ANEXO TÉCNICO

La entidad requiere **ADQUIRIR E IMPLEMENTAR UN SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR (Endpoint Detection and Response), PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF (WEB APPLICATION FIREWALL). PARA FORTALECER LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN**, los servicios deben se desplegados en nube estar relacionados bajo una sola marca y deberán ser administrados mediante una sola interfaz de administración.

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

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

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

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

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

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

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

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

- **Datos actuales:**

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

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

- Se solicita un throughput promedio de 14.3 MB/s. Este se calcula de la siguiente manera: redondeamos el actual throughput a 3,5 MB/s en promedio y sumamos un crecimiento proyectado de 2 MB/s para los próximos 12 meses, esta suma da como resultado 5.5 MB/s al cual le sumamos 160 % de holgura para atender variaciones o picos de consumo durante la vigencia del servicio.

Pormenorización de los Datos de Requerimiento Mínimo Exigido:

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

proactiva el estado de los diferentes componentes de los servicios, para reaccionar de forma proactiva a una posible falla o indisponibilidad.

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

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

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

II. PROTECCIÓN ENDPOINTS Y SERVIDORES.

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

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

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

III. PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS.

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

El INDER Medellín cuenta con M365, Se debe tener presente que el INDER actualmente cuenta con 2.300 cuentas de usuario de correo electrónico, que corresponden a una cantidad fija que no tendrá crecimiento durante la ejecución del contrato y la vigencia de las

licencias, toda vez que este número ya considera el margen máximo de usuarios previsto por la Entidad.

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

INICIO DE LA VIGENCIA DE LAS LICENCIAS

El Contratista deberá realizar, con anterioridad al 20 de noviembre de 2026, todas las actividades necesarias para la configuración, instalación, puesta en funcionamiento y verificación del sistema de ciberseguridad, incluyendo las respectivas pruebas de funcionamiento y la entrega del informe de instalación. Lo anterior deberá ser revisado y ser recibido a satisfacción por parte del supervisor y del apoyo técnico antes de dicha fecha, con el fin de garantizar que las licencias puedan iniciar su vigencia el 20 de noviembre de 2026. De cualquier forma, la vigencia no deberá iniciar sin el recibido a satisfacción.

IV. **IMPLEMENTACIÓN Y SOPORTE TÉCNICO.**

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

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

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

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

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

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

1. PROTECCIÓN ENDPOINTS Y SERVIDORES	
La Entidad solicita una solución que provea la seguridad de las estaciones de trabajo y servidores mediante prevención, detección y respuesta ante amenazas en el EndPoint, que incluya protección contra malware, ransomware, amenazas sin archivo residentes en memoria, explotación de vulnerabilidades, robo de credenciales y uso malicioso de herramientas legítimas del sistema operativo, gestionada desde una sola interfaz.	
Cantidad	1020
Vigencia	12 meses
Medida	Unidad
#	**Requerimiento Técnico Mínimo (de obligatorio cumplimiento)**
	GENERALIDADES
1.1	La Entidad requiere del licenciamiento de la solución EDR para 1020 dispositivos. **SERVIDORES ON-PREMISES (20)** Protección de servidores de centro de datos con diferentes sistemas operativos en cualquier versión: • Windows server 2008 • Windows server 2012 • Windows server 2016 • Windows server 2022

	• Windows server 2025 • Linux Ubuntu 22.04 • CentOS 8 **ENDPOINTS (900)** • Debe tener compatibilidad Multiplataforma principalmente Windows, macOS en cualquier versión. **RESERVA ENDPOINTS (100)** • Debe tener compatibilidad Multiplataforma principalmente Windows, macOS en cualquier versión.
1.2	La solución de EDR debe proporcionar a la Entidad un conjunto de protecciones tanto en pre-ejecución —antes de que la amenaza tenga capacidad de comprometer el sistema— como en post-ejecución —cuando la amenaza ya interactúa con el servidor o la estación de trabajo—, con capacidad de respuesta en tiempo real. La capa de pre-ejecución debe incorporar un motor de prevención basado en aprendizaje automático, capaz de emitir un veredicto sobre archivos no vistos previamente sin depender exclusivamente de firmas, operando de forma local en el agente para mantener la protección en equipos desconectados de la red. La capa de post-ejecución debe operar mediante análisis de comportamiento en tiempo de ejecución, con capacidad de bloquear comunicaciones salientes a nivel de proceso, impedir el acceso malicioso al sistema de archivos y al registro, y detener el cifrado por ransomware, incluso en equipos sin conectividad con la consola de gestión.
2	**FUNCIONALIDADES DE PREVENCIÓN**
2.1	El EDR debe utilizar un motor antivirus de aprendizaje automático para detener la ejecución previa de malware. Esta capacidad NGAV viene integrada en un agente único y ligero, lo que permite a los usuarios asignar protección antimalware a cualquier grupo de terminales sin necesidad de ninguna solución adicional.
2.2	Disponer de aprendizaje automático, NGAV basado en kernel y Machine learning (ML)
2.3	Enriquecer los eventos de seguridad con información de inteligencia de amenazas proveniente de una base de datos en la nube actualizada de forma continua, incluyendo reputación de archivos, dominios y direcciones IP.
2.4	Mantener la capacidad de prevención y detección en equipos sin conectividad con la consola de gestión o con los servicios en la nube del fabricante, conservando la telemetría localmente y sincronizándola al restablecerse la conexión.
2.5	Proporcionar un control de dispositivos de almacenamiento extraíble (**Almacenamiento USB, Pendrive, Periféricos externos**), sobre estaciones de trabajo Windows, con políticas asignables de forma diferenciada por grupo de equipos. La solución debe permitir el bloqueo del uso de dispositivos por categoría (**Almacenamiento USB, Dispositivos móviles, Unidades ópticas, impresoras escáner, Dispositivos de interfaz HID, dongles, y los que pertenezcan en esta categorías**), y disponer de un mecanismo de

