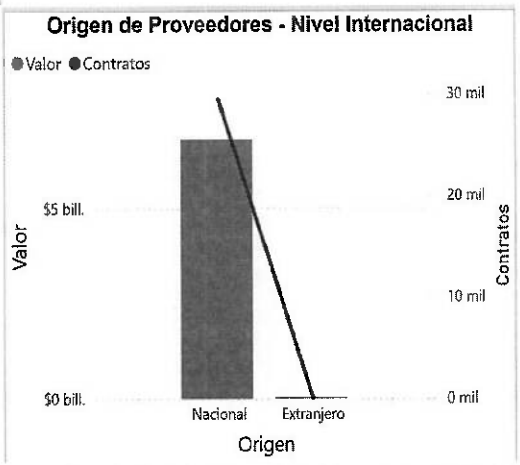
AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.





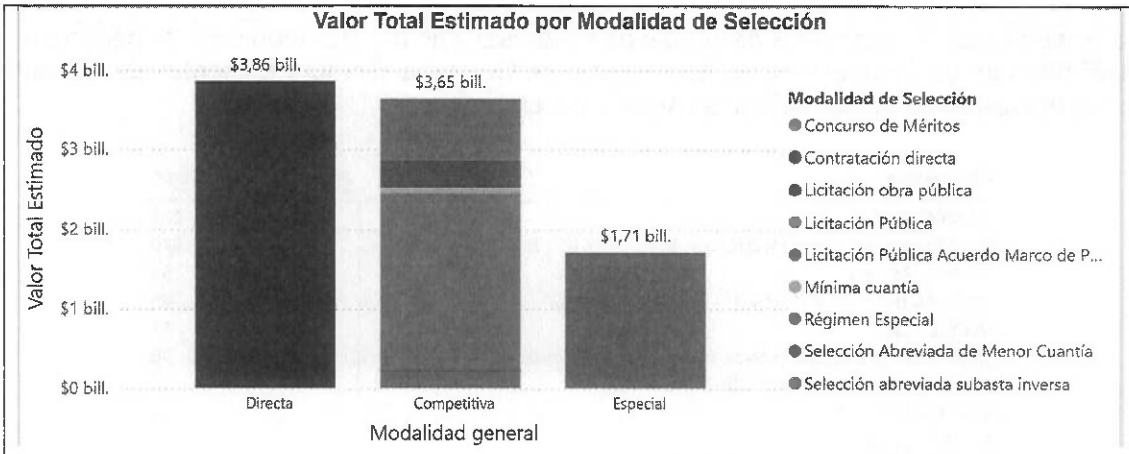
Dentro de la información arrojada por la herramienta de análisis de demanda, es posible observar la ubicación de los proveedores a nivel nacional que hacen parte del mercado relacionado con el código filtrado, evidenciando que los proveedores se encuentran a lo largo de todo el territorio nacional e incluso el mercado cuenta con oferentes del servicio con origen extranjero.





La modalidad más utilizada y aquella a la que se adjudicó el mayor presupuesto fue la Contratación Directa, seguida de la Licitación Pública, el Régimen Especial, la Selección Abreviada por Subasta Inversa, la Selección Abreviada de Menor Cuantía, la Mínima Cuantía y, en último lugar, el Concurso de Méritos.

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.



Es importante considerar que la modalidad de contratación depende de igual forma de la necesidad puntual de la Entidad, del régimen y del presupuesto asignado para la vigencia

3. Análisis de la oferta:

3.1. ¿Quién vende?

Los proveedores en el Mercado nacional de Seguridad Digital

- Microsoft
- ASF
- Controles Empresariales
- Software One
- Equiparo
- Némesis Asociados S.A
- Black Hat Archetype
- Etek International Corporation Sucursal Colombia
- B-Secure
- Technology Partners
- Internexa S.A
- Palo alto
- Fortinet
- Check point
- Sophos
- Cisco

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

La Entidad realizó búsqueda de procesos en el SECOP II y por medio de la herramienta MAE (Modelo de Abastecimiento Estratégico) de Colombia Compra Eficiente, identificando como proveedores del servicio a las siguientes empresas:

