SELECCIÓN ABREVIADA DE MENOR CUANTIA

1. DESCRIPCIÓN DE LA NECESIDAD.

La Constitución Política de Colombia de 1991, estable en su artículo 52 que, *"(…) El deporte y la recreación, forman parte de la educación y constituyen gasto público social. Se reconoce el derecho de todas las personas a la recreación, a la práctica del deporte y al aprovechamiento del tiempo libre. (…)".* A su vez, la Ley 181 de 1995 que desarrolló la anterior norma constitucional, establece las disposiciones para el fomento del deporte, la recreación, el aprovechamiento del tiempo libre y la educación física, y crea el Sistema Nacional del Deporte, consagrando en los entes deportivos municipales y distritales la responsabilidad de desarrollar acciones encaminadas a cumplir este propósito.

En concordancia con lo anterior, se crea el INSTITUTO DE DEPORTES Y RECREACIÓN - INDER, a través del Decreto 270 de 1993, modificado por el Decreto 271 de 1993, Acuerdo 65 de 1998 y Decreto 181 de 2002, entidad de orden distrital, se encuentra dotada de personería jurídica, autonomía administrativa y patrimonio independiente, cuyo objeto misional está enfocado al fomento del deporte, la recreación y la actividad física, mediante una amplia oferta institucional, en espacios que contribuyen al mejoramiento de la cultura ciudadana y la calidad de vida de los habitantes de la ciudad.

Así mismo, es importante considerar que en el PLAN DE DESARROLLO DISTRITAL MEDELLÍN TE QUIERE 2024 - 2027, específicamente en el Pilar 1, denominado "CREEMOS EN LA EDUCACIÓN Y EN LAS OPORTUNIDADES PARA EL BIENESTAR ECONÓMICO," se encuentra el componente "DEPORTE, RECREACIÓN Y ACTIVIDAD FÍSICA PARA EL BIENESTAR."

Este componente tiene como objetivo aumentar el acceso, uso y disfrute de espacios idóneos para la práctica del deporte, la recreación y la actividad física en el distrito de Medellín, promoviendo así el fortalecimiento del sector deportivo y el mejoramiento del bienestar y la calidad de vida de la población. Para alcanzar estos objetivos, se formularon los siguientes programas:

1. Fortalecimiento Distrital del Deporte, la Recreación y la Actividad Física
2. Escenarios Deportivos, Recreativos y de Actividad Física para el Bienestar
3. Posicionamiento y Liderazgo Deportivo y Recreativo.
4. Oportunidades para el Deporte, la Recreación, la Actividad Física y Mental, y el Aprovechamiento del Tiempo Libre

En este sentido, dentro del programa "Fortalecimiento Distrital del Deporte, la Recreación y la Actividad Física," se encuentra el área de tecnología adscrita a la Subdirección Administrativa y Financiera, cuyo objetivo es "*Liderar la transformación digital del INDER Medellín a través de la habilitación de capacidades tecnológicas que permitan el cumplimiento de los objetivos estratégicos."* Y como aporte estratégico del proceso "*Habilitar capacidades tecnológicas, mediante el uso y aprovechamiento de las tecnologías de la información que permitan ofrecer servicios y tramites innovadores".*

FIRMADO

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, en su calidad de entidad pública, cuenta con un Sistema de Seguridad de la Información conformado por diversas herramientas tecnológicas y controles orientados a garantizar la protección de sus activos digitales. Este sistema incluye componentes como soluciones de antivirus para equipos de escritorio y servidores on premise, mecanismos de filtrado antispam para la protección de las cuentas de correo institucionales y un firewall de aplicaciones web (WAF). En conjunto, estos elementos constituyen una base esencial para asegurar la integridad, disponibilidad y confidencialidad de la información institucional.

El antivirus permite la detección y mitigación de software malicioso que pueda comprometer los equipos de cómputo, mientras que el sistema antispam actúa como primera línea de defensa frente a ataques de ingeniería social, como el phishing y otros correos maliciosos que buscan vulnerar la seguridad de los usuarios. Por su parte, el firewall de aplicaciones web opera como un filtro avanzado de seguridad en los portales institucionales, encargado de supervisar, analizar y bloquear el tráfico malicioso, así como prevenir ataques comunes como inyecciones SQL, cross-site scripting (XSS) y otros intentos de explotación de vulnerabilidades.

Este conjunto de controles no solo contribuye al correcto funcionamiento de la infraestructura tecnológica, sino que también responde a las disposiciones establecidas en la política de Gobierno Digital en Colombia, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones. Dicha política establece la obligación de las entidades estatales de implementar estrategias integrales de seguridad digital, orientadas a la gestión de riesgos, la protección de la información y la continuidad de los servicios digitales.

En este marco, el fortalecimiento y la inversión continua en herramientas de Seguridad Digital no es opcional, sino un requisito normativo que busca garantizar la confianza de los ciudadanos en los servicios digitales del Estado. Asimismo, se alinea con buenas prácticas internacionales como las definidas en la norma ISO/IEC 27001, que promueve la implementación de sistemas de gestión de seguridad de la información basados en la mejora continua.

Por lo tanto, para mantener y robustecer este ecosistema de seguridad, el INDER Medellín requiere **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.** Los servicios deben ser desplegados en nube y estar relacionados bajo una sola marca y deberán ser administrados mediante una sola interfaz de administración.

Las soluciones deberán proporcionar 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.
Las plataformas deberán ser desplegadas y administradas en nube bajo una sola interfaz, soportar la protección de aplicaciones institucionales expuestas a internet en entornos de

FIRMADO ELECTRONICAMENTE

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.

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:

DIMENSIONAMIENTO DE LA SOLUCIÓN

La solución contará con los siguientes elementos principales con características actualizadas de protección y capacidad de escalamiento a sistemas mas completos de protección en ciberseguridad:

1. Un WAF (WEB APPLICATION FIREWALL) que permita la protección de máximo 10 sitios.
2. 1020 licencias para la PROTECCIÓN ENDPOINTS Y SERVIDORES en sitio.
3. 2300 licencias para la PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS.
4. Administración bajo una sola interfaz en nube.

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 diferentes segmentos (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	Descripción
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
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.

IMPRESO ES COPIA NO CONTROLADA

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.

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 / Telefono/ Correo electronico	CARRERA 74 A #52 A 70 - 3184111734 - alejandro.barrero@eycingenieros.com

COTIZACIÓN 2

ITEM	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	2300	Unidad	$ 182.651,00	$ 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	900915742 9
Dirección / Telefono/ Correo electronico	3106679297 - paola.moran@conviest.com

COPIA EN ORIGINAL

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.

COTIZACIÓN 3

T	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	$ 172,200.00	$ 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 / NIT	JUAN ALVARO ALEJANDRO ROJAS ERAS CC 12.991.662 900.836.520-1
Dirección / Telefono/ Correo electronico	AV CR 9 No. 115 - 06/30 OF 1207 ED. TIERRA FIRME - BOGOTA / 3175073040 - comercial@ritenteprise.com.co

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 de este estudio previo, por lo tanto, se sugiere tener en cuenta la modalidad de selección abreviada, ya que no hay un IAD que contenga la soluciones de seguridad requerida, y adelantar un proceso de selección que permita contratar un proveedor idóneo para el suministro del servicio apropiado para el presupuesto y naturaleza del proceso, con el fin de garantizar la eficiencia, transparencia y economía en la adquisición. Este procedimiento facilitará identificar un oferente con la capacidad técnica, experiencia y solvencia necesarias para cumplir con las condiciones establecidas, asegurando la continuidad y calidad de los servicios requeridos por el INDER Medellín, así como la adecuada ejecución de las actividades derivadas de los servicios tecnológicos institucionales.