	autorización granular que habilite dispositivos específicos mediante su fabricante, descripción o número de serie, o una combinación de estos criterios. Todo intento de uso de dispositivo extraíble debe generar un evento registrado y consultable en la consola de gestión.
2.6	La solución debe reducir el ruido operativo mediante: clasificación automática del veredicto de cada evento, con historial y reclasificación posterior; agrupación de eventos relacionados en un incidente único; y excepciones granulares —acotables por proceso, ruta y grupo de equipos— que supriman detecciones equivalentes sin recurrir a exclusiones amplias.
2.7	La solución deberá evaluar vulnerabilidades en sistemas operativos y aplicaciones de EndPoints Windows, Windows Server y Linux, identificando CVE/CVSS, activos afectados y nivel de riesgo, y proporcionando mecanismos de mitigación como virtual patching mientras se realiza el parcheo definitivo.
3	**FUNCIONALIDADES DE DESCUBRIMIENTO**
3.1	El EDR debe contar con un sistema automatizado de control de políticas de superficie de ataques, con evaluaciones y descubrimiento de vulnerabilidades que permiten al personal encargado de la seguridad dar gestión.
3.2	Descubrir y controlar dispositivos no autorizados (por ejemplo, dispositivos no protegidos o no administrados) y detectar dispositivos IoT.
3.3	Realizar un seguimiento de aplicaciones ejecutadas, y su clasificación de seguridad.
3.4	Descubrir y mitigar las vulnerabilidades del sistema y las aplicaciones con parches virtuales, mediante el análisis de sus comunicaciones e inhabilitando el acceso a su comunicación con el exterior.
3.5	Al descubrir las vulnerabilidades debe mostrar la clasificación de reputación y el detalle de los códigos CVE aplicables
3.6	Reducir la superficie de ataque con políticas proactivas basadas en niveles de riesgo.
4	**FUNCIONALIDADES DE DETECCIÓN Y PROTECCIÓN**
4.1	El EDR debe detectar y desactivar el malware así sean amenazas del tipo sin archivos o file-less y otros ataques avanzados en tiempo real para proteger los datos y evitar brechas en la seguridad en la entidad. Tan pronto como el EDR detecte flujos y comportamientos sospechosos, inmediatamente debe desactivar las amenazas potenciales, bloquear las comunicaciones salientes y el acceso al sistema de archivos desde esos procesos sospechosos, por otro lado, debe evitar la exfiltración de datos, las comunicaciones de comando y control (C&C), la manipulación de archivos y el cifrado de ransomware. Al mismo tiempo, el backend del EDR debe continuar recopilando evidencias adicionales, enriqueciendo los datos de eventos y clasificando los incidentes para aplicar de forma automatizada una estrategia de respuesta a incidentes, permitiendo así automáticamente la continuidad del negocio incluso en dispositivos ya comprometidos cumpliendo como mínimo con los siguientes ítems:
4.2	Detección basada en el análisis del comportamiento en tiempo de ejecución con visibilidad a nivel de kernel sobre los procesos y actividades del EndPoint, capaz de identificar técnicas de infiltración sigilosa, ataques residentes en memoria, ataques basados en