Proveedores	Número de Contratos
CAMERFIRMA	221
Gestión de Seguridad Electrónica SA	180
HEIMCORE SAS	55
GAMMA INGENIEROS SAS	45
WEXLER SAS	37
Royal Tech Group SAS (cotizacionesroyaltechgroup)	36
GRUPO MICROSISTEMAS COLOMBIA SAS	32
CERTICAMARA SA	31
KAVANTIC SAS	31
GLOBAL TECHNOLOGY SERVICES GTS SA	27
ANDES SCD SA	26
INFORTEC SOLUCIONES SAS	26
CLOUD CITY	23
ITSEC SAS	22
DATASEC SAS	21
REDCOMPUTO LTDA	21
STAR SOLUTIONS TI SAS	21
CLUSTER DE SERVICIOS SAS	20
MCE NET SOLUTIONS SAS	20
MCO GLOBAL SAS	20
REDNEET SAS	20
THOMAS SIGNE SAS	20
CCD COMPAÑIA DE CIBERSEGURIDAD Y DEFENSA SAS	19
STS SAS	19
PCM	18
GLOBALTEK SECURITY SAS	17
COMPAÑIA DE INGENIEROS DE SISTEMAS ASOCIADOS COINSA SAS	16
CONTROLES EMPRESARIALES SAS	16
SOLUCIONES EN SEGURIDAD INFORMATICA SAS	15
TEK SOLUCIONES TECNOLOGICAS SAS	15
GOLD SYS LTDA	14
SOFTSECURITY SAS	14
EYC INGENIEROS SAS	13
LEIDY JOHANA MONTOYA CARDONA	13
Olimpia IT	13
COLSOF SAS	12
INFO COMUNICACIONES SAS	12
MSL DISTRIBUCIONES Y CIA SAS	12
OPEN GROUP SAS	12

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Proveedores	Número de Contratos
SAFETY IN DEEP SAS	11
COLSISTEC	10
CORBAN COMPUTADORES SAS	10
MICROTEL SAS	10
SOLUCIONES ICG	10
COMCEL SA	9
CREAR IMAGEN DISEÑO WEB Y MULTIMEDIA SAS	9
EDEA NETWORKS SAS	9
INGENIERIA TELEMATICA SAS	9
PC ON LINE ALTA TECNOLOGIA SAS	9
ASF SOLUCIONES SAS	8
CorelP	8
CS TECNOLOGIA SA	8
INFORMACION LOCALIZADA SAS	8
INGENIERIA Y TELECOMUNICACIONES DE COLOMBIA SAS	8
LATTITUDE CORP SAS	8
Némesis Asociados sa	8
SANOLIVAR SAS	8
SS IP SAS	8
SUMINISTROS OBRAS Y SISTEMAS	8
ActivosTI	7
BUSINESS CENTER WAL SAS	7
COMUNICACIONES E INFORMATICA SAS	7
GREEN SERVICES AND SOLUTIONS SAS	7
GROW DATA SAS	7
GRUPO METRO Y CIA LTDA	7
Ona Systems SAS	7
REALTIME CONSULTING SERVICES SAS	7
Software Colombia Servicios Informáticos SAS	7
UNBIT LTDA	7
ARIE SAUL SAPORTAS BERMUDEZ	6
AXIS IT	6
BIT512 SOLUCIONES TI SAS	6
COMERCIALIZADORA SERLECOM	6
DATA INTEGRAL	6
DB SYSTEM SAS	6
ECOMIL SAS	6
EQUIPARO SAS	6
EUPHORIANET SAS	6

Determinación de requisitos de Capacidad Financiera y Organizacional

Para analizar y establecer los indicadores de Capacidad Financiera y Capacidad Organizacional para el presente proceso, la Entidad tomó como base la siguiente información:

Los indicadores de capacidad financiera y capacidad organizacional reportados en el RUP con corte al 31 de diciembre de 2024, así como aquellos actualizados al 31 de diciembre de 2025 —consulta realizada en SECOP II y RUES—, corresponden a cincuenta y cuatro (57) empresas que, en los últimos meses, se han presentado a procesos de selección con objetos contractuales similares al que pretende satisfacer la Entidad. Los datos obtenidos se relacionan a continuación:

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitaria al correo electrónico atencion.ciudadano@inder.gov.co.

