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".

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 INTEGRAL DE PROTECCIÓN (XDR, SIEM Y SOC) CON DETECCIÓN Y RESPUESTA DE CIBERSEGURIDAD PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN."**, entendida como un bien tecnológico único, que deberá ser suministrado, licenciado e implementado como un producto completo e indivisible, bajo un modelo de gobernanza centralizada, orientado a garantizar la seguridad de la información, la continuidad de los servicios digitales y la gestión del riesgo tecnológico institucional.

CAPACIDAD OPERATIVA DE LA PLATAFORMA INTEGRAL DE PROTECCIÓN (XDR, SIEM Y SOC)

La plataforma deberá integrar de manera **nativa, coherente y completamente interoperable** capacidades de protección de aplicaciones en sitio y en la nube, de la infraestructura tecnológica, identidades, datos, EndPoints, Servidores Windows y Linux, base de datos, de entornos colaborativos, fuga de información, control de riesgo internos, administración de dispositivos, auditoria de la información y gestión centralizada de eventos e incidentes de seguridad, permitiendo la correlación transversal, la automatización de respuestas y la trazabilidad de todos los eventos de seguridad desde una perspectiva unificada.

En ningún caso se aceptarán ofertas que presenten soluciones aisladas, independientes o no integradas entre sí. Todas las capacidades descritas deberán funcionar de manera articulada, compartiendo información, contexto y mecanismos de respuesta dentro de la misma plataforma integral.

CAPACIDAD OPERATIVA DE LA PLATAFORMA DE DETECCIÓN Y RESPUESTA

Para efectos de planeación contractual, la Entidad informa que actualmente cuenta con cargas operativas y consumos que sirven como referencia mínima para el dimensionamiento de la plataforma; no obstante, será responsabilidad del proponente garantizar que la solución ofertada cuente con una capacidad igual o superior que permita su operación adecuada durante toda la vigencia contractual, cubriendo el futuro crecimiento de la infraestructura.

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 auditoría, análisis forense y trazabilidad del tráfico. Para este propósito, la plataforma deberá soportar, como mínimo, una capacidad equivalente a cinco (5) unidades de procesamiento, doce mil quinientas (12.500) conexiones persistentes simultáneas, un rendimiento sostenido no inferior a once (11) MB/s y una transferencia mensual mínima de dos (2) terabytes de datos.

Adicionalmente, la plataforma integral deberá incluir capacidades centralizadas para la gestión de eventos e incidentes de seguridad, orientadas a la recolección, normalización, análisis y correlación de información proveniente de la infraestructura tecnológica local, en la nube y de los distintos componentes funcionales de la plataforma. Para ello, deberá soportar una ingesta mínima diaria de ocho (8) gigabytes de información, discriminada entre registros analíticos y registros básicos.

La plataforma deberá permitir la retención operativa de la información de seguridad por un periodo mínimo de tres (3) meses, así como el acceso a consultas interactivas, búsquedas programadas y trabajos de análisis masivo, con capacidad de restauración y análisis histórico de eventos, con fines de investigación, auditoría, cumplimiento normativo y respuesta a incidentes.

El requisito técnico sería el siguiente:

#	ARTÍCULO	DESCRIPCIÓN	CANTIDAD	VIGENCIA	MEDIDA
1	PROTECCIÓN ENDPOINTS Y SERVIDORES	**La plataforma debe tener una consola de administración centralizada y en la nube.** **SERVIDORES ON-PREMISES (20)** Protección de servidores de centro de datos con diferentes sistemas operativos: • Windows server 2008 • Windows server 2012 • Windows server 2016 • Windows server 2022 • Linux Ubuntu • CentOS - Debe contar con agente para la instalación en el servidor. -El agente de servidor debe contar con Protección avanzada contra amenazas (Advanced Threat Protection): Detección en tiempo real de actividades anómalas, incluyendo: -Ataques de inyección SQL (SQL injection) (7 instancias de base de datos). -Intentos de acceso por fuerza bruta. -Patrones de acceso inusuales o desde ubicaciones sospechosas. -Exfiltración de datos. **ENDPOINTS (900)** - Protección de equipos de cómputo de usuario final contra malware y ransomware. - Endpoint Detection and Response (EDR). - Gestión de vulnerabilidades y reducción de superficie de ataque. - Supervisión en tiempo real y análisis de amenazas. -Recomendaciones de seguridad por dispositivo. -Configuración de capacidades avanzadas de protección en Endpoints que incluya: -Control de archivos (permitir o bloquear). -Debe permitir habilitar filtrado de contenido web con Creación grupos de dispositivos* -Debe permitir la personalización de directiva de antivirus. -Debe permitir la parametrizar directiva de firewall de Windows. -Debe permitir habilitar protección contra alteraciones. -Debe permitir la administración de dispositivos por medio (live response) * -Informes de estado de antivirus, versiones, estado de ultima conexión y escaneos. - Debe permitir el Bloqueo USB.	1020	12	Unidad

			-Búsqueda avanzada de amenazas. -Monitoreo y alertamiento de vulnerabilidades en los dispositivos con agente instalado. -Gestión de incidentes y alertas por consola. -Protección de red -Bloqueo a primera vista -Protección de próxima generación -Investigaciones automatizadas* -Acciones recomendadas a nivel de alertas -Análisis de amenazas -Inventario de software			
2	**PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS**	**Debe ser compatible con la plataforma de correo de la institución (Microsoft 365)** - Debe contar con Investigación y respuesta (AIR) ante amenazas. -Debe permitir crear directivas de Spam para entrada, salida y filtro de conexión. (Bulk mail - correo masivo no deseado). -Debe detectar y bloquear phishing avanzado y ataques BEC (Business Email Compromise) y protección de identidad (usuarios 365 y Dominio). -Debe permitir la Clasificación de correos en: Bandeja de entrada Correo no deseado (Junk) Cuarentena - Debe realizar análisis de malware en archivos adjuntos (Safe Attachments) -La herramienta debe permitir la validación de enlaces en tiempo real para evitar URLs maliciosas (Safe Links) y proteger archivos y enlaces en: SharePoint OneDrive Microsoft Teams -Debe contar con el uso de inteligencia para detectar amenazas de Zero-Days y Zero-hour auto purge (ZAP). -Debe realizar detección en tiempo real de comportamientos sospechosos. -Debe permitir la generación Reportes en tiempo real de amenazas. -Debe permitir políticas anti-phishing configurables y personalizables. -La herramienta debe estar en la capacidad de simular campañas de phishing (incluido en la herramienta) y entrenar a los usuarios para evitar caer en ataques -Es necesario que la herramienta valide el estado de dominios con: SPF (Sender Policy Framework) DKIM (DomainKeys Identified Mail) DMARC -Bloqueo de remitentes falsificados (spoofing) -Consultas avanzadas de amenazas por medio de consola Advanced Hunting o DataLake.	2300	12	Unidad	