	scripts y uso malicioso de herramientas y binarios legítimos del sistema operativo (living off the land).
4.3	Debe Proporcionar protección en los procesos en ejecución, el inicio y parada de procesos, y en las interacciones entre procesos, así como frente a actividades sospechosas asociadas a librerías (archivos DLL en el caso de sistemas operativos Windows).
4.4	Debe poder Detener las amenazas en tiempo real y eliminar el tiempo de permanencia de dichas amenazas en la organización, incluso en los endpoints desconectados de la red corporativa.
4.5	Debe Bloquear las comunicaciones de forma granular a nivel de proceso, evitando exfiltraciones de datos, movimientos laterales y conexión con redes de comando y control.
4.6	Debe Impedir a los procesos maliciosos el acceso a los sistemas de ficheros, protegiendo frente a cifrados de ransomware, y la creación/modificación/eliminación maliciosa de archivos y/o registros.
4.7	Debe permitir definir listas de permitidos y denegados mediante criterios de identificación de archivos y aplicaciones que incluyan, como mínimo: hash del archivo, nombre y ruta de ubicación, y firma digital del editor, admitiendo para este último criterio la identificación por certificado, por huella digital del certificado o por nombre del firmante.
4.8	Debe Proporcionar la capacidad para marcar, tanto manual como automáticamente, determinada actividad como falso positivo, evitando además que ocurran detecciones similares.
4.9	La solución deberá conservar los eventos de seguridad y la telemetría de actividad del endpoint durante un período mínimo de noventa (90) días, disponibles para análisis retrospectivo mediante consultas estructuradas sobre la totalidad del período retenido.
4.10	La solución debe revalidar el veredicto de los eventos de seguridad mediante un análisis posterior en el servicio en la nube del fabricante, que incorpore inteligencia de amenazas. Cada reclasificación debe registrarse en un historial auditable, y las acciones de respuesta automatizada deben basarse en el veredicto final.
5	**FUNCIONALIDADES DE PROTECCIÓN CONTRA RANSOMWARE**
5.1	La solución de EDR debe contar con políticas predefinidas y exclusivas para la prevención de secuestro de información por ataques de ransomware, por lo cual debe incluir más de 30 estrategias de protección diferentes. Dichas estrategias deben incluir como mínimo:
5.2	1. Debug de Procesos.
5.3	2. Código dinámico.
5.4	3. Formato de archivo ejecutable incorrecto
5.5	4. Una pila con código ejecutable
5.6	5. El programa ejecutado no tiene instalador
5.7	6. Programa crítico falso.
5.8	7. Empaquetador falso.
5.9	8. File Encryptor.
5.10	9. Proceso oculto.
5.11	10. Ejecutable inyectado.

5.12	11. Proceso inyectado.
5.13	12. Hilo inyectado.
5.14	13. Suma de comprobación no válida.
5.15	14. Ejecución no válida.
5.16	15. Puntero no válido.
5.17	16. Inyección de kernel.
5.18	17. Empaquetador conocido.
5.19	18. Archivo malicioso detectado.
5.20	19. Proceso malicioso.
5.21	20. Ejecutable modificado.
5.22	21. Stack Parcialmente asignado.
5.23	22. Exploit de escalamiento de privilegios.
5.24	23. Proceso vacío.
5.25	24. Manipulación de pilas.
5.26	25. Aplicación sospechosa.
5.27	26. Empaquetador sospechoso.
5.28	27. Ejecutable manipulado.
5.29	28. Ejecutable no confirmado.
5.30	29. Ejecutable sin asignar.
5.31	30. Código grabable.
6	**FUNCIONALIDADES DE REMEDIACIÓN**
6.1	La Solución de EDR propuesta debe orquestar operaciones de respuesta a incidentes utilizando playbooks predefinidos en la solución, optimizando sí la respuesta a incidentes y los procesos de remediación, revirtiendo de modo automático los cambios maliciosos realizados por amenazas ya contenidas, en un único dispositivo o en dispositivos distribuidos a lo largo del entorno de la entidad, las características de remediación deben cumplir como mínimo con los siguientes requerimientos:
6.2	Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta.
6.3	La solución debe permitir definir playbooks de respuesta configurables por clasificación de evento y por grupo de dispositivos, con acciones ejecutables de forma automática o previa aprobación del analista.
6.4	Debe optimizar los recursos de seguridad, automatizando las acciones de respuesta a incidentes, como la eliminación de archivos, la finalización de procesos maliciosos, la reversión de cambios persistentes, la notificación a los usuarios, el aislamiento de aplicaciones y dispositivos, y la integración con una plataforma de ITMS para apertura de tickets.
6.5	Debe permitir la respuesta a incidentes basada en el contexto utilizando la clasificación de incidentes y los sujetos de los ataques (como, por ejemplo, grupos de estaciones de trabajo).
6.6	Visibilidad completa de la cadena de ataque y de los cambios realizados en el sistema, con representación gráfica de la secuencia de procesos involucrados desde el origen.