Se procede a continuación con el cálculo de estadísticas de posición que permitan generar conclusiones frente a los indicadores del proceso, así:

SISTEMA INTEGRAL DE PROTECCIÓN					
MUESTREO INDICADORES FINANCIEROS corte 2024-2025 / extraido 2026 / FUENTE RUP					
No.	CAPACIDAD FINANCIERA			CAPACIDAD ORGANIZACIONAL	
	INDICE DE LIQUIDEZ	INDICE DE ENDEUDAMIENTO	RAZÓN DE COBERTURA DE INTERESES	RENTABILIDAD DEL PATRIMONIO	RENTABILIDAD DEL ACTIVO
1	1,89	0,62	43,16	0,69	0,26
2	4,05	0,19	336,74	0,91	0,73
3	1,89	0,55	20,6	0,36	0,16
4	2,22	0,47	15,64	0,34	0,18
5	1,59	0,55	320,49	0,53	0,23
6	2,29	0,53	96,29	0,35	0,16
7	1,99	0,29	52,88	0,12	0,08
8	2,92	0,34	INDETERMINADO	0,13	0,08
9	2,17	0,44	7,7	0,2	0,11
10	1,44	0,60	5,96	0,6	0,24
11	3,29	0,26	27,94	0,12	0,09
12	2,08	0,44	164,53	0,45	0,25
13	3,23	0,45	3,01	0,17	0,09
14	6,99	0,54	22,37	0,67	0,3
15	1,84	0,46	24,42	0,21	0,11
16	1,46	0,58	261,39	0,3	0,12
17	2,5	0,38	521,73	0,16	0,1
18	9,33	0,31	69,22	0,22	0,14
19	2,14	0,64	INDETERMINADO	-0,01	0,00
20	2,51	0,39	608,97	0,34	0,21
21	1,45	0,64	662,34	0,18	0,06
22	2,57	0,44	29,65	0,18	0,10
23	2,29	0,42	4,39	0,05	0,03
24	2	0,59	6,91	0,29	0,11
25	1,27	0,69	25,66	0,28	0,08
26	6,19	0,23	26,66	0,19	0,14
27	2,9	0,61	1,75	0,2	0,08
28	1,6	0,52	61,29	0,28	0,13
29	5,22	0,5	17,7	0,25	0,12
30	1,51	0,59	12,12	0,24	0,1
31	1,71	0,67	1,45	0,09	0,03
32	2,34	0,59	10,86	0,42	0,17
33	3,19	0,28	1.011,77	0,4	0,28
34	1,51	0,65	10,81	0,61	0,21
35	1,03	0,63	1,92	0,17	0,06
36	1,99	0,26	INDETERMINADO	0,46	0,33

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitaria al correo electrónico atencion.ciudadano@inder.gov.co.

37	5,61	0,12	12,23	0,36	0,31
38	2,87	0,45	13,79	0,75	0,41
39	1,23	0,8	5,18	0,16	0,03
40	2,11	0,7	1,59	0,77	0,22
41	2,1	0,46	47,84	0,38	0,2
42	10,71	0,26	INDETERMINADO	0,13	0,1
43	16,16	0,07	58,59	0,15	0,14
44	2,4	0,36	INDETERMINADO	0,21	0,13
45	2,52	0,36	419,53	0,23	0,14
46	1,89	0,52	97,28	0,1	0,04
47	6,4	0,27	214,16	0,23	0,17
48	4,34	0,3	INDETERMINADO	0,21	0,14
49	2,06	0,59	7,5	0,09	0,03
50	3,04	0,53	8,77	0,26	0,12
51	6,99	0,43	34,7	0,21	0,11
52	1,42	0,75	11,54	0,96	0,23
53	3,12	0,48	6,51	0,40	0,20
54	2,63	0,61	7,1	0,64	0,25
55	3,39	0,45	39,68	0,53	0,29
56	1,45	0,59	17,14	0,55	0,22
57	2,22	0,56	5,02	0,32	0,14

Se procede a continuación con el cálculo de estadísticas de tendencia central, dispersión y posición que permitirán generar conclusiones frente a los indicadores del proceso, así:

ANÁLISIS NÚMERICO					
PROMEDIO	3,179824561	0,473684211	107,7739216	0,329649123	0,162982456
MINIMO	**1,03**	0,07	**1,45**	**0,05**	**0,03**
MAXIMO	16,16	**0,75**	1011,77	0,96	0,73
MEDIANA	2,29	0,48	22,37	0,26	0,14
DESVIACIÓN	2,6	0,2	209,8	0,2	0,1
MAX-DESV	13,5	0,59	802,0	0,7	0,6

	CAPACIDAD FINANCIERA			CAPACIDAD ORGANIZACIONAL	
	INDICE DE LIQUIDEZ	**NIVEL DE ENDEUDAMIENTO**	**COBERTURA DE INTERESES**	**RENTABILIDAD PATRIMONIO**	**RENTABILIDAD ACTIVO**
	Mayor o igual (≥) a 1,03	Menor o igual (≤) a 0.75	Mayor o igual (≥) a 1.45	Mayor o igual (≥) a 0.05	Mayor o igual (≥) a 0.03
% CUMPLIMIENTO	100%	100%	100%	98%	98%
	EL 100% DE LOS DATOS CUMPLE CON EL INDICADOR.	EL 100% DE LOS DATOS CUMPLE CON EL INDICADOR.	EL 100% DE LOS DATOS CUMPLE CON EL INDICADOR.	UN DATO DE LA MUESTRA NO CUMPLEN CON EL INDICADOR ARROJADO	UN DATO DE LA MUESTRA NO CUMPLEN CON EL INDICADOR ARROJADO

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Los indicadores obtenidos del análisis y que se fijan como requisitos habilitantes para el proceso de selección analizado son los siguientes:

INDICADORES DIFERENCIADOS PARA MIPYMES				
CAPACIDAD FINANCIERA			CAPACIDAD ORGANIZACIONAL	
INDICE DE LIQUIDEZ	NIVEL DE ENDEUDAMIENTO	COBERTURA DE INTERESES	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
Mayor o igual (≥) a 1.0	Menor o igual (≤) a 0.75	Mayor o igual (≥) a 1.3	Mayor o igual (≥) a 0.04	Mayor o igual (≥) a 0.02

3.2. ¿Cuál es la dinámica de producción, distribución y entrega de los bienes y servicios?

El proceso de producción, distribución y entrega de **SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (ENDPOINT DETECTION AND RESPONSE), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL)**

El proceso de producción, distribución y entrega de la necesidad actual, se detalla a continuación:

La dinámica de producción, distribución y entrega de soluciones de seguridad digital, como EDR, protección de correo electrónico, herramientas colaborativas y WAF, se caracteriza por modelos altamente industrializados, escalables y soportados principalmente en infraestructuras en la nube. A nivel técnico, los fabricantes desarrollan estas soluciones bajo esquemas de mejora continua, incorporando capacidades avanzadas de inteligencia artificial, aprendizaje automático, análisis de comportamiento, detección de amenazas en tiempo real y actualización permanente de sus mecanismos de protección, con el propósito de responder de manera oportuna a la evolución de las amenazas cibernéticas.
En este contexto, se ha consolidado el uso de soluciones especializadas de ciberseguridad orientadas a la protección de diferentes componentes tecnológicos de las organizaciones, como los endpoints, servidores, correo electrónico, herramientas colaborativas y aplicaciones web. Estas soluciones permiten fortalecer la postura de seguridad mediante controles específicos para cada uno de estos componentes, facilitando la prevención, detección y respuesta frente a amenazas como malware, ransomware, phishing, suplantación de identidad, archivos maliciosos, comportamientos anómalos, explotación de vulnerabilidades y ataques dirigidos contra aplicaciones y servicios web.
Estas herramientas son empaquetadas principalmente como software bajo modelos SaaS (Software como Servicio), así como mediante esquemas de implementación en la nube o, cuando las características técnicas lo requieren, mediante componentes instalados en la infraestructura de la entidad. Este modelo permite a los proveedores distribuir y actualizar las soluciones de manera global sin necesidad de medios físicos, reduciendo tiempos y

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

costos logísticos. En particular, las soluciones EDR pueden operar mediante agentes instalados en endpoints y servidores y administrados desde consolas centralizadas, mientras que la protección de correo, las herramientas colaborativas y el WAF pueden integrarse con los servicios tecnológicos correspondientes para aplicar controles de seguridad de manera continua.