		- Capacidades de monitoreo y trazabilidad en correo electrónico, permitiendo identificar amenazas y ejecutar acciones como eliminación, bloqueo o movimiento de mensajes desde los buzones			
3	**PROTECCIÓN DE LA INFORMACIÓN**	-Prevención de Pérdida de Datos (DLP) en plataformas colaborativas (Correo, OneDrive, SharePoint y Teams) -Etiquetado manual y automático de la Información sensible -Customer Lockbox que permite control total por parte del cliente sobre el acceso de personal del proveedor a los datos, garantizando que cualquier intervención requiera aprobación explícita -Supervisión y control de las comunicaciones internas para asegurar el cumplimiento de normativas organizacionales y regulatorias -Capacidades avanzadas para la búsqueda, recolección, análisis y preservación de información electrónica con fines legales, regulatorios o de auditoría en Datos en plataformas colaborativas (Correo, OneDrive, SharePoint y Teams) - Capacidades para la gestión del ciclo de vida de la información, incluyendo creación, clasificación, almacenamiento, retención y eliminación de datos. - Prevención de Pérdida de Datos (DLP) para EndPoints (100 usuarios) - Registro detallado y extendido de actividades, con capacidades avanzadas de monitoreo, análisis y retención para investigaciones y cumplimiento normativo hasta 10 años (100 usuarios) - Capacidades para detectar y analizar riesgos internos, identificando comportamientos anómalos asociados a fuga o uso indebido de información mediante señales y alertas de seguridad (100 usuarios).	2300	12	Unidad
4	**PROTECCIÓN Y ADMINISTRACION DE IDENTIDADES (IAM)**	- Protección de identidades del directorio local mediante monitoreo de autenticaciones y detección de actividades sospechosas. -Permitir a los usuarios acceder de manera segura a múltiples aplicaciones con una sola autenticación, mejorando la experiencia y reduciendo riesgos asociados a múltiples credenciales -Definición de políticas dinámicas de acceso basadas en condiciones como ubicación, dispositivo, nivel de riesgo o tipo de aplicación, asegurando que solo accesos confiables sean permitidos -Debe ser compatible con los siguientes factores de autenticación (App Authenticator, SMS, Temporary Access Pass, Voice call y/o Email OTP) para reforzar la seguridad en el acceso a recursos críticos. -Capacidades de autenticación sin contraseña mediante métodos biométricos como rostro, huella o PIN, integrados con los dispositivos para fortalecer la seguridad de acceso para sistemas operativos Windows. -Integración entre entornos on-premise y cloud, garantizando consistencia en identidades y accesos -Capacidad para que los usuarios gestionen sus contraseñas de forma autónoma, reduciendo carga operativa en mesa de ayuda -Administración centralizada de usuarios, grupos y asignación de accesos a aplicaciones empresariales -Detección y respuesta automática ante riesgos de identidad, como credenciales comprometidas o comportamientos anómalos, mediante análisis basado en inteligencia	2300	12	Unidad

			-Control y monitoreo de accesos privilegiados, incluyendo asignaciones just-in-time, aprobaciones y auditoría de roles críticos -Validación periódica de permisos y accesos de usuarios para asegurar el principio de mínimo privilegio -Capacidad de evaluar en tiempo real el riesgo asociado a usuarios y sesiones, aplicando controles automáticos -Detección de amenazas en tiempo real mediante análisis e inteligencia de comportamiento -Acciones de corrección para identidades en peligro -Proporciona evaluaciones de la postura de seguridad de identidad y genera recomendaciones prácticas para fortalecer la protección -Identificación de configuraciones y exposiciones de riesgo de las identidades -Monitoreo de intentos de movimiento lateral dentro del entorno de las identidades -Escalado de privilegios y cambios sospechosos de pertenencia a grupos o roles con las identidades			
	5	**ADMINISTRACIÓN DE DISPOSITIVOS (MAM / MDM)**	- Inscripción y configuración de dispositivos corporativos y personales (BYOD), incluyendo portátiles, móviles y tabletas (Windows y Android) (MDM). -Despliegue, actualización y configuración de aplicaciones (ej. Microsoft 365) sin necesidad de gestionar todo el dispositivo (MAM). -Capacidades para la implementación de políticas de seguridad, cumplimiento de directivas y mitigación de amenazas de los dispositivos. -Capacidades de gestión de actualizaciones del sistema operativo y control de versiones. -Capacidad de automatizar tareas de TI y despliegue de políticas. -Capacidades para la administración de aplicaciones corporativas. -Debe permitir borrar información empresarial de forma remota, proteger contra fugas de información y cifrar dispositivos -Capacidades de monitoreo continuo del estado y cumplimiento de los dispositivos. - Capacidades avanzadas para el análisis de riesgo y postura de seguridad de los dispositivos. -Debe garantizar que solo dispositivos seguros y conformes accedan a los datos de la empresa - Capacidades de asistencia y control remoto sobre dispositivos administrados (Windows).	1020	12	Unidad
	6	**PROTECCIÓN DE APLICACIONES EN LA NUBE**	-Capacidad para identificar y analizar el uso de más de 34.000 aplicaciones en la nube dentro de la organización -Clasificación de aplicaciones según su nivel de riesgo, cumplimiento y reputación -Generación de reportes detallados que permitan la toma de decisiones sobre aplicaciones permitidas o bloqueadas	2300	12	Unidad

			-Visibilidad completa sobre las actividades realizadas por los usuarios en aplicaciones cloud -Detección de comportamientos anómalos o sospechosos mediante análisis de patrones de uso -Alertamiento en tiempo real ante actividades de riesgo, como descargas masivas, accesos inusuales o exfiltración de datos. - Supervisión y control de sesiones en tiempo real de cualquier aplicación local y en la nube. - Capacidad de asistencia para DLP para aplicaciones entre SaaS, incluidos Office 365 para proteger datos sensibles en aplicaciones SaaS. - Configuraciones de seguridad para aplicaciones que estén en Azure, AWS y GCP. -Capacidad de integración con SIEM.			
7	**HERRAMIENTA DE DETECCIÓN Y RESPUESTA (SIEM/SOAR)**	**DEBE PERMITIR LA INGESTA DE DATOS DE APLICACIONES CONTRATADAS EN LA ENTIDAD:** • Firewall Fortinet • Antivirus EndPoint • Antispam • WAF • Servicios en Azure (tenant independiente). • Servidores locales y en nube (Azure). • La integración con 2 tenant de Microsoft La herramienta debe tener un motor de correlación con capacidades de: • Detectar comportamientos anómalos • Identificar patrones de ataque conocidos y desconocidos • Correlacionar eventos de múltiples fuentes Lenguaje de consultas avanzado para: • Búsquedas forenses. • Threat hunting (trasversal a todas las herramientas) • Análisis histórico de eventos de seguridad (90 días) Soporte para: • Consultas interactivas desde la herramienta. • Búsquedas programadas personalizables. • Trabajos de búsqueda masivos. Creación de flujos automáticos para: • Enriquecimiento de alertas. • Contención inicial de incidentes. • Flujos de respuesta automatizada. • Notificaciones automáticas • Aislamiento de dispositivos de usuario. • Deshabilitar identidades de Microsoft 365. • Recopilación de paquetes de investigación remota. • Restablecimiento de autenticación de usuario o marcación de usuario comprometido. Reducción del MTTR (Mean Time To Respond).	1	12	Unidad