N°. 1 del Art. 2.2.1.1.2.1.1 del Decreto 1082 de 2015

PLAN DE ACCIÓN: El objeto de este contrato aporta en el desarrollo y cumplimiento del plan de acción del proyecto 200317 “Administración del sistema municipal del deporte, la recreación y la actividad física”.

2. EL OBJETO A CONTRATAR. El Instituto de Deportes y Recreación de Medellín – INDER-, requiere seleccionar el contratista que ejecute el siguiente objeto contractual: **“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 entidad requiere **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.** Los servicios deben ser desplegados en nube y estar relacionados bajo una sola marca y deberán ser administrados mediante una sola interfaz de administración.

2.1. 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 desplegada 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:

La Entidad informa que actualmente cuenta con cargas operativas y consumos que sirven para el dimensionamiento de la plataforma; no obstante, con los datos entregados se espera que el oferente que resulte adjudicado pueda sostener la operación del WAF sin exceder su presupuesto estimado. Igualmente, será responsabilidad del Contratista garantizar que la solución ofertada cuente con una capacidad de operación adecuada durante toda la vigencia de las licencias sin generar un costo adicional para el INDER que sea diferente al presupuesto adjudicado en el contrato.

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

FIRMADO EN ORIGINAL

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.

- 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 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 las liciencias.

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, 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.

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.

FIRMADO EN ORIGINAL

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:

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 20 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 ser 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 20 de noviembre de 2026. De cualquier forma, la vigencia no deberá iniciar sin el recibido a satisfacción.

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

FIRMADO EN ORIGINAL

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.

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.

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

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.

FIRMADO EN ORIGINAL

	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.
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,

FIRMADO ORIGINAL

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.

	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.

FIRMADO EN ORIGINAL

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.

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.

COPIANDO EN ORIGINAL

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.

5.28	27. Ejecutable manipulado.
5.29	28. Ejecutable no confirmado.
5.30	29. Ejecutable sin asignar.
5.31	30. Código grabable.
6	**FUNCIONALIDADES DE REMEDIACIÓN**
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**

FIRMA - NO ORIGINAL

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.

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	consumo de memoria de 350 MB con todos los módulos activados, incluido Threat Hunting, y 1 GB de almacenamiento con todos los módulos activados, incluido Threat Hunting.
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.

FIRMADO ORIGINAL

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.

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
#	**Categoría**	**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	**Identificación de amenazas**	La solución debe utilizar fuentes de inteligencia sobre amenazas para identificar amenazas conocidas
1.8		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	**Amenazas avanzadas**	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		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

FIRMA COPIA ORIGINAL

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.

1.16	**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	**Gestión de archivos**	La solución debe escanear cientos de tipos de archivos diferentes
1.23		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

FIRMADO ORIGINAL

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.

3.4	**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		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	**Gestión de datos**	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	
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	

FIRMA ES ORIGINAL

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.

3.24		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).

FIRMADO EN ORIGINAL

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	**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:**	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.
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.

FIRMADO EN ORIGINAL

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.

1.56		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		Control de acceso basado en roles.
1.63	**Gestión:**	Soporte para inicio de sesión único (SSO).
1.64		Soporte API.
1.65		La solución debe ofrecer transferencia de conocimiento en la fase de implementación sin cargo adicional.
1.66	**Servicios:**	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: ○ Actualizaciones y mantenimiento de producto o Compatibilidad con nuevos sistemas operativos, acceso a versiones nuevas sin costo adicional dentro de la vigencia. ○ 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 ○ 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. ○ 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.

- 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 de la entrega a satisfacción y estar activa 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.

FIRMADO EN ORIGINAL

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 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:

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 contrato y 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 20 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.
   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 20 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 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

FIRMADO EN ORIGINAL

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.

Controls. Entregar evidencia documentada que incluya alcance, criterios de severidad, protocolo y demás contenido de la actividad una vez sea realizada

REQUISITOS HABILITANTES

EXPERIENCIA DEL PROPONENTE:

Todos los documentos deben ser presentados de forma individual (no unificar todo en un solo pdf).

Se tendrá como experiencia general mínima habilitante del proponente la acreditación de máximo dos (2) certificados de contratos ejecutados, terminados y liquidados por el proponente, que el valor sumado de los contratos y expresado en salarios mínimos mensuales legales vigentes (SMMLV) sea igual o superior al presupuesto oficial expresado en (SMMLV), es decir, igual o superior a 472

Los contratos deben encontrarse en el RUP del Proponente y debe relacionarlos en el Formato 3 (Experiencia del Proponente). El Proponente deberá presentar ambos documentos (RUP y Formato 3) para participar del Proceso.

Cada contrato acreditado debe estar identificado al menos en tres (03) de los códigos del clasificador de bienes y servicios de Naciones Unidas a nivel de clase señalados en el siguiente cuadro:

CLASIFICACIÓN	SEGMENTO	FAMILIA	CLASE
43233200	Tecnología de la Información, Radiodifusión y Telecomunicaciones	Software	Software de seguridad y protección
43222500	Tecnología de la Información, Radiodifusión y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de seguridad de red
81111800	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas
81112200	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Mantenimiento y soporte de software

Para la certificación se admite, acta de liquidación o recibido a satisfacción y deberán cumplir con los siguientes requisitos:

a. Fecha de expedición
b. Razón social del contratante

FIRMADO EN ORIGINAL

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. Razón del social del contratista con Nit
d. Teléfonos del contratante (si es empresa privada)
e. Valor final del contrato, expresado en pesos colombianos o SMMLV
f. Fecha de inicio y terminación del contrato.
g. Objeto del contrato, este debe tener relación con el suministro e implementación de soluciones, tecnologías o servicios especializados de ciberseguridad, destinados a fortalecer la protección y seguridad de infraestructuras tecnológicas.

El proponente deberá aportar un certificado expedido por el o los fabricante(s) de la solución ofertada, dirigido a la Entidad donde se especifique que cuenta con un nivel de partner o canal en la categoría más alta dentro del programa de canales del fabricante y su fecha de expedición no podrá ser superior a treinta (30) días calendario contados a partir del cierre del proceso de selección.

La o las certificación(es) deberá(n) demostrar que el o (los) oferente(s) cuenta(n) con mínimo una (1) especialidad del o los fabricante(s) consultable en el sitio web del o los fabricante (s).

PERSONAL PROFESIONAL REQUERIDO

Esta documentación será evaluada en la etapa de requisitos habilitantes.

El personal profesional requerido debe estar vinculado con la empresa interesada en el proceso y demostrar su vinculación de mínimo los últimos 3 meses.

El contratista debe contar con un equipo mínimo de trabajo de 4 integrantes para la ejecución del proyecto, el cual debe estar conformado de la siguiente manera:

ROL	DESCRIPCIÓN
Un (1) Gerente de Proyecto.	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** Debe contar con mínimo diez (10) años de experiencia general, contados a partir de la expedición de la matrícula profesional. **Título de Posgrado en:** Especialización o Maestría en áreas relacionadas con su carrera profesional Debe acreditar mediante una certificación, que tiene fundamentos en ciberseguridad, esta debe ser emitida por el fabricante. Debe acreditar mediante una certificación vigente, conocimientos a nivel profesional en gestión de proyectos.

FIRMADO EN ORIGINAL

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.