En la práctica, esto significa que, una vez adquirido el servicio, su activación, configuración y despliegue pueden realizarse de forma ágil mediante consolas web, mecanismos de administración centralizada, integraciones con servicios existentes y agentes de instalación remota cuando corresponda. La entrega puede incluir componentes como acceso a plataformas de gestión, configuración inicial, aplicación de políticas de seguridad, monitoreo de los activos protegidos, mecanismos de detección y respuesta, soporte técnico especializado y actualizaciones permanentes de los motores, reglas y mecanismos de protección frente a nuevas amenazas.

En resumen, se trata de soluciones de rápida disponibilidad, cuya distribución se encuentra principalmente digitalizada y que permiten reducir los tiempos asociados a su implementación y actualización. La incorporación de EDR, protección de correo electrónico, herramientas colaborativas y WAF permite a entidades públicas como el INDER Medellín fortalecer la protección de sus dispositivos, servidores, comunicaciones, información y aplicaciones web, estableciendo controles de seguridad en diferentes puntos de exposición y contribuyendo a prevenir, detectar y contener oportunamente amenazas cibernéticas, con soporte técnico especializado y posibilidades de escalabilidad de acuerdo con las necesidades institucionales.

3.3 ESTUDIO DE MERCADO

Se inició el estudio de mercado consultando en la TVEC si algún acuerdo marco incluye la solución a la medida del INDER Medellín y se encuentra lo siguiente:

En el acuerdo no hay una solución integral que cumpla con la especificidad del requerimiento técnico del INDER Medellín, ya que al filtrar los componentes necesarios para generar un ecosistema de seguridad encontramos que están en diferente segmento (Esto generaría diferentes eventos de cotización y un contrato diferente por cada segmento) y son de diferentes fabricantes lo cual puede interferir para realizar la integración de todos los componentes en una única plataforma.

La siguiente tabla corresponde a Información filtrada acuerdo software por catálogo

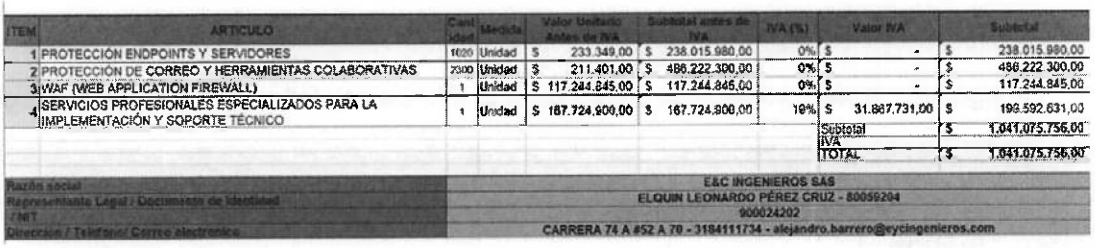
Codigo/SKU	Segmento	Catálogo/Fabricante	Descripcion
SRX4100-S-AS-1	Software General	JUNIPER	One year subscription for Juniper-cloud based Anti-spam service on SRX4100
SRX4100-S-AS-3	Software General	JUNIPER	Three year subscription for Juniper-cloud based Anti-spam service on SRX4100
SRX4200-S-AS-3	Software General	JUNIPER	Three year subscription for Juniper-cloud based Anti-spam service on SRX4200
SRX4200-S-AV-1	Software General	JUNIPER	One year subscription for Juniper-cloud based AV service on SRX4200