			Se calculan los requisitos diarios de ingesta de datos: • 5 GB/día de registros analíticos • 3 GB/día de registros básicos • Total: 8 GB diarios Retención operativa de la información: 3 Meses			
8	**WAF (WEB APPLICATION FIREWALL)**	**DEBE SER COMPATIBLE CON SERVICIOS DESPLEGADOS EN MICROSOFT AZURE EN NUBE** La entidad requiere un **Firewall de Aplicaciones Web (WAF)** que proteja aplicaciones expuestas a internet frente a: • Ataques OWASP Top 10 • Explotación de vulnerabilidades web • Tráfico malicioso automatizado • Ataques de denegación de servicio a nivel aplicación • Gestión de bots maliciosos • Reescritura y enmascaramiento de URLs El WAF debe incluir: ○ Reglas administradas basadas en OWASP Core Rule Set ○ Protección contra: ○ Inyección SQL ○ Cross-Site Scripting (XSS) ○ Command Injection ○ Path Traversal ○ Mitigación de ataques DDoS a nivel de aplicación ○ Geobloqueo y control por IP ○ Carga de archivos maliciosos ○ Capacidad de detección y prevención (modo prevención). Arquitectura **Layer 7 (HTTP/HTTPS)**. Soporte para: • Escalabilidad automática. • Balanceo de carga. • Alta disponibilidad. Capacidad mínima equivalente a: • **5 unidades de procesamiento** • **12.500 conexiones persistentes** • **Rendimiento mínimo de 11 MB/s** • **Transferencia mensual de al menos 2 TB** Integración nativa con soluciones SIEM: • Exportación de logs • Alertas de seguridad Capacidad de: • Auditoría de tráfico • Análisis forense o log analitycs • Trazabilidad de eventos Consola centralizada para: • Definición de políticas • Excepciones	1	12	Unidad

		• Reglas personalizadas Capacidad de: • Actualización automática de reglas • Operación sin impacto en producción Generación de reportes: • Ataques bloqueados • Tráfico permitido • Tendencias de riesgo - Integración con SIEM y herramientas de monitoreo - Soporte para HTTPS y certificados			

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

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

La siguiente tabla corresponde a Información filtrada acuerdo software por catálogo

Codigo/SKU	Segmento	Catálogo/Fabricante	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.
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.
NL1-00001EAEASAP	Suite Corporativa	MICROSOFT	Defender Experts Hunt XDR
NL8-00001EAEASAP	Suite Corporativa	MICROSOFT	Defender Experts XDR
NL8-00002EAEASAP	Suite Corporativa	MICROSOFT	Defender Experts XDR
SNI-00001AP	Suite Corporativa	MICROSOFT	Defender Experts Hunt XDR Edu
SNI-00001STU	Suite Corporativa	MICROSOFT	Defender Experts Hunt XDR Edu

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	Tarifa IVA (%)	Valor Unitario IVA	Precio unitario IVA incluido	PRECIO TOTAL
1	PROTECCIÓN ENDPOINTS Y SERVIDORES	1	Unidad	$ 190.000.000,00	0%	$ -	$ 190.000.000,00	$ 190.000.000,00
2	PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS	1	Unidad	$ 165.000.000,00	0%	$ -	$ 165.000.000,00	$ 165.000.000,00
3	PROTECCIÓN DE LA INFORMACIÓN	1	Unidad	$ 80.000.000,00	0%	$ -	$ 80.000.000,00	$ 80.000.000,00
4	PROTECCIÓN Y ADMINISTRACION DE IDENTIDADES (IAM)	1	Unidad	$ 120.000.000,00	0%	$ -	$ 120.000.000,00	$ 120.000.000,00
5	ADMINISTRACIÓN DE DISPOSITIVOS (MAM / MDM)	1	Unidad	$ 174.000.000,00	0%	$ -	$ 174.000.000,00	$ 174.000.000,00
6	PROTECCIÓN DE APLICACIONES EN LA NUBE	1	Unidad	$ 45.000.000,00	0%	$ -	$ 45.000.000,00	$ 45.000.000,00
7	HERRAMIENTA DE DETECCIÓN Y RESPUESTA (SIEM con SOAR)	1	Unidad	$ 60.000.000,00	0%	$ -	$ 60.000.000,00	$ 60.000.000,00
8	WAF (WEB APPLICATION FIREWALL)	1	Unidad	$ 100.000.000,00	0%	$ -	$ 100.000.000,00	$ 100.000.000,00
							Subtotal	$ 934.000.000,00
							IVA	$ -
							TOTAL	$ 934.000.000,00

Razón social	ASF SOLUCIONES S.A.S.
Representante Legal / Documento de identidad	Karen Yuleymi Gallego Diaz C.C. 1.128.386.454
/ NIT	900.617.221-5
Dirección / Teléfono/ Correo electrónico	Carrera 78 A No. 54 - 04 / (4) 3220162 - 3244527018 / licitaciones@asfsoluciones.com

COTIZACIÓN 2

ITEM	ARTICULO	Cantidad	Medida	Valor Unitario Antes de IVA	Tarifa IVA (%)	Valor Unitario IVA	Precio unitario IVA incluido	PRECIO TOTAL
1	PROTECCIÓN ENDPOINTS Y SERVIDORES	1	Unidad	$ 184.921.560,00	0%	$ -	$ 184.921.560,00	$ 184.921.560,00
2	PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS	1	Unidad	$ 154.149.090,00	0%	$ -	$ 154.149.090,00	$ 154.149.090,00
3	PROTECCIÓN DE LA INFORMACIÓN	1	Unidad	$ 43.907.900,00	0%	$ -	$ 43.907.900,00	$ 43.907.900,00
4	PROTECCIÓN Y ADMINISTRACION DE IDENTIDADES (IAM)	1	Unidad	$ 110.067.700,00	0%	$ -	$ 110.067.700,00	$ 110.067.700,00
5	ADMINISTRACIÓN DE DISPOSITIVOS (MAM / MDM)	1	Unidad	$ 174.575.250,00	0%	$ -	$ 174.575.250,00	$ 174.575.250,00
6	PROTECCIÓN DE APLICACIONES EN LA NUBE	1	Unidad	$ 21.953.950,00	0%	$ -	$ 21.953.950,00	$ 21.953.950,00
7	HERRAMIENTA DE DETECCIÓN Y RESPUESTA (SIEM con SOAR)	1	Unidad	$ 53.280.000,00	0%	$ -	$ 53.280.000,00	$ 53.280.000,00
8	WAF (WEB APPLICATION FIREWALL)	1	Unidad	$ 92.401.809,00	0%	$ -	$ 92.401.809,00	$ 92.401.809,00
							Subtotal	$ 835.257.259,00
							IVA	$ -
							TOTAL	$ 835.257.259,00

Razón social	EXPERTOS TECNOLOGICOS SAS
Representante Legal / Documento de Identidad	EDWIN ANDRES MEDINA RUEDA CC 15371998
/ NIT	NIT 900428395-7
Dirección / Telefono/ Correo electronico	Carrera 42 Nº 3 Sur 81 Medellín - info@expertech.com.co