6.7	Reversión automatizada de cambios de persistencia introducidos por la amenaza, incluyendo entradas de registro, tareas programadas y servicios creados o modificados.
6.8	Debe realizar la contención y respuesta de forma automática
6.9	Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta.
7	**FUNCIONALIDADES DE INVESTIGACIÓN**
7.1	La solución de EDR debe enriquecer automáticamente los registros de los eventos con información detallada sobre el malware antes y después de la infección, para realizar análisis forenses en los endpoints infiltrados. Su interfaz guiada debe proporcionar una guía útil, mejores prácticas y sugerir los próximos pasos lógicos a los analistas de seguridad, estas características de investigación deben cumplir como mínimo con los siguientes requerimientos:
7.2	Debe tener la capacidad de contención automática de la amenaza debe permitir que el análisis forense posterior se realice sin presión de tiempo, manteniendo el equipo operativo.
7.3	Debe contar con la capacidad de visualización de la cadena de ataque completa con identificación del origen de la infección (paciente cero), disponible incluso cuando el dispositivo se encuentre fuera de línea.
7.4	Debe conservar instantáneas de memoria, de los ataques sin archivo o file-less para la búsqueda de amenazas basada en memoria.
7.5	La interfaz grafica debe mostrar explicaciones claras por qué el evento está marcado como sospechoso o malicioso, enumera el marco de ataque MITRE correspondiente, así como el siguiente paso lógico para la investigación forense.
8	**FUNCIONALIDADES DE EDR**
8.1	La solución de EDR debe disponer de capacidades de integración con otras plataformas de seguridad del ecosistema de la Entidad, ya sea mediante conectores nativos preconfigurados por el fabricante o mediante interfaces de programación de aplicaciones (API) documentadas públicamente. La integración deberá permitir, como mínimo, el intercambio bidireccional de información de eventos e indicadores de compromiso, y la ejecución de acciones de respuesta coordinada. El proponente deberá acreditar, mediante documentación técnica oficial del fabricante, la disponibilidad de la integración para cada una de las siguientes categorías de solución:
8.2	1. Next Generation Firewall de la Entidad
8.3	2. Control de Acceso a la Red.
8.4	3. Análisis dinámico de archivos en entorno aislado SandBoxing.
8.5	4. Plataformas de engaño (deception) o honeypots
8.6	5. Correlacionador de Eventos, SIEM.
8.7	6. Plataforma de Orquestación, automatización y respuesta a incidentes, SOAR.
8.8	7. Plataforma de Análisis de comportamiento de usuario UEBA
8.9	8. Plataforma de Manejo de Identidades, IAM
8.10	Debe contar con la funcionalidad de INVESTIGACIÓN IMPULSADA POR INTELIGENCIA ARTIFICIAL

8.11	Debe contar con la funcionalidad de RESPUESTA AUTOMATIZADA
9	**COMPONENTES DE LA SOLUCIÓN DE EDR**
9.1	La plataforma de seguridad del endpoint EDR debe ser una arquitectura distribuida, la cual debe constar de una agente en software el cual debe ser compatible con los siguientes sistemas operativos y entornos, en versiones de 32 y 64 bits:
9.2	Windows: XP SP2/SP3, 7, 8, 8.1 y 10.
9.3	Windows Server: 2003 R2 SP2, 2008 R2 SP2, 2012, 2012 R2, 2016 y 2019.
9.4	MacOS: Yosemite (10.10), El Captain (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15).
9.5	Linux: Redhat Enterprise Linux and CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 and 7.7, y Ubuntu LTS 16.04.5, 16.04.6, 18.04.2 server, en 64-bit.
9.6	Entornos VDI: VMware Horizons 6 y 7, y Citrix Desktop 7.
9.7	consumo de memoria de 350 MB con todos los módulos activados, incluido Threat Hunting, y 1 GB de almacenamiento con todos los módulos activados, incluido Threat Hunting.
9.8	Adicional la solución debe permitir ser desplegada de cualquiera de las siguientes maneras:
9.9	Nube: En la Nube del Fabricante.
9.10	On-Premise: En el Datacenter de la entidad.
9.11	Hibrida: En Nube y On-premise.
9.12	AirGapped o Sistemas Cerrados.
9.13	El producto debe incluir servicios de mejores prácticas implementadas por personal de servicios de Fabrica o un partner de servicios autorizado por Fabrica
10	**Servicios Profesionales**
10.1	La solución debe ofrecer transferencia de conocimiento en la fase de implementación sin cargo adicional.
10.2	El servicio de atención al cliente deberá estar disponible las 24 horas del día, los 7 días de la semana por correo electrónico, chat y teléfono.
10.3	El soporte del servicio debe entregarse por 12 meses

2. PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS		
La Entidad solicita una solución que provea la seguridad del sitio de trabajo a través de protección del correo electrónico, plataformas de colaboración, que incluya protección contra phishing, ransomware, ataques de día cero y apropiaciones de cuentas en una sola consola.		
Cantidad		2300
Vigencia		12 meses
Medida		Unidad
#	**Categoría**	**Requerimiento Técnico Mínimo (de obligatorio cumplimiento)**
1	**Protección de correo electrónico.**	
1.1	**Escaneo de correo electrónico**	La solución debe analizar dinámicamente el 100% de los correos electrónicos