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

MCS-WAF	Software General	MEGA MLA, S.A. DE C.V.	Licencias en nube Herramienta HOPEX
aSEC	Software General	SANGFOR	Licensed per physical CPU. Standard security module includes real-time virus prevention, ransomware prevention, vulnerabilities discovery and repair, etc,. Security out of the box: host security module auto-installation. Asset identification: automatically identify and report the installation status of OSes and apps, visualize asset security status. Threat handling: support threat handling features of Endpoint Secure, such as anti-virus, scanning and detection, anti-ransomware, etc,. Vulnerabilities management: scan and repair VMs' vulneratbilities, automatic snapshot for VMs before repair Real-time correlated snapshot: all assets are protected on a daily basis through scheduled snapshot, data can be protected by snapshots once uninstallation of security module, risk of ransomware and vulnerabilities repair and such situations are detected.
aSEC	Software General	SANGFOR	Licensed per physical CPU. Standard security module includes real-time virus prevention, ransomware prevention, vulnerabilities discovery and repair, etc,. Security out of the box: host security module auto-installation. Asset identification: automatically identify and report the installation status of OSes and apps, visualize asset security status. Threat handling: support threat handling features of Endpoint Secure, such as anti-virus, scanning and detection, anti-ransomware, etc,. Vulnerabilities management: scan and repair VMs' vulneratbilities, automatic snapshot for VMs before repair Real-time correlated snapshot: all assets are protected on a daily basis through scheduled snapshot, data can be protected by snapshots once uninstallation of security module, risk of ransomware and vulnerabilities repair and such situations are detected.
aSEC	Software General	SANGFOR	Licensed per physical CPU. Standard security module includes real-time virus prevention, ransomware prevention, vulnerabilities discovery and repair, etc,. Security out of the box: host security module auto-installation. Asset identification: automatically identify and report the installation status of OSes and apps, visualize asset security status. Threat handling: support threat handling features of Endpoint Secure, such as anti-virus, scanning and detection, anti-ransomware, etc,. Vulnerabilities management: scan and repair VMs' vulneratbilities, automatic snapshot for VMs before repair Real-time correlated snapshot: all assets are protected on a daily basis through scheduled snapshot, data can be protected by snapshots once uninstallation of security module, risk of ransomware and vulnerabilities repair and such situations are detected.

Dentro del estudio de mercado también se procedió a realizar un estudio solicitando cotizaciones a varias empresas del sector comercial que proveen este tipo de servicio y se obtuvieron las siguientes cotizaciones.

COTIZACIÓN 1



ITEM	ARTICULO	Cantidad	Medida	Valor Unitario Antes de IVA	Subtotal antes de IVA	IVA (%)	Valor IVA	Subtotal
1	PROTECCIÓN ENDPOINTS Y SERVIDORES	1020	Unidad	$ 233.349,00	$ 238.015.980,00	0%	$ -	$ 238.015.980,00
2	PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS	2300	Unidad	$ 211.401,00	$ 486.222.300,00	0%	$ -	$ 486.222.300,00
3	WAF (WEB APPLICATION FIREWALL)	1	Unidad	$ 117.244.845,00	$ 117.244.845,00	0%	$ -	$ 117.244.845,00
4	SERVICIOS PROFESIONALES ESPECIALIZADOS PARA LA IMPLEMENTACIÓN Y SOPORTE TÉCNICO	1	Unidad	$ 167.724.900,00	$ 167.724.900,00	19%	$ 31.867.731,00	$ 199.592.631,00
							Subtotal	$ 1.041.075.756,00
							IVA	
							TOTAL	$ 1.041.075.756,00
Razón social					E&C INGENIEROS SAS			
Representante Legal / Documento de identidad					ELQUIN LEONARDO PÉREZ CRUZ - 80059204			
/ NIT					900024202			
Dirección / Teléfono / Correo electrónico					CARRERA 74 A #52 A 70 - 3184111734 - alejandro.barrero@eycingenieros.com			

COTIZACIÓN 2

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

	ARTICULO	Cantidad	Medida	Valor Unitario Antes de IVA	Subtotal antes de IVA	IVA (%)	Valor IVA	Subtotal
1	PROTECCIÓN ENDPOINTS Y SERVIDORES	1020	Unidad	$ 201.613,00	$ 205.645.260,00	0%	$ -	$ 205.645.260,00
2	PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS	2380	Unidad	$ 182.851,00	$ 420.097.300,00	0%	$ -	$ 420.097.300,00
3	WAF (WEB APPLICATION FIREWALL)	1	Unidad	$ 101.299.546,00	$ 101.299.546,00	0%	$ -	$ 101.299.546,00
4	SERVICIOS PROFESIONALES ESPECIALIZADOS PARA LA IMPLEMENTACIÓN Y SOPORTE TÉCNICO	1	Unidad	$ 144.914.314,00	$ 144.914.314,00	19%	$ 27.533.720,00	$ 172.448.034,00
							Subtotal	$ 899.490.140,00
							IVA	
							TOTAL	$ 899.490.140,00