COTIZACIÓN 3

ITEM	ARTICULO	Cantidad	Medida	Valor Unitario Antes de IVA	Tarifa IVA (%)	Valor Unitario IVA	Precio unitario IVA incluido	PRECIO TOTAL
1	PROTECCIÓN ENDPOINTS Y SERVIDORES	1	Unidad	$ 184.800.000,00	0%	$ -	$ 184.800.000,00	$ 184.800.000,00
2	PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS	1	Unidad	$ 154.000.000,00	0%	$ -	$ 154.000.000,00	$ 154.000.000,00
3	PROTECCIÓN DE LA INFORMACIÓN	1	Unidad	$ 49.000.000,00	0%	$ -	$ 49.000.000,00	$ 49.000.000,00
4	PROTECCIÓN Y ADMINISTRACION DE IDENTIDADES (IAM)	1	Unidad	$ 109.000.000,00	0%	$ -	$ 109.000.000,00	$ 109.000.000,00
5	ADMINISTRACIÓN DE DISPOSITIVOS (MAM / MDM)	1	Unidad	$ 174.000.000,00	0%	$ -	$ 174.000.000,00	$ 174.000.000,00
6	PROTECCIÓN DE APLICACIONES EN LA NUBE	1	Unidad	$ 40.000.000,00	0%	$ -	$ 40.000.000,00	$ 40.000.000,00
7	HERRAMIENTA DE DETECCIÓN Y RESPUESTA (SIEM con SOAR)	1	Unidad	$ 53.200.000,00	0%	$ -	$ 53.200.000,00	$ 53.200.000,00
8	WAF (WEB APPLICATION FIREWALL)	1	Unidad	$ 92.000.000,00	0%	$ -	$ 92.000.000,00	$ 92.000.000,00
							Subtotal	$ 856.000.000,00
							IVA	$ -
							TOTAL	$ 856.000.000,00

Razón social	DMR SOFTWARE Y TECNOLOGIA S.A.S
Representante Legal / Documento de Identidad	43.976.730
/ NIT	900.956.402-5
Dirección / Telefono/ Correo electronico	CRA 42 3 SUR 81 - 3002793634 - morozco@dmrqi.com

Con las cotizaciones obtenidas en las respuestas de los proveedores evidenciamos que si existen empresas en el mercado que pueden proveer el servicio descrito en las especificaciones técnicas 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 INTEGRAL DE PROTECCIÓN (XDR, SIEM Y SOC) CON DETECCIÓN Y RESPUESTA DE CIBERSEGURIDAD PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN."**

ALCANCE: suministrar, implementar y poner en operación una solución integral de ciberseguridad para el INDER Medellín, bajo un esquema de servicios administrados y/o en la nube, que incluya el aprovisionamiento, configuración y aseguramiento de servidores virtuales, servicios en la nube, almacenamiento, conectividad y demás componentes tecnológicos requeridos para su funcionamiento, garantizando condiciones adecuadas de seguridad, disponibilidad, escalabilidad y desempeño, licencias, suscripciones, componentes y servicios necesarios para la operación de la solución, debidamente legalizados y registrados a nombre del INDER Medellín, soporte y actualización durante el plazo contractual, ejecutar actividades de instalación, configuración, parametrización, hardening, integración, pruebas funcionales, ajustes técnicos y puesta en funcionamiento de la solución, de manera que esta quede completamente operativa y a satisfacción del supervisor designado, realizar pruebas técnicas, simulacros y ejercicios controlados de validación para verificar el correcto funcionamiento de la solución y su capacidad de detección, análisis y respuesta frente a eventos e incidentes de seguridad, brindar capacitación técnica y funcional al personal designado por el INDER Medellín para la administración, monitoreo y operación de la solución, incluyendo actividades de transferencia de conocimiento, entrega de documentación técnica y adopción de buenas prácticas, garantizar soporte técnico especializado, atención de incidentes, diagnóstico, escalamiento, resolución de fallas, acompañamiento técnico y funcional en la operación, monitoreo continuo, ajuste de configuraciones, afinamiento de reglas, recomendaciones de mejora y apoyo en la gestión de eventos e incidentes de seguridad, asegurar la actualización permanente de firmas, motores, parches, versiones, políticas y demás componentes de la solución, con el fin de mantener su estabilidad, efectividad y protección frente a amenazas emergentes, generar y entregar informes periódicos al supervisor del contrato sobre el estado general de la seguridad, la disponibilidad de la solución, los eventos e incidentes detectados, los análisis realizados, las acciones de mitigación implementadas, los indicadores de gestión, las recomendaciones y las oportunidades de mejora, garantizando en todo momento el correcto funcionamiento, estabilidad, continuidad y disponibilidad de la solución integral de ciberseguridad durante toda la vigencia contractual.

2.1. ESPECIFICACIONES: A continuación, se describen las especificaciones técnicas por cada uno de los ítems requeridos en el presente proceso contractual:

La Entidad requiere la provisión de un **SISTEMA INTEGRAL DE PROTECCIÓN (XDR, SIEM Y SOC) CON DETECCIÓN Y RESPUESTA DE CIBERSEGURIDAD**, entendida como un bien tecnológico único, que deberá ser suministrado, licenciado e implementado como un producto completo e indivisible, bajo un modelo de gobernanza centralizada, orientado a garantizar la seguridad de la información, la continuidad de los servicios digitales y la gestión del riesgo tecnológico institucional.

CAPACIDAD OPERATIVA DE LA PLATAFORMA INTEGRAL DE PROTECCIÓN (XDR, SIEM Y SOC)

La plataforma deberá integrar de manera **nativa, coherente y completamente interoperable** capacidades de protección de aplicaciones on premises y en la nube, de la infraestructura tecnológica, identidades, datos, EndPoints, Servidores Windows y Linux, base de datos, de entornos colaborativos, fuga de información, control de riesgo internos, administración de dispositivos, auditoria de la información y gestión centralizada de eventos e incidentes de seguridad, permitiendo la correlación transversal, la automatización de respuestas y la trazabilidad de todos los eventos de seguridad desde una perspectiva unificada.

En ningún caso se aceptarán ofertas que presenten soluciones aisladas, independientes o no integradas entre sí. Todas las capacidades descritas deberán funcionar de manera articulada, compartiendo información, contexto y mecanismos de respuesta dentro de la misma plataforma integral.

CAPACIDAD OPERATIVA DE LA PLATAFORMA DE DETECCIÓN Y RESPUESTA

Para efectos de planeación contractual, la Entidad informa que actualmente cuenta con cargas operativas y consumos que sirven como referencia mínima para el dimensionamiento de la plataforma; no obstante, será responsabilidad del proponente garantizar que la solución ofertada cuente con una capacidad igual o superior que permita su operación adecuada durante toda la vigencia contractual, soportando el crecimiento futuro de la infraestructura.

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 auditoría, análisis forense y trazabilidad del tráfico. Para este propósito, la plataforma deberá soportar, como mínimo, una capacidad equivalente a cinco (5) unidades de procesamiento, doce mil quinientas (12.500) conexiones persistentes simultáneas, un rendimiento sostenido no inferior a once (11) MB/s y una transferencia mensual mínima de dos (2) terabytes de datos.

Adicionalmente, la plataforma integral deberá incluir capacidades centralizadas para la gestión de eventos e incidentes de seguridad, orientadas a la recolección, normalización, análisis y

correlación de información proveniente de la infraestructura tecnológica local, en la nube y de los distintos componentes funcionales de la plataforma. Para ello, deberá soportar una ingesta mínima diaria de ocho (8) gigabytes de información, discriminada entre registros analíticos y registros básicos.

La plataforma deberá permitir la retención operativa de la información de seguridad por un periodo mínimo de tres (3) meses, así como el acceso a consultas interactivas, búsquedas programadas y trabajos de análisis masivo, con capacidad de restauración y análisis histórico de eventos, con fines de investigación, auditoría, cumplimiento normativo y respuesta a incidentes.