1.2		La solución debe analizar todas las URL y archivos adjuntos de los correos electrónicos entrantes
1.3		La solución debe escanear dinámicamente los correos electrónicos a una velocidad media de 15 segundos
1.4		El administrador de la solución debe estar en capacidad de acceder automáticamente a los detalles del análisis para ver las razones exactas por las que se marca un correo electrónico como malicioso
1.5		La solución debe proteger activamente contra el spam
1.6		La solución debe identificar amenazas después de la entrega de correo. Debe estar en capacidad de notificar a los usuarios y recuperar correos electrónicos maliciosos de sus bandejas de entrada para ponerlos en cuarentena automáticamente
1.7	**Identificación de amenazas**	La solución debe utilizar fuentes de inteligencia sobre amenazas para identificar amenazas conocidas
1.8		La solución debe utilizar capacidades internas de búsqueda de amenazas asistidas por humanos
1.9		La solución debe escanear los correos electrónicos de forma estática utilizando motores Antivirus
1.10		La solución debe utilizar herramientas para identificar firmas muy complejas
1.11	**Amenazas avanzadas**	La solución debe proteger contra los ataques de phishing a través del reconocimiento de imágenes, el análisis de texto y los evaluadores de reputación
1.12		La solución debe proteger contra los ataques BEC cuando se realizan comprobaciones SPF, DKIM y DMARC
1.13		La solución debe proteger contra los ataques de suplantación de identidad mediante el uso de técnicas para descubrir la suplantación de nombres de visualización y la suplantación de VIP
1.14		La solución debe proteger contra ataques de día cero y día N al inspeccionar datos a nivel de CPU
1.15		La solución debe detectar ATO mediante la observación de anomalías en el comportamiento del usuario
1.16	**Manejo de URL**	La solución debe hacer clic y escanear activamente las direcciones URL para identificar enlaces maliciosos antes de que lleguen al buzón del usuario final
1.17	**Sandbox**	La solución contar con la tecnología Sandbox para identificar archivos maliciosos
1.18		La solución debe utilizar datos de nivel de CPU para inspeccionar el flujo de ejecución de archivos
1.19		La solución debe mantener la integridad de los archivos durante los análisis, evitando alterar la estructura de los archivos

1.20		La solución debe identificar vulnerabilidades de daño en la memoria
1.21		La solución debe detectar errores lógicos y macros dentro de los documentos
1.22	**Gestión de archivos**	La solución debe escanear cientos de tipos de archivos diferentes
1.23		La solución debe descomprimir el contenido de forma recursiva, buscando enlaces y archivos incrustados para escanear
1.24		La tecnología de la solución para escanear enlaces y archivos incrustados debe tener al menos 7 capas de profundidad
1.25		La solución debe analizar contenido protegido con contraseña al entregarse el password
1.26		La solución debe analizar archivos comprimidos/comprimidos
1.27	**Situación del mercado**	La solución debe estar en la Guía de mercado de Gartner para la seguridad del correo electrónico
1.28		La solución debe estar catalogada en los tres primeros lugares en la evaluación de SE Labs.
2	**Protección de herramientas de colaboración**	
2.1	**Protección de Herramientas de colaboración**	La solución debe ser compatible con Slack, Microsoft 365 (Teams, One Drive, SharePoint), Google Drive, Box, Salesforce, Dropbox, Zendesk, AWS S3 Buckets y otras aplicaciones usando APIs.
2.2		La solución debe detectar y bloquear archivos maliciosos, URLs, y ataques avanzados en las soluciones protegidas
2.3		La solución debe tener la capacidad de integrarse a un servicio de Incident&Response (IR) para evaluar casos particulares o solicitados por el usuario final.
2.4		Debe escanear el 100% de los datos
2.5		La solución debe evaluar los correos y URLs que se envíen por las plataformas evaluadas
2.6		El servicio debe tener un Objetivo de nivel de servicio de mínimo 99.98%
2.7		Debe proveer servicios de Análisis de amenazas, Análisis dinámico y estático de archivos, protección de toma de cuenta (mínimo MS365)
3	**Uso**	
3.1	**Duración**	La solución debe ser nativa de la nube y está totalmente alojada en la nube
3.2		La solución debe actualizarse automáticamente
3.3		La solución debe satisfacer las necesidades de escalamiento de licenciamiento de un cliente sin afectar la experiencia del usuario ni requerir la compra de equipos adicionales

3.4	**Instalación**	La solución debe permitir la implementación en modo de prevención de amenazas, evitando las amenazas antes de que lleguen a los usuarios finales
3.5		La solución debe permitir ser implementada en modo CCO/Journaling, así como en línea para una protección completa en M365 como mínimo
3.6		La solución debe permitir la implementación para los usuarios a través de una invitación por correo electrónico
3.7		La solución debe ser implementada automáticamente con la integración de Office 365
3.8	**Integración**	La solución debe tener la posibilidad de conectarse a través de API a otras aplicaciones
3.9		La solución debe integrarse con Office 365 a través de API sin necesidad de cambiar el registro MX
3.10		La solución debe poderse ajustar a las políticas e integrarse a un SIEM, y no requiere cambios en la infraestructura e integración vía REST APIs
3.11		La solución debe estar en capacidad de exportar registros en tiempo real a un SIEM
3.12		La solución debe estar en capacidad de integrarse con gestores de Identidades a través de SAML
3.13		Los usuarios se deben asignan automáticamente permisos a roles y grupos en función de un esquema RBAC
3.14		La solución debe estar en capacidad mediante licencias adicionales de proteger el uso del cliente del almacenamiento compartido, las herramientas de colaboración y el navegador
3.15	**Gestión de datos**	La solución debe cifrar los datos en reposo con AES-256 y en tránsito con TLS 1.2+
3.16		Las claves de cifrado deben estar protegidas con soluciones como AWS KMS
3.17		La solución debe cumplir con: SOC2, GDPR, HIPAA, ISO 27001
3.18		La solución debe estar alojada en servidores separados ubicados en Europa, EE. UU. y APAC para garantizar resiliencia del servicio
3.19	**Gestión**	La solución debe proporcionar un panel de administración informativo que muestre datos de incidentes, informes y políticas
3.20		la solución debe tener la opción de incluir en las listas negras o blancas en función de la IP, las URL, los dominios, los remitentes, los tipos de archivos, etc.
3.21		La solución debe registrar las acciones del usuario, como los intentos de inicio de sesión, los cambios en el veredicto, la publicación de correos electrónicos y las solicitudes de investigación