	Experiencia específica: Especifica mínima de ocho (8) años gerenciando y/o coordinando proyectos en temas relacionados con seguridad de la información y/o seguridad informática.
Un (1) Ingeniero de Soporte	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** mínimo tres (3) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. **Título de Posgrado:** Especialización o maestría en seguridad informática o ciberseguridad Debe estar Certificado como profesional en seguridad de redes por el fabricante y debe estar vigente Debe acreditar mediante una certificación que cuenta con conocimientos para brindar soluciones de seguridad de redes y debe estar vigente y debe ser emitida por el fabricante. Experiencia específica: Mínimo Dos (2) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad.
Un (1) Especialista en Ciberseguridad:	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** Mínimo cinco (5) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. **Título de Posgrado:** Especialización o maestría en seguridad informática o ciberseguridad Debe acreditar mediante una certificación que cuenta con conocimientos para brindar soluciones de seguridad de redes, debe estar vigente y debe ser emitida por el fabricante. Debe contar con certificación de EH-Ethical Hacker vigente. **Experiencia específica:** Mínimo Dos (2) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad.

FIRMADO EN ORIGINAL

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.

Un (1) Ingeniero de apoyo a la implementación WAF	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática. **Experiencia general:** Mínimo tres (3) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. Debe contar con certificación como Profesional de seguridad en nube emitida por el fabricante. **Experiencia específica:** Mínimo un (1) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad

Documentación para entregar

- Cedula de ciudadanía
- Hoja de vida del profesional
- Diploma de título Profesional
- Tarjeta Profesional con Certificación de vigencia
- Certificaciones que acrediten experiencia especifica
- Certificaciones acreditadas de especialista o maestría en las áreas solicitadas, según aplique.
- Certificaciones técnicas solicitadas en cada uno de los perfiles
- Planilla de seguridad social u otro documento que acredite la vinculación con la empresa interesada en el proceso.

Teniendo en cuenta que el personal propuesto es objeto de verificación dentro de los requisitos habilitantes, las hojas de vida y el personal acreditado por el proponente durante el proceso de selección no podrán ser sustituidos, sin embargo, durante la ejecución del contrato, cuando por razones de fuerza mayor sea necesario solicitar el cambio de un profesional, el contratista deberá presentar la documentación de un profesional que cumpla, como mínimo, con las mismas condiciones y requisitos establecidos para el perfil que se pretende reemplazar.

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.

FIRMADO EN ORIGINAL

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.

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.
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: A más tardar el 20 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 20 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 31 de octubre de 2027, el contratista deberá continuar prestando de forma ininterrumpida, todos los servicios contratados y previstos en las especificaciones técnicas incluyendo 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 correspondiente a 1 año.

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

PONDERABLE

COPIA FIEL DEL ORIGINAL

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.

CALIDAD	PUNTAJE MÁXIMO
PLAN DE MEJORA CONTINUA DE LA POSTURA DE CIBERSEGURIDAD: El plan deberá estar estructurado a partir de una metodología de evaluación de ciberseguridad reconocida, basada en alguno de los siguientes marcos de referencia: NIST Cybersecurity Framework (CSF), ISO/IEC 27001 o CIS Controls, y deberá contemplar como mínimo: 1. Metodología propuesta para realizar la evaluación de la postura actual de ciberseguridad. 2. Análisis de la postura de ciberseguridad y definición iniciativas de fortalecimiento. 3. Propuesta de acciones de mejora orientadas al fortalecimiento de la postura de ciberseguridad. 4. Definición de responsables, recursos y tiempos estimados para la implementación de las acciones. 5. Sesión de seguimiento y actualización del plan de mejora continua antes de finalizar el contrato. **Perfil del profesional que lidera la actividad** Esta actividad debe ser liderada por un profesional con: Título profesional: Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Electrónica, Ingeniería de Software o Ingeniería de Telecomunicaciones. Título de posgrado: Especialización o maestría en áreas relacionadas con Seguridad Informática, Ciberseguridad o Seguridad de la Información. Certificaciones vigentes: Una (1) certificación vigente CEH – Certified Ethical Hacker. Una (1) certificación vigente como Lead Cybersecurity Manager en ISO/IEC 27032. Una (1) certificación vigente como Auditor Líder o Auditor Interno en ISO/IEC 27001:2022.	28

Documentación para entregar

- Cedula de ciudadanía
- Hoja de vida del profesional
- Diploma de título Profesional
- Tarjeta Profesional con Certificación de vigencia
- Certificaciones que acrediten experiencia especifica
- Certificaciones acreditadas de especialista o maestría en las áreas solicitadas, según aplique.
- Certificaciones técnicas solicitadas en cada uno de los perfiles

FIRMADO EN ORIGINAL

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.

- Planilla de seguridad social u otro documento que acredite la vinculación con la empresa interesada en el proceso.

El profesional que cumpla con el perfil descrito en este ítem podrá, a su vez, hacer parte del equipo de profesionales exigido, sin que ello constituya impedimento alguno.

2.3.5 APOYO A LA INDUSTRIA NACIONAL (10 PUNTOS)

Con el fin de establecer el apoyo que los proponentes NACIONALES y EXTRANJEROS otorguen a la industria nacional, en virtud de lo dispuesto en el Artículo 2 de la Ley 816 de 2003, se otorgará el puntaje de la siguiente manera:

- **SERVICIOS DE ORIGEN NACIONAL (10 PUNTOS)**

Se verificará de la siguiente manera:

Persona natural colombiana: Con la presentación de la cédula de ciudadanía del proponente en copia simple, la cual deberá ser aportada con su oferta.

Persona natural extranjera residente en Colombia, con la presentación de la visa correspondiente que le permita la ejecución del objeto contractual de conformidad con la ley. La cual deberá ser aportada con la oferta en copia simple

Persona jurídica constituida en el país, se verificará con el certificado de Cámara y Comercio que el domicilio de la persona jurídica esté dentro del territorio nacional, con expedición no superior a 30 días.

Servicios extranjeros con trato nacional

Se asignará puntaje de los servicios nacionales a aquellos servicios que provengan de otros estados (i) con los cuales exista un acuerdo comercial aplicable al proceso de contratación y (ii) respecto de los cuales exista un trato nacional por reciprocidad.

- **SERVICIOS DE ORIGEN EXTRANJERO CON INCORPORACIÓN DE COMPONENTE COLOMBIANO (5 PUNTOS)**

Se asignará puntaje a aquel proponente que, mediante certificación expedida por el representante legal manifieste bajo gravedad de juramento el origen del personal ofrecido y su compromiso de vinculación a la ejecución del contrato, en caso de resultar adjudicatario del proceso.

Este puntaje se otorgará en el evento en que se presenten proponentes de origen extranjero sin derecho a trato nacional, que ofrezcan servicios profesionales, técnicos u operativos de origen colombiano. Se le otorgará el puntaje de conformidad con la tabla de componente nacional que se establece a continuación:

CRITERIO	PUNTAJE
Profesionales nacionales 100%	3

FIRMADO EN ORIGINAL

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.

Técnicos y tecnólogos nacionales 100%	2
Profesionales y técnicos extranjeros	0

NOTA 1: En el caso que algún profesional o técnico sea extranjero, no se otorgará el puntaje correspondiente.

NOTA 2: En el caso de consorcios o uniones temporales, conformados por participantes nacionales y extranjeros sin derecho a trato nacional, el puntaje se otorgará con la sumatoria del puntaje que obtendría cada uno de sus integrantes en proporción a su porcentaje de participación en la figura asociativa.

Persona natural extranjera residente en Colombia, con la presentación de la visa correspondiente que le permita la ejecución del objeto contractual de conformidad con la ley. La cual deberá ser aportada con la oferta en copia simple.

Persona jurídica constituida en el país, se verificará con el certificado de Cámara y Comercio que el domicilio de la persona jurídica esté dentro del territorio nacional.

Servicios extranjeros con trato nacional

Se asignará puntaje de los servicios nacionales a aquellos servicios que provengan de otros estados (i) con los cuales exista un acuerdo comercial aplicable al proceso de contratación y (ii) respecto de los cuales exista un trato nacional por reciprocidad.