REQUISITOS

- Todos los componentes deber ser del mismo fabricante.
- La vigencia de la solución de seguridad debe iniciar a partir del 1 de noviembre de 2026 por 12 meses.
- Las licencias de la plataforma de seguridad deben ser en la última versión publicada por el fabricante y deben quedar a nombre del INDER Medellín.
- La plataforma de seguridad debe contar con acceso a actualizaciones periódicas para la protección contra nuevas amenazas.
- La garantía comercial 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 y telefónica 24/7 o en horario hábil, Gestión y solución de incidentes técnicos, Asistencia para configuración y despliegue, Guías técnicas, manuales y base de conocimientos, SLA (acuerdo de nivel de servicio), asistencia e implementación de mejoras ante nuevas vulnerabilidades.
    - Acompañamiento postventa: Validación con periodicidad 15 días sobre el funcionamiento de la plataforma (Despliegue de agentes, superficie de vulnerabilidad, aplicar correcciones, informe de diagnóstico). Informe estadístico mensual.
    - Capacitación inicial sobre uso del producto mínimo 30 horas: Entrenamiento para administradores o equipos técnicos, Sesiones de transferencia de conocimiento, Documentación de mejores prácticas.
    - Recuperación de contraseñas en caso de pérdida: Reinstalación sin costo adicional dentro del periodo de garantía, migración de consola de administración en caso de que aplique.

- **La solución de seguridad debe cumplir con las siguientes capacidades técnicas:**

#	ARTÍCULO	DESCRIPCIÓN	CANTIDAD	VIGENCIA MESES	MEDIDA
1	PROTECCIÓN ENDPOINTS Y SERVIDORES	**La plataforma debe tener una consola de administración centralizada y en la nube.** **SERVIDORES ON-PREMISES (20)** Protección de servidores de centro de datos con diferentes sistemas operativos: • Windows server 2008 • Windows server 2012 • Windows server 2016 • Windows server 2022 • • Linux Ubuntu • CentOS - Debe contar con agente para la instalación en el servidor. -El agente de servidor debe contar con Protección avanzada contra amenazas (Advanced Threat Protection): Detección en tiempo real de actividades anómalas, incluyendo: -Ataques de inyección SQL (SQL injection) (7 instancias de base de datos). -Intentos de acceso por fuerza bruta. -Patrones de acceso inusuales o desde ubicaciones sospechosas. -Exfiltración de datos. **ENDPOINTS (900)** - Protección de equipos de cómputo de usuario final contra malware y ransomware. - Endpoint Detection and Response (EDR). - Gestión de vulnerabilidades y reducción de superficie de ataque. - Supervisión en tiempo real y análisis de amenazas. -Recomendaciones de seguridad por dispositivo. -Configuración de capacidades avanzadas de protección en Endpoints que incluya: -Control de archivos (permitir o bloquear). -Debe permitir habilitar filtrado de contenido web con Creación grupos de dispositivos* -Debe permitir la personalización de directiva de antivirus. -Debe permitir la parametrizar directiva de firewall de Windows. -Debe permitir habilitar protección contra alteraciones. -Debe permitir la administración de dispositivos por medio (live response) * -Informes de estado de antivirus, versiones, estado de ultima conexión y escaneos. - Debe permitir el Bloqueo USB. -Búsqueda avanzada de amenazas. -Monitoreo y alertamiento de vulnerabilidades en los dispositivos con agente instalado.	1020	12	Unidad

			-Gestión de incidentes y alertas por consola. -Protección de red -Bloqueo a primera vista -Protección de próxima generación -Investigaciones automatizadas* -Acciones recomendadas a nivel de alertas -Análisis de amenazas -Inventario de software			
	2	**PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS**	**Debe ser compatible con la plataforma de correo de la institución (Microsoft 365)** - Debe contar con Investigación y respuesta (AIR) ante amenazas. -Debe permitir crear directivas de Spam para entrada, salida y filtro de conexión. (Bulk mail - correo masivo no deseado). -Debe detectar y bloquear phishing avanzado y ataques BEC (Business Email Compromise) y protección de identidad (usuarios 365 y Dominio). -Debe permitir la Clasificación de correos en: Bandeja de entrada Correo no deseado (Junk) Cuarentena - Debe realizar análisis de malware en archivos adjuntos (Safe Attachments) -La herramienta debe permitir la validación de enlaces en tiempo real para evitar URLs maliciosas (Safe Links) y proteger archivos y enlaces en: SharePoint OneDrive Microsoft Teams -Debe contar con el uso de inteligencia para detectar amenazas de Zero-Days y Zero-hour auto purge (ZAP). -Debe realizar detección en tiempo real de comportamientos sospechosos. -Debe permitir la generación Reportes en tiempo real de amenazas. -Debe permitir políticas anti-phishing configurables y personalizables. -La herramienta debe estar en la capacidad de simular campañas de phishing (incluido en la herramienta) y entrenar a los usuarios para evitar caer en ataques -Es necesario que la herramienta valide el estado de dominios con: SPF (Sender Policy Framework) DKIM (DomainKeys Identified Mail) DMARC -Bloqueo de remitentes falsificados (spoofing) -Consultas avanzadas de amenazas por medio de consola Advanced Hunting o DataLake. - Capacidades de monitoreo y trazabilidad en correo electrónico, permitiendo identificar amenazas y ejecutar acciones como eliminación, bloqueo o movimiento de mensajes desde los buzones	2300	12	Unidad

3	PROTECCIÓN DE LA INFORMACIÓN	-Prevención de Pérdida de Datos (DLP) en plataformas colaborativas (Correo, OneDrive, SharePoint y Teams) -Etiquetado manual y automático de la Información sensible -Customer Lockbox que permite control total por parte del cliente sobre el acceso de personal del proveedor a los datos, garantizando que cualquier intervención requiera aprobación explícita -Supervisión y control de las comunicaciones internas para asegurar el cumplimiento de normativas organizacionales y regulatorias -Capacidades avanzadas para la búsqueda, recolección, análisis y preservación de información electrónica con fines legales, regulatorios o de auditoría en Datos en plataformas colaborativas (Correo, OneDrive, SharePoint y Teams) - Capacidades para la gestión del ciclo de vida de la información, incluyendo creación, clasificación, almacenamiento, retención y eliminación de datos. - Prevención de Pérdida de Datos (DLP) para EndPoints (100 usuarios) - Registro detallado y extendido de actividades, con capacidades avanzadas de monitoreo, análisis y retención para investigaciones y cumplimiento normativo hasta 10 años (100 usuarios) - Capacidades para detectar y analizar riesgos internos, identificando comportamientos anómalos asociados a fuga o uso indebido de información mediante señales y alertas de seguridad (100 usuarios).	2300	12	Unidad	
4	PROTECCIÓN Y ADMINISTRACION DE IDENTIDADES (IAM)	- Protección de identidades del directorio local mediante monitoreo de autenticaciones y detección de actividades sospechosas. -Permitir a los usuarios acceder de manera segura a múltiples aplicaciones con una sola autenticación, mejorando la experiencia y reduciendo riesgos asociados a múltiples credenciales -Definición de políticas dinámicas de acceso basadas en condiciones como ubicación, dispositivo, nivel de riesgo o tipo de aplicación, asegurando que solo accesos confiables sean permitidos -Debe ser compatible con los siguientes factores de autenticación (App Authenticator, SMS, Temporary Access Pass, Voice call y/o Email OTP) para reforzar la seguridad en el acceso a recursos críticos. -Capacidades de autenticación sin contraseña mediante métodos biométricos como rostro, huella o PIN, integrados con los dispositivos para fortalecer la seguridad de acceso para sistemas operativos Windows. -Integración entre entornos on-premise y cloud, garantizando consistencia en identidades y accesos -Capacidad para que los usuarios gestionen sus contraseñas de forma autónoma, reduciendo carga operativa en mesa de ayuda -Administración centralizada de usuarios, grupos y asignación de accesos a aplicaciones empresariales -Detección y respuesta automática ante riesgos de identidad, como credenciales comprometidas o comportamientos anómalos, mediante análisis basado en inteligencia -Control y monitoreo de accesos privilegiados, incluyendo asignaciones just-in-time, aprobaciones y auditoría de roles críticos -Validación periódica de permisos y accesos de usuarios para asegurar el principio de mínimo privilegio	2300	12	Unidad	