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

3. WAF (WEB APPLICATION FIREWALL)		
La entidad requiere una solución unificada para proteger aplicaciones web (**10 sitios máximo**) y debe permitir APIs, optimizar el rendimiento y simplificar la gestión en entornos híbridos y multi-nube, que cumpla con los siguientes requerimientos		
Cantidad		1
Vigencia		12 meses
Medida		Unidad
#	**Categoría**	**Requerimiento Técnico Mínimo (de obligatorio cumplimiento)**
1	**CARACTERÍSTICA/FUNCIONALIDAD**	
1.1	**Seguridad de Aplicaciones Web y API (WAF y API Security):**	Protección contra ataques de día cero mediante aprendizaje automático dual.
1.2		Eliminación de falsos positivos analizando y filtrando tráfico antes de llegar a las aplicaciones.
1.3		Protección contra los riesgos principales de OWASP Top 10.
1.4		Actualizaciones automáticas con inteligencia de amenazas en tiempo real.
1.5		Configuración simplificada a través de una interfaz intuitiva.
1.6		Protección basada en firmas.
1.7		Inteligencia de amenazas IP.
1.8		Inteligencia GEO-IP.
1.9		Reglas de seguridad personalizadas.
1.10		Cumplimiento de HTTP.
1.11		Protección de URL, parámetros y CORS.
1.12		Protección de cookies.
1.13		Prevención de fugas de información.

1.14		Antivirus para cargas de archivos.
1.15		Sandbox para cargas de archivos.
1.16		Protección contra ataques de día cero basada en aprendizaje automático.
1.17		Cumplimiento de esquemas (Open API, XML, JSON).
1.18		API Gateway.
1.19		Protección de API móviles.
1.20		Descubrimiento, catálogo de PII y protección basada en aprendizaje automático.
1.21		Protección de encabezados HTTP.
1.22		Protección contra CSRF y ataques Man-in-the-Browser (MiTB).
1.23	**Protección Avanzada contra Bots:**	Detección basada en comportamiento mediante análisis biométrico y de comportamiento.
1.24		Perfilado avanzado de dispositivos para bloquear ataques de bots.
1.25		Identificación y bloqueo de rastreadores web no deseados y amenazas automatizadas.
1.26		Análisis en tiempo real e histórico del tráfico y actividades de bots.
1.27		Protección avanzada contra bots (detección biométrica, firma y engaño).
1.28	**Balanceo de Carga Global de Servidores:**	Balanceo de carga basado en DNS para distribuir tráfico entre múltiples centros de datos.
1.29		Distribución geográfica del tráfico según métricas de salud y ubicación.
1.30		Integración sencilla con la plataforma de Protección Web.
1.31		Alta disponibilidad incluso durante interrupciones regionales.
1.32		Capacidad para realizar chequeos de salud (health checks) sobre servicios y aplicaciones, permitiendo identificar el estado operativo de sus componentes, detectar de manera anticipada posibles fallas o indisponibilidades y generar acciones de respuesta proactiva.
1.33	**Análisis de Amenazas:**	Identificación de patrones de ataque ocultos mediante correlación de eventos basada en IA.
1.34		Visibilidad en tiempo real de eventos de seguridad en toda la infraestructura.
1.35		Respuesta proactiva a incidentes con inteligencia de amenazas y flujos de trabajo automatizados.
1.36		Reducción de la fatiga de alertas consolidando múltiples alertas en incidentes significativos.
1.37	**Automatización**	Automatización de tareas de seguridad como actualizaciones de políticas y correcciones de configuración.
1.38		Priorización de amenazas de alto riesgo y caza adaptativa de amenazas.
1.39		Enriquecimiento de inteligencia de amenazas para mejorar la defensa proactiva.
1.40		Seguimiento de usuarios.