Adicional a lo anterior, para la obtención del puntaje por el factor de Industria Nacional, el proponente Nacional o Extranjero con trato Nacional, deberá presentar el formato 9 debidamente diligenciado y suscrito por la persona natural o representante legal de la persona jurídica o representante legal del proponente plural.

2.3.6 VINCULACIÓN DE PERSONAS CON DISCAPACIDAD

Para la calificación de este aspecto se asignará un puntaje máximo de DOS (2) del valor total de los puntos y se tendrá en cuenta lo establecido en el artículo 2.2.1.2.4.2.7.4. **del Decreto 0287 del 2026,** que regula lo relacionado con la adopción de medidas afirmativas que incentiven la participación en el sistema de compras públicas.

2.3.7 EMPRENDIMIENTOS – EMPRESAS DE MUJERES (DECRETO 1860 DE 2021) – (0,25 PUNTOS)

Para la calificación de este aspecto se asignará un puntaje máximo de PUNTO VEINTICINCO (0.25) del valor total de los puntos y se tendrá en cuenta lo establecido en el artículo 2.2.1.2.4.2.15 del Decreto 1082 de 2015, que regula lo relacionado con la adopción de medidas afirmativas que incentiven la participación de las mujeres en el sistema de compras públicas.

FIRMADO EN ORIGINAL

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 asignará el puntaje asignado a este criterio, únicamente a aquellos oferentes que acrediten alguna de las siguientes condiciones:

No	Condición	Medio de Prueba
1	Cuando más del cincuenta por ciento (50%) de las acciones, partes de interés o cuotas de participación de la persona jurídica (proponente) pertenezcan a mujeres y los derechos de propiedad hayan pertenecido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección.	Esta circunstancia se acreditará mediante certificación expedida por el representante legal y el revisor fiscal del proponente, cuando exista de acuerdo con los requerimientos de ley, o el contador, donde conste la distribución de los derechos en la sociedad y el tiempo en el que las mujeres han mantenido su participación.
2	Cuando por lo menos el cincuenta por ciento (50%) de los empleos del nivel directivo[1] de la persona jurídica sean ejercidos por mujeres y éstas hayan estado vinculadas laboralmente a la empresa durante al menos el último año anterior a la fecha de cierre del Proceso de Selección en el mismo cargo u otro del mismo nivel.	Esta circunstancia se acreditará mediante certificación expedida por el representante legal y el revisor fiscal del proponente, cuando exista de acuerdo con los requerimientos de ley, o el contador, donde se señale de manera detallada todas las personas que conforman los cargos de nivel directivo del proponente, el número de mujeres y el tiempo de vinculación. La certificación deberá relacionar el nombre completo y el número de documento de identidad de cada una de las personas que conforman el nivel directivo del proponente. Además, se deberá allegar como soporte, copia de los respectivos documentos de identidad, copia de los contratos de trabajo o certificación laboral con las funciones, así como el certificado de aportes a seguridad social del último año en el que se demuestren los pagos realizados por el empleador.
3.	Cuando la persona natural sea una mujer y haya ejercido actividades comerciales a través de un establecimiento de comercio durante al menos el último año anterior a la fecha de cierre del proceso de selección.	Esta circunstancia se acreditará mediante la copia de cédula de ciudadanía, la cédula de extranjería o el pasaporte, así como la copia del registro mercantil vigente.
4.	Para las asociaciones y cooperativas, cuando más del cincuenta por ciento (50%) de los asociados sean mujeres y la participación haya correspondido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección.	Esta circunstancia se acreditará mediante certificación expedida por el representante legal.

Las certificaciones de trata el presente artículo deben expedirse bajo la gravedad de juramento con una fecha de máximo treinta (30) días calendario anteriores a la prevista para el cierre del procedimiento de selección.

Para obtener el puntaje previsto en este criterio, en el caso de consorcios y uniones temporales, por lo menos uno de sus integrantes deberá acreditar que (i) es una empresa de mujeres, según alguna de las condiciones antes descritas y que, (ii) tiene una participación igual o superior al diez por ciento (10%) en la figura asociativa.

FIRMADO EN ORIGINAL

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

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.

2.3.8 MIPYMES (DECRETO 1860 DE 2021) – (0,25 PUNTOS).

Para la calificación de este aspecto se asignará un puntaje máximo de PUNTO VEINTICINCO (0.25) del valor total de los puntos y se tendrá en cuenta lo establecido en el artículo 2.2.1.2.4.2.18 del Decreto 1082 de 2015, que regula lo relacionado con la adopción de criterios diferenciales para MiPymes domiciliadas en Colombia.

Para acreditar la condición de MiPymes se verificará lo pertinente, en el certificado del Registro Único de Proponentes de los oferentes. de conformidad con el parágrafo primero del artículo 2.2.1.2.4.2.4. del Decreto 1082 de 2015.

Para obtener el puntaje previsto en este criterio, en el caso de consorcios y uniones temporales, por lo menos uno de sus integrantes deberá acreditar la calidad de MiPymes y tiene una participación igual o superior al diez por ciento (10%) en la figura asociativa.

Nota. Este puntaje se otorgará siempre y cuando la convocatoria pública no haya sido limitada a Mipyme conforme a los artículos 2.2.1.2.4.2.2 y 2.2.1.2.4.2.3 del Decreto 1082 de 2015.

2.3.9. CRITERIOS DE DESEMPATE

En caso de empate en el puntaje total de dos o más ofertas deberán aplicarse las siguientes reglas de acuerdo con cada uno de los numerales, de forma sucesiva y excluyente, para seleccionar al proponente favorecido, respetando en todo caso los compromisos internacionales vigentes:

1. Preferir la oferta de servicios nacionales frente a la oferta de servicios extranjeros. El Proponente acreditará el origen de los servicios con los documentos señalados en la sección 4.4.1. del Pliego de Condiciones. Para el caso de los Proponentes Plurales, todos los integrantes deberán acreditar el origen nacional de la oferta en las condiciones señaladas en la ley.

2. Preferir la propuesta de la mujer cabeza de familia. Su acreditación se realizará en los términos del artículo 1 de la Ley 1232 de 2008, o la norma que lo modifique, aclare, adicione o sustituya, es decir, la condición de mujer cabeza de familia y la cesación de esta se adquirirá desde el momento en que ocurra el respectivo evento y se declare ante un notario. Esta declaración debe tener una fecha de expedición no mayor a treinta (30) días calendarios anteriores a la fecha del cierre del Proceso de Contratación.

Igualmente, se preferirá la propuesta de la mujer víctima de violencia intrafamiliar, la cual acreditará esta condición de conformidad con el artículo 21 de la Ley 1257 de 2008 o la norma que lo modifique, aclare, adicione o sustituya, esto es, cuando se profiera una medida de protección expedida por la autoridad competente. En virtud del artículo 16 de la Ley 1257 de 2008 o la norma que lo modifique, aclare, adicione o sustituya, la medida de protección la debe impartir el comisario de familia del lugar donde ocurrieron los hechos y a falta de este del juez civil

FIRMADO EN ORIGINAL

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.

municipal o promiscuo municipal, o la autoridad indígena en los casos de violencia intrafamiliar en las comunidades de esta naturaleza.

En el caso de las personas jurídicas se preferirá a aquellas en las que participen mayoritariamente mujeres cabeza de familia y/o mujeres víctimas de violencia intrafamiliar, para lo cual el representante legal o el revisor fiscal, según corresponda, diligenciará el Formato 10A – Participación mayoritaria de mujeres cabeza de familia y/o mujeres víctimas de violencia intrafamiliar (persona jurídica), mediante el cual certifica, bajo la gravedad de juramento, que más del cincuenta por ciento (50 %) de la composición accionaria o cuota parte de la persona jurídica está constituida por mujeres cabeza de familia y/o mujeres víctimas de violencia intrafamiliar. Además, deberá acreditar la condición indicada de cada una de las mujeres que participen en la sociedad, aportando los documentos de cada una de ellas, de acuerdo con los dos incisos anteriores.