			-Capacidad de evaluar en tiempo real el riesgo asociado a usuarios y sesiones, aplicando controles automáticos -Detección de amenazas en tiempo real mediante análisis e inteligencia de comportamiento -Acciones de corrección para identidades en peligro -Proporciona evaluaciones de la postura de seguridad de identidad y genera recomendaciones prácticas para fortalecer la protección -Identificación de configuraciones y exposiciones de riesgo de las identidades -Monitoreo de intentos de movimiento lateral dentro del entorno de las identidades -Escalado de privilegios y cambios sospechosos de pertenencia a grupos o roles con las identidades			
	5	**ADMINISTRACIÓN DE DISPOSITIVOS (MAM / MDM)**	- Inscripción y configuración de dispositivos corporativos y personales (BYOD), incluyendo portátiles, móviles y tabletas (Windows y Android) (MDM). -Despliegue, actualización y configuración de aplicaciones (ej. Microsoft 365) sin necesidad de gestionar todo el dispositivo (MAM). -Capacidades para la implementación de políticas de seguridad, cumplimiento de directivas y mitigación de amenazas de los dispositivos. -Capacidades de gestión de actualizaciones del sistema operativo y control de versiones. -Capacidad de automatizar tareas de TI y despliegue de políticas. -Capacidades para la administración de aplicaciones corporativas. -Debe permitir borrar información empresarial de forma remota, proteger contra fugas de información y cifrar dispositivos -Capacidades de monitoreo continuo del estado y cumplimiento de los dispositivos. - Capacidades avanzadas para el análisis de riesgo y postura de seguridad de los dispositivos. -Debe garantizar que solo dispositivos seguros y conformes accedan a los datos de la empresa - Capacidades de asistencia y control remoto sobre dispositivos administrados (Windows).	1020	12	Unidad
	6	**PROTECCIÓN DE APLICACIONES EN LA NUBE**	-Capacidad para identificar y analizar el uso de más de 34.000 aplicaciones en la nube dentro de la organización -Clasificación de aplicaciones según su nivel de riesgo, cumplimiento y reputación -Generación de reportes detallados que permitan la toma de decisiones sobre aplicaciones permitidas o bloqueadas -Visibilidad completa sobre las actividades realizadas por los usuarios en aplicaciones cloud -Detección de comportamientos anómalos o sospechosos mediante análisis de patrones de uso	2300	12	Unidad

			-Alertamiento en tiempo real ante actividades de riesgo, como descargas masivas, accesos inusuales o exfiltración de datos. - Supervisión y control de sesiones en tiempo real de cualquier aplicación local y en la nube. - Capacidad de asistencia para DLP para aplicaciones entre SaaS, incluidos Office 365 para proteger datos sensibles en aplicaciones SaaS. - Configuraciones de seguridad para aplicaciones que estén en Azure, AWS y GCP. -Capacidad de integración con SIEM.				
	7	**HERRAMIENTA DE DETECCIÓN Y RESPUESTA (SIEM/SOAR)**	**DEBE PERMITIR LA INGESTA DE DATOS DE APLICACIONES CONTRATADAS EN LA ENTIDAD:** • Firewall Fortinet • Antivirus EndPoint • Antispam • WAF • Servicios en Azure (tenant independiente). • Servidores locales y en nube (Azure). • La integración con 2 tenant de Microsoft La herramienta debe tener un motor de correlación con capacidades de: • Detectar comportamientos anómalos • Identificar patrones de ataque conocidos y desconocidos • Correlacionar eventos de múltiples fuentes Lenguaje de consultas avanzado para: • Búsquedas forenses. • Threat hunting (trasversal a todas las herramientas) • Análisis histórico de eventos de seguridad (90 días) Soporte para: • Consultas interactivas desde la herramienta. • Búsquedas programadas personalizables. • Trabajos de búsqueda masivos. Creación de flujos automáticos para: • Enriquecimiento de alertas. • Contención inicial de incidentes. • Flujos de respuesta automatizada. • Notificaciones automáticas • Aislamiento de dispositivos de usuario. • Deshabilitar identidades de Microsoft 365. • Recopilación de paquetes de investigación remota. • Restablecimiento de autenticación de usuario o marcación de usuario comprometido. Reducción del MTTR (Mean Time To Respond). Se calculan los requisitos diarios de ingesta de datos: • 5 GB/día de registros analíticos • 3 GB/día de registros básicos • Total: 8 GB diarios	1	12	Unidad	

		Retención operativa de la información: 3 Meses				
8	**WAF (WEB APPLICATION FIREWALL)**	**DEBE SER COMPATIBLE CON SERVICIOS DESPLEGADOS EN MICROSOFT AZURE EN NUBE** La entidad requiere un **Firewall de Aplicaciones Web (WAF)** que proteja aplicaciones expuestas a internet frente a: • Ataques OWASP Top 10 • Explotación de vulnerabilidades web • Tráfico malicioso automatizado • Ataques de denegación de servicio a nivel aplicación • Gestión de bots maliciosos • Reescritura y enmascaramiento de URLs El WAF debe incluir: O Reglas administradas basadas en OWASP Core Rule Set O Protección contra: O Inyección SQL O Cross-Site Scripting (XSS) O Command Injection O Path Traversal O Mitigación de ataques DDoS a nivel de aplicación O Geobloqueo y control por IP O Carga de archivos maliciosos O Capacidad de detección y prevención (modo prevención). Arquitectura **Layer 7 (HTTP/HTTPS).** Soporte para: • Escalabilidad automática. • Balanceo de carga. • Alta disponibilidad. Capacidad mínima equivalente a: • **5 unidades de procesamiento** • **12.500 conexiones persistentes** • **Rendimiento mínimo de 11 MB/s** • **Transferencia mensual de al menos 2 TB** Integración nativa con soluciones SIEM: • Exportación de logs • Alertas de seguridad Capacidad de: • Auditoría de tráfico • Análisis forense o log analitycs • Trazabilidad de eventos Consola centralizada para: • Definición de políticas • Excepciones • Reglas personalizadas Capacidad de: • Actualización automática de reglas	1	12	Unidad	

		• Operación sin impacto en producción Generación de reportes: • Ataques bloqueados • Tráfico permitido • Tendencias de riesgo - Integración con SIEM y herramientas de monitoreo - Soporte para HTTPS y certificados			

La vigencia debe iniciar en las siguientes fechas: Todo el sistema de seguridad debe iniciar vigencias desde el 1 de noviembre de 2026 y por 12 meses.