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

4. IMPLEMENTACIÓN Y SOPORTE TÉCNICO	
4.1	● Soporte Técnico durante 12 meses de la plataforma seguridad deberá contar como mínimo con las siguientes características: ○ Actualizaciones y mantenimiento de producto o Compatibilidad con nuevos sistemas operativos, acceso a versiones nuevas sin costo adicional dentro de la vigencia. ○ Soporte técnico: Deberá incluir, atención remota telefónica 24/7, asistencia para configuración y despliegue, guías técnicas, manuales y base de conocimientos, SLA (acuerdo de nivel de servicio). Medios de escalamiento mínimo helpdesk con usuario y contraseña

	○ Transferencia de Conocimiento: Actividad de transferencia de conocimiento inicial sobre uso del producto 20 horas; laboratorios de aprendizaje de uso de la solución para administradores o equipos técnicos, documentación de mejores prácticas. ○ Interfaz de administración: Recuperación, restablecimiento o migración sin costo adicional, en caso de que aplique.
4.2	● Realizar todas las actividades necesarias para la configuración, instalación, puesta en funcionamiento y verificación del sistema de ciberseguridad, incluyendo las respectivas pruebas de funcionamiento y la entrega del informe de instalación con el protocolo y resultados de pruebas realizadas. Lo anterior deberá ser recibido a satisfacción por parte del supervisor y del apoyo técnico.

- Todas las actividades, comunicaciones y documentos relacionados con el proceso de contratación y la ejecución del contrato deberán realizarse y presentarse en idioma castellano.
- Todos los componentes deber ser del mismo fabricante.
- La vigencia de la solución de seguridad debe iniciar a partir de la entrega a satisfacción y estar activa por 12 meses.
- Las licencias de la plataforma de seguridad deben ser en la última versión publicada por el fabricante y deben quedar a nombre del INDER Medellín.
- La plataforma de seguridad debe contar con acceso a actualizaciones periódicas para la protección contra nuevas amenazas.
- La garantía comercial del fabricante:
- El licenciamiento de los productos tendrá una vigencia de doce (12) meses, durante los cuales deberá mantenerse vigente el soporte del fabricante. El fabricante deberá garantizar la disponibilidad de soporte técnico 24x7, permitiendo la apertura y atención de casos de soporte durante todo el periodo de vigencia del licenciamiento.

ACTIVIDADES A EJECUTAR POR EL CONTRATISTA:

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

1. Una vez suscrita el Acta de Inicio por las partes, el Contratista deberá realizar un análisis del nivel de seguridad actual del INDER Medellín y presentar los resultados de dicho

examen al Instituto, el cual deberá ser entregado mediante un informe por escrito a más tardar 15 días calendario contados a partir de la suscripción del Acta de Inicio.

2. Con anterioridad al 20 de noviembre de 2026, el Contratista deberá proceder con la Instalación, configuración y puesta en marcha de las soluciones definidas (EDR, PROTECCIÓN DE CORREO Y HERRAMIENTAS COLABORATIVAS Y WAF) en el presente alcance:

    a. Despliegue del 40% de los 1020 agentes en los EndPoint.
    b. Despliegue de agentes en 5 de los 20 para servidores.
    c. Despliegue de la solución WAF con la configuración de las políticas de protección para 10 sitios Web.
    d. Despliegue y configuración de la protección para 2300 buzones de correo y herramientas colaborativas.
    e. Configuración de la interfaz de administración e integración de los servicios.

3. Con anterioridad al 20 de noviembre de 2026, deberá alinear la solución de seguridad según las políticas de ciberseguridad del INDER Medellín.
4. Transferencia de conocimiento a 3 integrantes del personal técnico del INDER Medellín sobre la administración del **SISTEMA DE PROTECCIÓN EN CIBERSEGURIDAD EDR, PROTECCIÓN DE CORREO, HERRAMIENTAS COLABORATIVAS Y WAF**.
5. Envió de Campañas de entrenamiento para usuarios finales en la identificación de situaciones de riesgo, “Boletines de sensibilización de Ciberseguridad” a través de correo electrónico, a los usuarios del instituto (gestionado y coordinado entre el oferente y la coordinación de TI.).
6. Capacitación virtual (dos al año), sobre concienciación en ciberseguridad para usuarios finales durante la vigencia del contrato y las licencias, entregar evidencia documentada que incluya el contenido o protocolo de la actividad una vez sea realizada.
7. Durante la vigencia de las licencias y a solicitud del apoyo técnico del instituto, realizar una evaluación de ciberseguridad basado en algún framework cómo: NIST, ISO 27001 o CIS Controls. Entregar evidencia documentada que incluya alcance, criterios de severidad, protocolo y demás contenido de la actividad una vez sea realizada

REQUISITOS HABILITANTES

EXPERIENCIA DEL PROPONENTE:

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

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

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

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

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

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

a. Fecha de expedición
b. Razón social del contratante
c. Razón del social del contratista con Nit
d. Teléfonos del contratante (si es empresa privada)
e. Valor final del contrato, expresado en pesos colombianos o SMMLV
f. Fecha de inicio y terminación del contrato.

g. Objeto del contrato, este debe tener relación con el suministro e implementación de soluciones, tecnologías o servicios especializados de ciberseguridad, destinados a fortalecer la protección y seguridad de infraestructuras tecnológicas.

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

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

PERSONAL PROFESIONAL REQUERIDO

Esta documentación será evaluada en la etapa de requisitos habilitantes.