Finalmente, en el caso de los Proponentes Plurales, se preferirá la oferta cuando cada uno de los integrantes acredite alguna de las condiciones señaladas en los incisos anteriores de este numeral.

Debido a que para el otorgamiento de este criterio de desempate se entregan certificados que contienen datos sensibles, de acuerdo con el artículo 6 de la Ley 1581 de 2012 o la norma que lo modifique, aclare, adicione o sustituya, se requiere que el titular de la información, como es el caso de las mujeres víctimas de violencia intrafamiliar, diligencie el Formato 11 – Autorización para el tratamiento de datos personales como requisito para el otorgamiento del criterio de desempate.

3. Preferir la propuesta presentada por el Proponente que acredite en las condiciones establecidas en la ley que por lo menos el diez por ciento (10 %) de su nómina está en condición de discapacidad, de acuerdo con el artículo 24 de la Ley 361 de 1997 o la norma que lo modifique, aclare, adicione o sustituya, debidamente certificadas por la oficina de trabajo de la respectiva zona, que hayan sido contratados con por lo menos un (1) año de anterioridad a la fecha de cierre del presente Proceso de Contratación o desde el momento de la constitución de la persona jurídica cuando esta es inferior a un (1) año y que manifieste adicionalmente que mantendrá dicho personal por un lapso igual al término de ejecución del contrato, para lo cual deberá diligenciar el Formato 10 B – Vinculación de personas en condición de discapacidad. Para aquellos eventos en los que el diez por ciento (10 %) de la nómina corresponda a un número cuyo primer digito decimal sea 5, 6, 7, 8 o 9 deberá realizarse la aproximación decimal al número entero siguiente.

Si la oferta es presentada por un Consorcio o una Unión Temporal, el integrante del Proponente que acredite que el diez por ciento (10 %) de su nómina está en condición de discapacidad en los términos del presente numeral, debe tener una participación de por lo menos el veinticinco por ciento (25 %) en el Consorcio o en la Unión Temporal y aportar mínimo el veinticinco por ciento (25 %) de la experiencia general habilitante.

FIRMADO EN ORIGINAL

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 tiempo de vinculación en la planta referida de que trata este numeral se acreditará con el certificado de aportes a seguridad social del último año o del tiempo de su constitución cuando su conformación sea inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador.

4. Preferir la propuesta presentada por el oferente que acredite la vinculación en mayor proporción de personas mayores que no sean beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de edad de pensión establecido en la ley, para lo cual la persona natural, el representante legal de la persona jurídica o el revisor fiscal, según corresponda, diligenciará el Formato 10 C – Vinculación de personas mayores y no beneficiarias de la pensión de vejez, familiar o sobrevivencia – (Empleador – proponente), mediante la cual certificará bajo la gravedad de juramento las personas vinculadas en su nómina y el número de trabajadores mayores de edad que no son beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que cumplieron el requisito de edad de pensión. Solo se tendrá en cuenta la vinculación de aquellas personas mayores que se encuentren en las condiciones descritas y que hayan estado vinculadas con una anterioridad igual o mayor a un (1) año contado a partir de la fecha del cierre del Proceso de Contratación. Para los casos de constitución inferior a un (1) año se tendrá en cuenta a aquellos que hayan estado vinculados desde el momento de la constitución de la persona jurídica.

El tiempo de vinculación en la planta referida de que trata el inciso anterior se acreditará con el certificado de aportes a seguridad social del último año o del tiempo de constitución de la persona jurídica en caso de que la constitución sea inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador.

En el caso de los Proponentes Plurales, su representante legal diligenciará el Formato 10 C – Vinculación de personas mayores y no beneficiaria de pensión de vejez, familiar o sobrevivencia – (Empleador – proponente), mediante el cual certifique el número de trabajadores vinculados que siendo personas mayores no beneficiarias de la pensión de vejez, familiar o de sobrevivencia y que cumplieron el requisito de edad de pensión establecido en la ley, de todos los integrantes del Consorcio o de la Unión Temporal. Las personas enunciadas anteriormente podrán estar vinculadas a cualquiera de sus integrantes.

En cualquiera de los dos supuestos anteriores, para el otorgamiento del criterio de desempate cada uno de los trabajadores que cumpla las condiciones previstas por la ley diligenciará el Formato 10 C – Vinculación de personas mayores y no beneficiaria de pensión de vejez, familiar o sobrevivencia (Trabajador), mediante el cual certifica bajo la gravedad de juramento que no es beneficiario de pensión de vejez, familiar o sobrevivencia y cumple la edad de pensión, además, se deberá allegar el documento de identificación del trabajador que lo firma.

La mayor proporción se definirá en relación con el número total de trabajadores vinculados en la planta de personal, por lo que se preferirá al oferente que acredite un porcentaje mayor. En el

FIRMADO EN ORIGINAL

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.

caso de Proponentes Plurales, la mayor proporción se definirá con la sumatoria de trabajadores vinculados en la planta de personal de cada uno de sus integrantes.

5. Preferir la propuesta presentada por el oferente que acredite, en las condiciones establecidas en la Ley 2069 de 2020, que por lo menos el diez por ciento (10 %) de su nómina pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitana, para lo cual, la persona natural, el representante legal o el revisor fiscal, según corresponda, diligenciará el Formato 10D – Vinculación de población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitanas mediante el cual certifica las personas vinculadas a su nómina y el número de identificación y el nombre de las personas que pertenecen a la población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitana. Solo se tendrá en cuenta la vinculación de aquellas personas que hayan estado vinculadas con una anterioridad igual o mayor a un (1) año contado a partir de la fecha del cierre del Proceso de Contratación. Para los casos de constitución inferior a un (1) año, se tendrá en cuenta a aquellos que hayan estado vinculados desde el momento de constitución de la persona jurídica.

El tiempo de vinculación en la planta referida de que trata el inciso anterior se acreditará con el certificado de aportes a seguridad social del último año o del tiempo de su constitución cuando su conformación es inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador.

Además, deberá aportar la copia de la certificación expedida por el Ministerio del Interior en la cual acredite que el trabajador pertenece a la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana en los términos del Decreto Ley 2893 de 2011, o la norma que lo modifique, sustituya o complemente.

En el caso de los Proponentes Plurales, su representante legal diligenciará el Formato 10 D – Vinculación de población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitanas, mediante el cual certifica que por lo menos el diez por ciento (10 %) del total de la nómina de sus integrantes pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o

CAPÍTULO V. RIESGOS ASOCIADOS AL CONTRATO, FORMA DE MITIGARLOS Y ASIGNACIÓN DE RIESGOS

La Matriz 2 – Riesgos incluye los Riesgos que se pueden presentar durante la ejecución del Contrato. Esta Matriz describe cada uno de los Riesgos, la consecuencia de su ocurrencia, a quien se le asigna, cual es el tratamiento en caso de ocurrencia y quién es su responsable, entre otros aspectos.

En caso de que al proponente o a algún integrante del consorcio o unión temporal se le haya impuesto una o más multas o cláusulas penales durante el último año, contado a partir de la fecha prevista para la presentación de las ofertas, sin importar la cuantía, del total de puntaje obtenido, se realizará un descuento correspondiente al dos por ciento (2%).

FIRMADO EN ORIGINAL

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.

Dicha reducción no se aplicará en caso de que los actos administrativos que hayan impuesto las multas sean objeto de medios de control jurisdiccional a través de las acciones previstas en la Ley 1437 de 2011 o las normas que la modifiquen, adicionen o sustituyan; para lo cual el proponente deberá presentar CON LA OFERTA, la demanda debidamente radicada ante la autoridad judicial correspondiente, la cual deberá haberse radicado antes del cierre de presentación de ofertas.