Razón social	CONVIEST S A S
Representante Legal / Documento de Identidad	LUIS GUILLERMO MOLANO NAVAS
NIT	900157429
Dirección / Teléfono / Correo electrónico	3106578297 - paola.morant@conviest.com

COTIZACIÓN 3

	ARTICULO	Cantidad	Medida	Valor Unitario Antes de IVA	Subtotal antes de IVA	IVA (%)	Valor IVA	Subtotal
1	PROTECCIÓN ENDPOINTS Y SERVIDORES	1020	Unidad	$ 189,500.00	$ 193,290,000.00	0%	$ -	$ 193,290,000.00
2	PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS	2300	Unidad	$ 172,205.00	$ 396,060,000.00	0%	$ -	$ 396,060,000.00
3	WAF (WEB APPLICATION FIREWALL)	1	Unidad	$ 96,800,000.00	$ 96,800,000.00	0%	$ -	$ 96,800,000.00
4	SERVICIOS PROFESIONALES ESPECIALIZADOS PARA LA IMPLEMENTACIÓN Y SOPORTE TÉCNICO	1	Unidad	$ 118,000,000.00	$ 118,000,000.00	19%	$ 22,420,000.00	$ 140,420,000.00
							Subtotal	$ 826,570,000.00
							IVA	
							TOTAL	$ 826,570,000.00

Razón social	RIT ENTERPRISE SOLUTIONS SAS
Representante Legal / Documento de Identidad	JUAN ALVARO ALEJANDRO ROJAS ERAS CC 17.351.683
NIT	900.838.520-1
Dirección / Teléfono / Correo electrónico	AV CR 9 No. 115 - 06/08 OF 1207 BG TERRA PARK - 6043218 / 3124218481 - comercial@ritenterprise.com

Con las cotizaciones obtenidas en las respuestas de los proveedores evidenciamos que si existen empresas en el mercado que pueden proveer el servicio descrito en las especificaciones técnicas

ESTUDIO DE MERCADO:

El comité estructurador del proceso analizado realizó un sondeo de posibles empresas que pueden satisfacer la necesidad objeto del presente estudio, con el fin de conocer los precios del mercado para "ADQUIRIR E IMPLEMENTAR UN SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (ENDPOINT DETECTION AND RESPONSE), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL) PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN", la solicitud de cotizaciones se realizó por medio de correo electrónico a empresas del sector, obteniendo el siguiente resultado:

					CONVIEST SAS	RIT ENTERPRISE SOLUTION SAS	E&C INGENIEROS SAS
					COTIZANTE 1	COTIZANTE 2	COTIZANTE 3
Ítem	Nombre	Unidad	Cantidad	TARIFA DE IVA	VALOR TOTAL CON CANTIDADES	VALOR TOTAL CON CANTIDADES	VALOR TOTAL CON CANTIDADES

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

1	PROTECCIÓN ENDPOINTS Y SERVIDORES	UNIDAD	1020	0%	$ 198.028.920	$ 193.290.000	$ 205.645.260
2	PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS	UNIDAD	2300	0%	$ 404.537.800	$ 396.060.000	$ 420.097.300
3	WAF (WEB APPLICATION FIREWALL)	UNIDAD	1	0%	$ 97.547.711	$ 96.800.000	$ 101.299.546
4	SERVICIOS PROFESIONALES ESPECIALIZADOS PARA LA IMPLEMENTACIÓN Y SOPORTE TÉCNICO	UNIDAD	1	19%	$ 166.061.069	$ 140.420.000	$ 172.448.034

Para los efectos, las cotizaciones se analizaron utilizando formulas estadísticas diversas, como el MÍNIMO, MÁXIMO, MEDIANA y PROMEDIO esto con el objeto de establecer de manera razonable con la dinámica del mercado los precios de referencia.