El contratista deberá prever el crecimiento de la infraestructura para garantizar la continuidad de la seguridad, si fuere necesario.

ACTIVIDADES A EJECUTAR POR EL CONTRATISTA:

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 (pruebas de penetración y de ataques) 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. Tramitar EARLY BILLING con el fabricante si aplica.
3. Realizar la configuración y el despliegue de la PLATAFORMA INTEGRAL DE PROTECCIÓN (XDR, SIEM Y SOC) CON DETECCIÓN Y RESPUESTA DE CIBERSEGURIDAD en toda la infraestructura de la entidad.
4. Alinear la solución de seguridad según las políticas de ciberseguridad del INDER Medellín.
5. Capacitar el personal técnico (3 Usuarios) del INDER Medellín en la administración de la PLATAFORMA INTEGRAL DE PROTECCIÓN (XDR, SIEM Y SOC) CON DETECCIÓN Y RESPUESTA DE CIBERSEGURIDAD.
6. Envió de campañas de Phishing y entrenamiento a usuarios final por medio de la solución por lo menos 2 veces al año.

7. Realización de una prueba de acceso no autorizado (pentesting), una evaluación de seguridad tipo Ethical hacking, y una capacitación virtual sobre concienciación en ciberseguridad para usuarios finales durante la vigencia del contrato.

8. Debe incluir un servicio de Security Operations Center (SOC) que incluya capacidades de atención en (horario 5x8) donde se ejecute el análisis y la correlación de eventos provenientes de identidades, endpoints, servidores, sistemas operativos, aplicaciones y dispositivos de red/seguridad. Debe incluir la gestión y clasificación de alertas e incidentes (Crítico/Alto/Medio/Bajo), la apertura y gestión de tickets, respuesta inicial (análisis, evaluación de impacto y alcance, activación de playbooks y recomendaciones inmediatas de contención), y la coordinación con el equipo de TI del INDER para ejecutar acciones correctivas conforme al SLA contratado.

9. Las demás que la entidad determine para el correcto desarrollo del objeto contractual.

REQUISITOS TÉCNICOS HABILITANTES:

Con la finalidad de asegurar que los oferentes analizaron los requisitos técnicos y entendieron la necesidad técnica del INDER Medellín deberá entregar como requisito habilitante:

1. Un modelo gráfico detallado de la arquitectura propuesta para la implementación de la plataforma XDR, incluyendo sus componentes SIEM / SOAR, en el que se identifiquen las superficies y fuentes de datos a proteger y monitorear, los productos y fabricantes involucrados, y las integraciones previstas. El diagrama deberá evidenciar la interoperabilidad nativa de la solución, así como el esquema de gestión y administración centralizada.

2. Una carta firmada por el representante legal en la cual indique que, en su calidad de oferente analizó y entendió todos los requisitos técnicos, obligaciones específicas, compromisos, activades de implementación, garantía y acompañamiento postventa indicado en el proceso.

2.2. AUTORIZACIONES: No aplica

2.3. PERMISOS Y LICENCIAS: No aplica

2.4. DISEÑOS: No aplica

2.5. 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 tres (03) certificados de contratos ejecutados, terminados y liquidados por el proponente, que el valor sumado de los contratos ejecutados expresados en salarios mínimos mensuales legales vigentes (SMMLV) sea igual o superior el valor total del presupuesto oficial estimado para la presente contratación expresado en (SMMLV), es decir, VALOR DEL PRESUPUESTO DIVIDO EN SMMLV (475,6), y corresponder como mínimo tres (3) de los siguientes códigos del Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC), así:

Tipo	Código	Nombre Producto
Clase	43233200	Software de seguridad y protección
Clase	81111800	Servicios de Sistemas y administración de componentes
Clase	81111500	Ingenieria de Software o Hardware
Clase	43233700	Software de administración de sistemas
Clase	43233500	Software de intercambio de información

Dichos contratos deben encontrarse en el RUP del proponente y debe relacionarlos en el Formato 3 de Experiencia del Proponente. Deberá presentar ambos documentos con la oferta (RUP y Formato 3).

CONDICIONES GENERALES DE EXPERIENCIA

Las certificaciones, acta de liquidación o recibido a satisfacción aportadas (ya sea por contratos suscritos con entidades estatales, o contratos suscritos entre particulares) deberán cumplir con los siguientes requisitos:

a. Fecha de expedición
b. Razón social del contratante con Nit
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. Fecha de expedición.
h. Objeto del contrato (Debe tener relación con prestación de servicios de seguridad informática y ciberseguridad).
i. Funcionario competente que expide la certificación.

La Entidad se reserva el derecho de verificar las certificaciones aportadas o de solicitar los respectivos documentos que soporten la certificación

2.6 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 2.2.1.1.2.2.1 del Decreto 1082 de 2015, los factores de selección que permitirán al Instituto de Deportes y Recreación de Medellín –INDER- identificar la oferta más favorable serán los siguientes criterios:

CRITERIO	PUNTAJE MÁXIMO
VALOR DE LA PROPUESTA	59,5
FACTOR DE CALIDAD	28
ESTIMULO A LA INDUSTRIA NACIONAL	10
PUNTAJE ADICIONAL PARA EMPLEADORES DE PERSONAS CON DISCAPACIDAD Y PARA EMPRENDIMIENTOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD	2
PUNTAJE ADICIONAL PARA EMPRENDIMIENTOS Y EMPRESAS DE MUJERES (0.25%)	0,25
PUNTAJE ADICIONAL PARA MIPYME EN EL SISTEMA DE COMPRAS PÚBLICAS (0.25%)	0,25
TOTAL	100

2.6.1 VALOR DE LA PROPUESTA

Se asignará el mayor puntaje a la propuesta de menor precio y de forma proporcional a los demás oferentes, de conformidad con la fórmula que se detalla más abajo, para lo cual, el oferente consignará su oferta en el anexo respectivo publicado por la entidad.

El valor que se tomará para efectos de la evaluación, será el corregido por la entidad, si hubo lugar a ello.

PE = 59,5*(Vm /VE)

PE: Puntos del proponente evaluado.

Vm: Valor menor ofertado.

VE: Valor del proponente a evaluar.

Los precios ofrecidos serán fijos no reajustables y deberán ser en cifras enteras sin decimales, en moneda colombiana, para toda la vigencia del contrato.

2.6.2 CORRECCIONES ARITMÉTICAS

La Entidad solo efectuará correcciones aritméticas originadas por:

A. Las operaciones aritméticas a que haya lugar en la propuesta económica, cuando exista un error que surja de un cálculo meramente aritmético cuando la operación ha sido erróneamente realizada.

B. El ajuste al Peso ya sea por exceso o por defecto de los Precios Unitarios contenidos en la propuesta económica de las operaciones aritméticas a que haya lugar y del valor del IVA, así: cuando la fracción decimal del Peso sea igual o superior a punto cinco (0.5) se aproximará por exceso al número entero siguiente del Peso y cuando la fracción decimal del Peso sea inferior a punto cinco (0.5) se aproximará por defecto al número entero.