NOTA 1: Para efectos de aplicar lo dispuesto en el artículo 58 de la Ley 2195 de 2022 y parágrafos, las decisiones correspondientes a la imposición de multas o cláusulas penales deben estar en firme e inscritas en el RUP para que sean tenidas en cuenta en el presente proceso de selección, lo anterior de conformidad con lo establecido en el artículo 29 y 83 de la Constitución Política de Colombia, siempre que las mismas se hayan impuesto y publicado después del 18 de enero de 2022.

3. PERSONAL PROFESIONAL Y TÉCNICO REQUERIDO.

Esta documentación será evaluada en la etapa de requisitos habilitantes.

El personal profesional requerido debe estar vinculado con la empresa interesada en el proceso y demostrar su vinculación de mínimo los últimos 3 meses.

El Contratista debe contar con un equipo mínimo de trabajo de 4 integrantes para la ejecución del proyecto, el cual debe estar conformado de la siguiente manera:

ROL	DESCRIPCIÓN
Un (1) Gerente de Proyecto.	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** Debe contar con mínimo diez (10) años de experiencia general, contados a partir de la expedición de la matrícula profesional. **Título de Posgrado en:** Especialización o Maestría en áreas relacionadas con su carrera profesional Debe acreditar mediante una certificación, que tiene fundamentos en ciberseguridad, esta debe ser emitida por el fabricante. Debe acreditar mediante una certificación vigente, conocimientos a nivel profesional en gestión de proyectos.

FIRMADO EN ORIGINAL

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.

	Experiencia específica: Especifica mínima de ocho (8) años gerenciando y/o coordinando proyectos en temas relacionados con seguridad de la información y/o seguridad informática.
Un (1) Ingeniero de Soporte	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** mínimo tres (3) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. **Título de Posgrado:** Especialización o maestría en seguridad informática o ciberseguridad Debe estar Certificado como profesional en seguridad de redes por el fabricante y debe estar vigente Debe acreditar mediante una certificación que cuenta con conocimientos para brindar soluciones de seguridad de redes y debe estar vigente y debe ser emitida por el fabricante. Experiencia específica: Mínimo Dos (2) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad.
Un (1) Especialista en Ciberseguridad:	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática **Experiencia general:** Mínimo cinco (5) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. **Título de Posgrado:** Especialización o maestría en seguridad informática o ciberseguridad Debe acreditar mediante una certificación que cuenta con conocimientos para brindar soluciones de seguridad de redes, debe estar vigente y debe ser emitida por el fabricante. Debe contar con certificación de EH-Ethical Hacker vigente.

FIRMADO EN ORIGINAL

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.

	Experiencia específica: Mínimo Dos (2) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad.
Un (1) Ingeniero de apoyo a la implementación WAF	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática. **Experiencia general:** Mínimo tres (3) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. Debe contar con certificación como Profesional de seguridad en nube emitida por el fabricante. **Experiencia específica:** Mínimo un (1) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad

Documentación para entregar

- Cedula de ciudadanía
- Hoja de vida del profesional
- Diploma de título Profesional
- Tarjeta Profesional con Certificación de vigencia
- Certificaciones que acrediten experiencia especifica
- Certificaciones acreditadas de especialista o maestría en las áreas solicitadas, según aplique.
- Certificaciones técnicas solicitadas en cada uno de los perfiles
- Planilla de seguridad social u otro documento que acredite la vinculación con la empresa interesada en el proceso.

Teniendo en cuenta que el personal propuesto es objeto de verificación dentro de los requisitos habilitantes, las hojas de vida y el personal acreditado por el proponente durante el proceso de selección no podrán ser sustituidos. En consecuencia, en caso de resultar adjudicado, el contratista deberá garantizar que el personal presentado y aprobado durante la etapa de selección sea el mismo que ejecute el proyecto.

4. OBLIGACIONES DEL CONTRATISTA.

4.1. GENERALES:

FIRMADO EN ORIGINAL

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. Realizar las actividades necesarias para el cumplimiento del objeto del contrato a entera satisfacción, así como las demás actividades que relacionadas con el objeto del mismo sean necesarias para lograr los fines buscados.
2. Cumplir con las especificaciones técnicas solicitadas para el desarrollo del contrato.
3. Velar por el cumplimiento del plazo establecido para la ejecución del objeto contractual.
4. Atender las consultas que la Contratante o el Supervisor hagan sobre los servicios prestados.
5. Participar en la elaboración de la liquidación respectiva en el término que se ha establecido, cuando aplique.
6. Mantener vigentes las garantías otorgadas, en caso de que procedan.
7. Cumplir con todas las obligaciones laborales, de Seguridad Social, ARL y el pago de las obligaciones Parafiscales vigentes de los empleados y/o contratistas que utilice en el desarrollo del objeto contractual, y con las obligaciones del Sistema de Gestión de Seguridad y Salud en el Trabajo de conformidad con lo señalado en el Decreto 1072 del 2015.
8. Respetar los buenos usos sociales, la cultura ciudadana y las buenas costumbres en la ejecución contractual.
9. Dar aplicación a los principios de seguridad, confidencialidad, disponibilidad, acceso y circulación restringida respecto de la información y datos a que tenga acceso con ocasión del desarrollo del objeto contractual.

4.2. ESPECÍFICAS:

10. Dentro de los primeros 3 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.
11. 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.
12. 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.
13. El Contratista 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.
14. 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.
15. El Contratista deberá entregar de forma digital, la evidencia de las licencias(s) de la plataforma a nombre del INDER Medellín.

FIRMADO EN ORIGINAL

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.

16. 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.
17. 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.
18. 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.

4.3 OBLIGACIONES ALMBIENTALES: Con base al objeto y los requerimientos técnicos establecidos, no aplican obligaciones ambientales.

5. OBLIGACIONES DEL CONTRATANTE.

1. Designar el personal idóneo para realizar la función de supervisión del contrato para su debida ejecución.
2. Pagar el valor del contrato de acuerdo a la forma de pago estipulada.
3. Facilitar la información y los elementos necesarios para el cabal cumplimiento del objeto del contrato"
4. Hacer efectivas las garantías constituidas por el contratista cuando a ellos hubiere lugar.
5. Verificar el pago de salarios, honorarios, prestaciones sociales, seguridad social integral entre otros, del personal vinculado al contrato por el contratista.
6. Requerir al contratista cuando se presenten situaciones que ameriten adoptar acciones de mejora para el cumplimiento del contrato.
7. Expedir el recibo a satisfacción correspondiente.
8. Las demás que sean necesarias para el efectivo cumplimiento del objeto contractual.

6. PLAZO DE EJECUCIÓN: Desde la firma del acta de inicio hasta el 31 de diciembre de 2026

PARÁGRAFO: 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 la finalizacióni de la vigencia de las licencias, el contratista deberá continuar prestando de forma ininterrumpida, todos los servicios contratados y previstos en las especificaciones técnicas incluyendo garantía, soporte, mantenimiento, disponibilidad, actividades con alcance dentro de la vigencia de las licencias y las demás

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.

COPIA ADOPTADA EN ORIGINAL

obligaciones detalladas en las especificaciones técnicas, obligaciones específicas y garantizando el correcto funcionamiento de la solución durante todo el período de prestación del servicio correspondiente a 1 año.

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

6.2. ACTA DE INICIO: Luego de la publicación del contrato y de cumplidos los demás requisitos de legalización y ejecución del contrato, se procederá a suscribir el acta de iniciación del mismo por parte del supervisor y el contratista.