El criterio utilizado en este caso para el establecimiento de los **PRECIOS UNITARIOS** de referencia es el **MÍNIMO**, se presenta en la siguiente tabla el resultado obtenido:

					ANALISIS NUMERICO			
Ítem	**Nombre**	**Unidad**	**Cantidad**	**TARIFA DE IVA**	**PROMEDIO**	**MINIMO**	**MAXIMO**	**MEDIANA**
1	PROTECCIÓN ENDPOINTS Y SERVIDORES	UNIDAD	1020	0%	$ 195.086	$ 189.500,00	$ 201.613,00	$ 194.146
2	PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS	UNIDAD	2300	0%	$ 176.912	$ 172.200,00	$ 182.651,00	$ 175.886
3	WAF (WEB APPLICATION FIREWALL)	UNIDAD	1	0%	$ 98.549.086	$ 96.800.000	$ 101.299.546,00	$ 97.547.711
4	SERVICIOS PROFESIONALES ESPECIALIZADOS PARA LA IMPLEMENTACIÓN Y SOPORTE TÉCNICO	UNIDAD	1	19%	$150.465.128	$ 140.420.000	$ 166.061.069,	$ 144.914.314

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.

Valor presupuesto estimado:

De acuerdo con la necesidad puntual del Instituto y los precios unitarios de referencia definidos para el proceso se determinó el valor estimado del proceso así:

					PRECIO UNITARIO Y TOTAL, PRECIO OFICIAL (POR PROMEDIO)			PRESUPUESTO ESTIMADO BASADO EN EL MÍNIMO
					PRECIO DE REFERENCIA			ESTIMADO
Ítem	Nombre	Unidad	Cantidad	TARIFA DE IVA	VALOR UNITARIO ANTES DE IVA	VALOR IVA	VALOR UNITARIO IVA INCLUIDO	VALOR TOTAL
1	PROTECCIÓN ENDPOINTS Y SERVIDORES	UNIDAD	1020	0%	$ 189.500	$ 0	$ 189.500	$ 193.290.000
2	PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS	UNIDAD	2300	0%	$ 172.200	$ 0	$ 172.200	$ 396.060.000
3	WAF (WEB APPLICATION FIREWALL)	UNIDAD	1	0%	$ 96.800.000	$ 0	$ 96.800.000	$ 96.800.000
4	SERVICIOS PROFESIONALES ESPECIALIZADOS PARA LA IMPLEMENTACIÓN Y SOPORTE TÉCNICO	UNIDAD	1	19%	$118.000.000	$ 22.420.000	$ 140.420.000	$ 140.420.000
							TOTAL PRESUPUESTO OFICIAL	$ 826.570.000

Presupuesto estimado:

Del análisis realizado es posible concluir que el presupuesto estimado para el cumplimiento del objeto "**ADQUIRIR E IMPLEMENTAR UN SISTEMA DE PROTECCIÓN EN**

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitaria al correo electrónico atencion.ciudadano@inder.gov.co.

CIBERSEGURIDAD EDR (ENDPOINT DETECTION AND RESPONSE), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL) PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN" asciende a la suma de **OCHOCIENTOS VEINTISÉIS MILLONES QUINIENTOS SETENTA MIL PESOS M.L ($ 826.570.000),**incluidos todos los impuestos, costos directos, indirectos, tasas, estampillas, timbres y contribuciones a que hubiere lugar.

Comité de Estructuración y Evaluación Contractual,

JORGE ALEJANDRO ANGEL OSORIO
Subdirector Administrativo y Financiero

Maria Alejandra Cañola Estrada V.Bo. Financiera	Harrison Alexander Hernández Rúa Vo. Bo. Técnico Sergio Antonio Henao Botero Vo. Bo. Técnico	Santiago Restrepo Vasquez Vo. Bo. Jurídica	Alejandro Mesa Giraldo Vo. Bo Ambiental

AVISO DE PRIVACIDAD
INDER - MEDELLÍN con NIT 800194096-0 dando cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios, le informa a todos los titulares de datos personales insertos en el presente documento, que el uso ha sido realizado con previa autorización, preservando la protección de sus datos personales en la recolección, circulación y tratamiento para la(s) finalidad(es) que han sido autorizadas de acuerdo con la política de tratamiento y protección de datos personales que se encuentra a disposición en el sitio web oficialwww.inder.gov.co, en la sede administrativa ubicada en calle 47D # 75 – 276 barrio Velódromo, Medellín – Colombia, y/o solicitarla al correo electrónico atencion.ciudadano@inder.gov.co.