2.6.3 PRECIO ARTIFICIALMENTE BAJO

En el evento en el que el precio de una oferta, al momento de su evaluación, no parezca suficiente para garantizar una correcta ejecución del Contrato, de acuerdo con la información recogida durante la etapa de planeación y particularmente en el estudio del sector, la Entidad podrá acudir a los parámetros definidos en la Guía para el manejo de ofertas artificialmente bajas en Procesos de Contratación de Colombia Compra Eficiente, como un criterio metodológico.

2.6.4 FACTOR DE CALIDAD

Se otorgará puntaje al proponente que ofrezca para la solución, configuración y puesta en funcionamiento de la solución, lo siguiente:

CERTIFICACIONES	PUNTAJE
Presentar un (1) profesional por cada rol del personal técnico	10 puntos
Pruebas de seguridad adicionales • Ejercicios de Red Team. • Simulaciones de phishing. • Pruebas de ingeniería social. • Validación de controles implementados	10 puntos
Plan de mejora continua Presentación de un plan de fortalecimiento de la postura de Ciberseguridad.	8. puntos

Para la asignación del puntaje por el factor de calidad, el proponente deberá presentar los documentos de los profesionales ofrecidos.

La no presentación o indebida presentación de los documentos que acreditan los profesionales, tendrá como calificación cero (0) puntos.

Los documentos de los profesionales ofrecidos deben acreditarse durante la etapa de requisitos habilitantes, lara esto leer detenidamente el punto 3 del estudio previo donde están las condiciones del personal técnico:

1. Copia de la Cedula.
2. Copia del Diploma o acta de grado.
3. Copia de la Tarjeta Profesional .
4. Certificados de experiencia.
5. Los Certificados requeridos, los cuales deben ser expedidos por el Fabricante .

2.6.5 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
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.

2.6.6 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.

2.6.7 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.

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	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

[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.

	a la fecha de cierre del Proceso de Selección en el mismo cargo u otro del mismo nivel.	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.

2.6.8 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.

2.6.9 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 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.

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 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.

REDUCCIÓN DE PUNTAJE POR INCUMPLIMIENTO

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%).

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.

ESTOS DOCUMENTOS SERAN EVALUADOS EN LA ETAPA DE REQUISITOS HABILITANTES

- Mínimo 1 Ingeniero certificado como arquitecto en ciberseguridad por parte del fabricante en la solución a entregar
- Mínimo 1 Ingeniero certificado en operación de seguridad por parte del fabricante en la solución a entregar
- Mínimo 1 Técnico o tecnólogo con experiencia soportada en operación de seguridad en la solución a entregar.
- Mínimo 1 Ingeniero certificado como arquitecto de soluciones de nube por parte del fabricante en la solución a entregar
- Mínimo 1 Ingeniero especialista en proyectos, certificado en ITILV4, con experiencia en seguridad que garantice la correcta ejecución del objeto del contrato

El contratista deberá presentar la tarjeta profesional vigente de cada profesional y para los roles de arquitecto en ciberseguridad, operación de seguridad, arquitecto de soluciones de nube, deberá presentar las certificaciones emitidas por el fabricante de la marca ofertada.

Cada profesional deberá entregar certificado laboral con funciones que evidencie que cuenta con mínimo con 3 años de experiencia.

El mínimo aceptable para todos los roles será de 3 personas. Esto debido a que 1 ingeniero puede contar con varios de estos certificados.

4. OBLIGACIONES DEL CONTRATISTA.

4.1. GENERALES:

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:

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, obligaciones y dudas.
2. Cumplir con los requisitos técnicos y actividades descritas en el numeral 2.1 ESPECIFICACIONES TÉCNICAS del Estudio Previo. Entregable: Informe técnico de entrega final, el cual debe contener cada ítem de numeral 2.1 e indicar actividad realizada o licencia entregada.
3. Mediante carta firmada por el Representante Legal, Informar detalladamente el alcance de la garantía comercial del servicio, la cual debe coincidir con las características mencionadas en las especificaciones técnicas.
   Entregable: Carta firmada por el representante legal.
4. Brindar el soporte técnico con referencia al especificado en la carta de garantía comercial, 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. El contratista deberá realizar una visita presencial con periodicidad quince (15) días para analizar y determinar la reducción de superficies de ataque y realizar implementaciones de hardening.
8. 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.
9. Las demás que determine la entidad en función del correcto funcionamiento del objeto contractual.

4.3 OBLIGACIONES ALMBIENTALES:

En 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, en todo caso no podrá exceder el plazo en días, contados a partir que se hayan cumplido los requisitos de ejecución, legalización del contrato y suscrito el acta de inicio.

6.1. LUGAR DE EJECUCIÓN: Será la ciudad de Medellín, en las instalaciones del INDER Alcaldía de 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 C del numeral 2 del artículo 2° de la Ley 1150 de 2007 en armonía con el artículo 2.2.1.2.1.2.21 del Decreto 1082 de 2015 el cual establece:
N°. 3 del Art. 2.2.1.1.2.1.1 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 a 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 la suma de **OCHOCIENTOS TREINTA Y DOS MILLONES OCHOCIENTOS SESENTA Y UN MIL OCHOCIENTOS CINCUENTA PESOS M.L ($ 832.861.850),** 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
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 el valor del contrato, una vez sean recibidos el 100% los servicios solicitados, previo visto bueno y recibido a satisfacción por parte del supervisor del contrato y cumpliendo los requisitos exigidos por parte de la entidad.

Todos los pagos estarán supeditados al recibo a satisfacción de los materiales e informes y del cumplimiento de las actividades contractuales.

Los pagos de las facturas estarán sujetos 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.

La factura debe ser enviada 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 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 2.2.1.1.2.2.1 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.

De acuerdo con lo previsto en el artículo 2.2.1.2.1.2.4. del Decreto 1082 de 2015, El INDER adjudicará el contrato al oferente que haya presentado el lance más bajo una vez surtida la subasta, en caso de presentarse un solo oferente se adjudicará de conformidad con lo señalado en el artículo 2.2,1.2.1.2.2 ibídem.

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:

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 hasta la liquidación.</td><td>Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato.</td></tr>
<tr><td>Calidad del servicio</td><td>Plazo del contrato y un (1) año más.</td><td>Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato.</td></tr>
<tr><td>Pago de salarios, prestaciones sociales legales e indemnizaciones laborales</td><td>Plazo del contrato y tres (3) años más</td><td>Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato.</td></tr>
</table>
</td></tr>
<tr><td>Tomador</td><td>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.</td></tr>
<tr><td>Información necesaria dentro de la póliza</td><td>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.</td></tr>
</table>

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.

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 INTEGRAL DE PROTECCIÓN (XDR, SIEM Y SOC) CON DETECCIÓN Y RESPUESTA DE CIBERSEGURIDAD PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN."**
PRESUPUESTO OFICIAL	**OCHOCIENTOS TREINTA Y DOS MILLONES OCHOCIENTOS SESENTA Y UN MIL OCHOCIENTOS CINCUENTA PESOS M.L ($ 832.861.850),** 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

María Alejandra Cañola Estrada
V.Bo. Financiera

Harrison Alexander Hernández Rúa
Vo. Bo. Técnico

Sergio Antonio Henao Botero
Vo. Bo. Técnico

Santiago Restrepo Vasquez
Vo. Bo. Jurídica

Juan Felipe Hernandez Galvis
Vo. Bo Ambiental