6.3. SUPERVISIÓN: La supervisión estará a cargo del Subdirector Administrativo y financiero, o quien haga sus veces, quien ejercerá funciones de supervisión y vigilancia técnica, administrativa y financiera del contrato. Es responsabilidad del Supervisor verificar que EL CONTRATISTA haya adecuado sus afiliaciones al Sistema Integral de Seguridad Social en Salud, Pensiones y ARL de conformidad con lo dispuesto en el artículo 23 de la Ley 1150 de 2007.

7. MODALIDAD DE SELECCIÓN DEL CONTRATISTA:

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:

FIRMADO EN ORIGINAL

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.

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

8. VALOR ESTIMADO DEL CONTRATO. El Instituto de Deportes y Recreación –INDER- en cumplimiento de lo establecido en la Ley 80 de 1993, la Ley 1150 de 2007 y el Decreto 1082 de 2015, elaboró un presupuesto oficial de acuerdo con los precios y condiciones del mercado y a las incidencias propias en el desarrollo del proyecto, de igual manera, determinó el presupuesto oficial para este proceso de selección luego de un estudio serio y el análisis detallado.

Conforme a lo anterior, el presupuesto oficial para el presente proceso de selección asciende a **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 con cargo a la siguiente disponibilidad presupuestal:

DISPONIBILIDAD	FECHA CDP	VALOR DISP	POSICIÓN DOCUMENTO	DESCRIPCION POSICIÓN PRESUPUESTAL	CENTRO GESTOR	FONDO
1160015664	22.05.2026	800.589.423 COP	001	2320201004	905924008103	911070126
1160015679	02.06.2026	32.272.427 COP	001	2320201004	905924008103	911070126

AREA FUNCIONAL	PROYECTO	NOMBRE RUBRO PRESUPUESTAL	MONTO RECUERSOS (APRO.INICIAL)	TIPO DE GASTO	ORIGEN DEL PRESUPUESTO
45991000.0254.99	9240081	Fortalecimiento de infraestructura tecnológica	$ 3.273.495.941	Inversión	R. Ordinarios Mpio

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.

45991000.0254.99	9240081	Fortalecimiento de infraestructura tecnológica	$ 3.273.495.941	Inversión	R. Ordinarios Mpio

N°. 4 del Art. 2.2.1.1.2.1.1 del Decreto 1082 de 2015

9. FORMA DE PAGO

El INSTITUTO DE DEPORTES Y RECREACION DE MEDELLIN - INDER MEDELLÍN pagará en un solo contado una vez se dé el cumplimiento de 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 15 de noviembre de 2026.

El pago de la factura estará sujeto a las políticas y las disposiciones de Tesorería y según disponibilidad del Plan Anualizado de Caja- PAC.

La factura deberá ser presentada de forma electrónica, la cual debe cumplir como mínimo, los requisitos de las normas fiscales establecidas en el artículo 616-1 del Estatuto Tributario, o en su defecto la factura de venta presentada en original y con copia, la cual debe cumplir como mínimo, los requisitos de las normas fiscales establecidas en el artículo 617 del Estatuto Tributario. La fecha de la factura debe corresponder al mes de su elaboración, y en ella constará el número del contrato, el concepto del bien o servicio que se está cobrando y el nombre del Supervisor designado o funcionario responsable.

Una vez sea recibido a satisfacción área financiera solicitará una pro forma de la factura, una vez se autorice la pro forma de la factura, el contratista deberá subir la copia a la plataforma de CCE utilizada y enviar el comprobante al área financiera, posteriormente enviar la factura al correo facturacion@inder.gov.co. independientemente al envió de la factura electrónica, se deberán enviar los documentos soporte de la factura, certificado de paz y salvo de seguridad social y parafiscal, copia de la tarjeta profesional del revisor fiscal y certificado de antecedentes disciplinarios expedido por la Junta Central de Contadores no superior a 90 días, o cualquier otro que la supervisión del contrato considere.

El Contratista deberá informar al INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN - INDER, la cuenta bancaria (corriente o de ahorros), abierta a su nombre, en la cual le serán consignados o transferidos electrónicamente, los pagos que, por este concepto, le efectúe el Instituto.

De conformidad con el artículo 23 de la Ley 1150 de 2007, el contratista, deberá acreditar que se encuentra al día en el pago de aportes parafiscales relativos al Sistema de Seguridad Social Integral, así como los propios del SENA, ICBF y Cajas de Compensación Familiar, cuando corresponda. Esta información deberá ser acreditada por el CONTRATISTA para cada pago a

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.

efectuar, situación que deberá ser verificada por el Supervisor del INDER Medellín, pena de incurrir en causal de mala conducta.

Además, deberá acreditar que se encuentra al día en el pago de las obligaciones adquiridas con los proveedores, con quien tenga relación comercial emanada de la ejecución del contrato suscrito con el INDER.

Si el contratista no se encuentra a paz y salvo con el INDER, con la suscripción del contrato, autoriza para que la Tesorería del Instituto, en el momento de un pago, automáticamente y sin previo aviso realice el correspondiente cruce de cuentas, para compensar los valores que tenga en mora por cualquier concepto.

En el evento en que el contratista pretenda hacer cesión de derechos económicos o cualquier otro negocio jurídico financiero que conlleve a que los pagos derivados de la ejecución del contrato se hagan a terceras personas o a un patrimonio autónomo constituido por el contratista, deberá mediar autorización de la Entidad, previa acreditación de encontrarse a paz y salvo con proveedores y subcontratistas con quienes tenga relación comercial emanada de la ejecución del contrato.

Los recursos no ejecutados durante el plazo contractual serán reembolsados administrativamente al rubro y/o rubros respectivos.

Los recursos no ejecutados en la presente vigencia se someterán a las autorizaciones respectivas del consejo distrital de política fiscal CODFIS, para el visto bueno de constitución de reservas presupuestales y por ende los pagos estarán sujetos a la incorporación de estas al presupuesto del Instituto en la siguiente vigencia.

10. CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE. De conformidad con lo establecido en el artículo 5 de la ley 1150 de 2007 y en el artículo 2.2.1.1.2.2.2 del Decreto 1082 de 2015, los factores de selección que permitirán al Instituto de Deportes y Recreación – INDER- identificar la oferta más favorable será el siguiente:

El precio es el factor de selección de la oferta. El INDER debe adjudicar el proceso de contratación al proponente que cumpla con todos los requisitos exigidos en los documentos del proceso y que ofrezca el menor valor.

N°. 5 del Art. 2.2.1.1.2.1.1 del Decreto 1082 de 2015

11. ANÁLISIS DE LOS RIESGOS Y LA FORMA DE MITIGARLOS.

Para efectos del presente capítulo se entenderá las siguientes categorías de riesgo:

FIRMADO

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.

RIESGO PREVISIBLE: Son los posibles hechos o circunstancias que por la naturaleza del contrato y de la actividad a ejecutar es factible su ocurrencia, esta corresponde a la estimación y asignación de los riesgos previsibles, así como su tipificación.

TIPIFICACIÓN DEL RIESGO: Es la enunciación que la entidad hace de aquellos hechos previsibles constitutivos de riesgo que en su criterio pueden presentarse durante y con ocasión de la ejecución del contrato.

ESTIMACIÓN DEL RIESGO: Es la valoración, en términos monetarios o porcentuales respecto del valor del contrato, que hace la entidad de ellos, de acuerdo con la tipificación que ha establecido.

ASIGNACIÓN DEL RIESGO: Es el señalamiento que hace la entidad de la parte contractual que deberá soportar total o parcialmente la ocurrencia de la circunstancia tipificada, asumiendo su costo.

RIESGO IMPREVISIBLE: Son aquellos hechos o circunstancias donde no es factible su previsión, es decir el acontecimiento de su ocurrencia, estos riesgos deberán estar considerados como costo del contrato en el ítem de gastos contingentes.

(***Los principales riesgos previsibles son los que se encuentren consignados en el Anexo Matriz de Riesgos, que hace parte integrante de este documento***)

N°. 6 del Art. 2.2.1.1.2.1.1 del Decreto 1082 de 2015

12. GARANTÍAS.

Una vez analizadas las condiciones generales para la ejecución del contrato producto de este procedimiento de selección, el Instituto de Deportes y Recreación –INDER- determinó que el Proponente favorecido con la adjudicación del contrato constituirá, a favor de la Entidad, una garantía única, otorgada por un banco o una compañía de seguros legalmente establecida en Colombia, o por cualquier mecanismo de cobertura de riesgo tal y como lo contempla el artículo 7 de la Ley 1150 de 2007, y los artículo 2.2.1.2.3.1.1 y s.s del Decreto 1082 de 2015, con los siguientes amparos, cuantías y vigencias:

<table>
<tr><th>CARACTERÍSTICA</th><th>CONDICIÓN</th></tr>
<tr><td>Clase</td><td>Cualquiera de las clases permitidas por el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, a saber: (i) Contrato de seguro contenido en una póliza para Entidades Estatales, (ii) patrimonio autónomo, (iii) Garantía bancaria.</td></tr>
<tr><td>Asegurado/ beneficiario</td><td>INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN – INDER, identificada con el NIT 800.194.096-0.</td></tr>
<tr><td>Amparos, vigencia y valores asegurados</td><td>
<table>
<tr><th>AMPARO</th><th>VIGENCIA</th><th>VALOR ASEGURADO</th></tr>
<tr><td>Cumplimiento general del Contrato y el pago de las multas y la cláusula penal pecuniaria que se le impongan</td><td>Plazo del contrato y (1) un año más</td><td>Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato.</td></tr>
</table>
</td></tr>
</table>

FIRMADO EN ORIGINAL

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.

	Calidad del servicio	Plazo del contrato y un (1) año más.	Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato.	
	Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	Plazo del contrato y tres (3) años más	Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato.	
Tomador	A. Para las personas jurídicas: la Garantía deberá tomarse con el nombre o razón social y tipo societario que figura en el certificado de existencia y representación legal expedido por la cámara de comercio respectiva, y no sólo con su sigla, a no ser que en el referido documento se exprese que la sociedad podrá denominarse de esa manera. B. No se aceptan Garantías a nombre del representante legal o de alguno de los integrantes del Consorcio o de la Unión Temporal. Cuando el Contratista sea una Unión Temporal o Consorcio, se debe incluir el nombre, el NIT y el porcentaje de participación de cada uno de los integrantes. C. Para el Contratista conformado por un Proponente Plural (Unión Temporal o Consorcio): la Garantía deberá ser otorgada por todos los integrantes del Contratista, para lo cual se deberá relacionar claramente los integrantes, su identificación y porcentaje de participación, quienes para todos los efectos serán los otorgantes de esta.			
Información necesaria dentro de la póliza	D. Número y año del Contrato E. Objeto del Contrato F. Firma del representante legal del Contratista G. En caso de no usar centavos, los valores deben aproximarse al mayor Ej. Cumplimiento si el valor a asegurar es $14.980.420,20 aproximar a $14.980.421.			

NOTA 1: La garantía de CUMPLIMIENTO deberá constituirse de la siguiente manera:
Tomador: Contratista;
Asegurado: El contratista y el INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN – INDER.
Beneficiarios: El INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN – INDER.

El Contratista está obligado a restablecer el valor de la Garantía cuando esta se vea reducida por razón de las reclamaciones que efectúe la Entidad, así como, a ampliar las Garantías en los eventos de adición y/o prórroga del Contrato. El no restablecimiento de la Garantía por parte del Contratista o su no adición o prórroga, según el caso, constituye causal de incumplimiento del Contrato y se iniciarán los procesos sancionatorios a que haya lugar.

GARANTÍA DE SERIEDAD:

El Proponente debe incluir en su propuesta, una garantía de seriedad, consistente en póliza de seguro, fiducia mercantil en garantía, garantía bancaria a primer requerimiento, endoso en garantía de títulos valores y depósito de dinero en garantía, con los requisitos exigidos a continuación:

Si se trata de personas naturales o jurídicas extranjeras sin domicilio o sucursal en Colombia podrán otorgar como garantía carta de crédito stand by expedidas en el exterior.

Expedición de la Garantía: La Garantía de Seriedad podrá ser expedida por una compañía de seguros legalmente constituida en Colombia o podrá constar en una garantía bancaria expedida por entidades bancarias legalmente establecidas en Colombia y deberá ser expedida con fecha anterior a la presentación de la oferta.

FIRMADO EL ORIGINAL

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.

Beneficiario de la Garantía: La Garantía de Seriedad debe estar debidamente firmada y establecer como beneficiario al INDER, y al proponente como tomador y afianzado de la misma. Cuando el ofrecimiento sea presentado por un proponente plural bajo la figura de Unión Temporal, Consorcio o Contrato de Asociación Futura, la garantía deberá ser otorgada por todos los integrantes del proponente plural.

Monto de la Garantía: El valor de la garantía será del valor equivalente al diez por ciento (10%) del valor total del presupuesto oficial de la presente contratación, incluido el impuesto al valor agregado IVA, si se causa.

Vigencia de la Garantía: La Garantía de Seriedad deberá tener una vigencia de tres (3) meses, que como mínimo, cubra desde la fecha y hora del cierre del presente proceso y hasta la aprobación de la garantía que ampara los riegos propios de la etapa contractual.

El Proponente deberá ampliar la vigencia de la póliza en el caso de presentarse prórrogas en los plazos de la Selección, de la adjudicación, o de la suscripción del contrato según sea el caso, no cubiertas con la vigencia inicial. La no aceptación de prorrogar la garantía por el término señalado, o el no hacerlo oportunamente, es signo evidente de la voluntad de abandonar el proceso y en consecuencia se rechazará la propuesta, con base en lo establecido en el Artículo 2.2.1.2.3.1.6 del Decreto 1082 de 2015.

Si la oferta es presentada por un proponente plural, como Unión Temporal, Consorcio o promesa de sociedad futura, la garantía debe ser otorgada por todos sus integrantes.

N°. 7 del Art. 2.2.1.1.2.1.1 del Decreto 1082 de 2015.

13. La presente Contratación esta cobijada por un Acuerdo Internacional o un Tratado de Libre Comercio vigente para el Estado Colombiano?

SI _X_ NO ___

¿CUAL? De conformidad con el análisis realizado, el presente proceso de contratación se encuentra cubierto por la Decisión 439 de 1998 de la Secretaría de la CAN.

N°. 8 del Art. 2.2.1.1.2.1.1 del Decreto 1082 de 2015

RESUMEN DEL PROCESO	
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."

FIRMADO EN ORIGINAL

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 OFICIAL	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
PLAZO DE EJECUCIÓN	DESDE LA FIRMA DEL ACTA DE INICIO HASTA EL 31 DE DICIEMBRE DE 2026
COMUNA QUE BENEFICIA	TODAS LAS COMUNAS

Para el efecto Firman,

JORGE ALEJANDRO ANGEL OSORIO
Subdirector Administrativo y Financiero

Maria Alejandra Cañola Estrada Vo. Bo. Financiera	Harrison Alexander Hernández Rúa Vo. Bo. Técnico Sergio Antonio Henao Botero Vo. Bo. Técnico	Ana Maria Aristizabal Salazar Vo. Bo. Jurídica	Alejandro Mesa Giraldo Vo. Bo Ambiental

FIRMADO EN ORIGINAL

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.