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

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

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

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

	Debe acreditar mediante una certificación que cuenta con conocimientos para brindar soluciones de seguridad de redes, debe estar vigente y debe ser emitida por el fabricante. Debe contar con certificación de EH-Ethical Hacker vigente. **Experiencia específica:** Mínimo Dos (2) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad.
Un (1) Ingeniero de apoyo a la implementación WAF	**Nivel Profesional:** Ingeniero eléctrico o electrónico o de sistemas o telecomunicaciones o telemática. **Experiencia general:** Mínimo tres (3) años de experiencia general profesional contados a partir de la expedición de la matrícula profesional. Debe contar con certificación como Profesional de seguridad en nube emitida por el fabricante. **Experiencia específica:** Mínimo un (1) años de experiencia profesional especifica de apoyo en soporte de soluciones de seguridad

Documentación para entregar

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

Teniendo en cuenta que el personal propuesto es objeto de verificación dentro de los requisitos habilitantes, las hojas de vida y el personal acreditado por el proponente durante el proceso de selección no podrán ser sustituidos, sin embargo, durante la ejecución del

contrato, cuando por razones de fuerza mayor sea necesario solicitar el cambio de un profesional, el contratista deberá presentar la documentación de un profesional que cumpla, como mínimo, con las mismas condiciones y requisitos establecidos para el perfil que se pretende reemplazar.

OBLIGACIONES ESPECÍFICAS

1. Dentro de los primeros 5 días hábiles posteriores a la fecha de inicio del contrato, el contratista deberá asistir a una reunión presencial o virtual para socializar requisitos exigidos por INDER Medellín, obligaciones establecidas por INDER Medellín y dudas del contratista.
2. Cumplir con los requisitos técnicos y actividades descritas en el anexo técnico y ESPECIFICACIONES TÉCNICAS del Estudio Previo. Entregable: Informe técnico de entrega final, el cual debe contener cada ítem indicar actividad realizada o licencia entregada.
3. Mediante carta firmada por el Representante Legal, Informar detalladamente el alcance de la garantía del fabricante y soporte técnico adquirido para los servicios contratados, la cual debe coincidir con las características mencionadas en las especificaciones técnicas.
   Entregable: Carta firmada por el representante legal.
4. El contrista deberá brindar el soporte técnico, de conformidad con las condiciones y alcance establecidos en la carta de garantía, cuando sea requerido por la supervisión durante la vigencia de la plataforma adquirida.
5. El contratista deberá presentar un informe cuantitativo del desempeño de toda la solución de seguridad con periodicidad mensual durante la vigencia de la plataforma adquirida.
   Entregable: Carta firmada por el representante legal con este compromiso.
6. El contratista deberá entregar de forma digital, la evidencia de las licencias(s) de la plataforma a nombre del INDER Medellín.
7. Deberá contar con un sistema de escalamiento de solicitudes, medios de contacto y SLA. Entregable: Incluir esta información en el informe técnico de entrega final.
8. El contratista deberá desarrollar cronogramas, planes de trabajo e implementación, procedimientos y contenidos que sean necesarios para la correcta ejecución de todas las actividades que conlleve el proyecto.
9. Durante la vigencia de las licencias, realizar dos (2) pruebas de penetración, en las fechas que sean determinadas y solicitadas por el apoyo técnico designado por la Entidad, quien comunicará oportunamente al contratista los momentos en los cuales deberán ejecutarse dichas pruebas. una vez realizada cada prueba deberá entregar el informe al instituto con todo el protocolo realizado.

PLAZO: Hasta el 31 de diciembre de 2026

PARÁGRAFO: A más tardar el 20 de noviembre de 2026, el contratista deberá haber culminado las actividades de diagnóstico, instalación, configuración y parametrización, de manera que la solución se encuentre completamente implementada y en operación.

El plazo comprendido entre el 20 de noviembre y el 31 de diciembre de 2026 estará destinado a la ejecución de actividades posteriores a la implementación, tales como la elaboración de informes, actividades derivadas de la puesta en funcionamiento de la solución y verificaciones necesarias para la autorización de pago.

A partir del 31 de diciembre de 2026 y hasta el 31 de octubre de 2027, el contratista deberá continuar prestando de forma ininterrumpida, todos los servicios contratados y previstos en las especificaciones técnicas incluyendo garantía, soporte, mantenimiento, disponibilidad, actividades con alcance dentro de la vigencia de las licencias y las demás obligaciones detalladas en las especificaciones técnicas, obligaciones específicas y garantizando el correcto funcionamiento de la solución durante todo el período de prestación del servicio correspondiente a 1 año.

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

PONDERABLE

CALIDAD	PUNTAJE MÁXIMO
PLAN DE MEJORA CONTINUA DE LA POSTURA DE CIBERSEGURIDAD: El plan deberá estar estructurado a partir de una metodología de evaluación de ciberseguridad reconocida, basada en alguno de los siguientes marcos de referencia: NIST Cybersecurity Framework (CSF), ISO/IEC 27001 o CIS Controls, y deberá contemplar como mínimo: **1.** Metodología propuesta para realizar la evaluación de la postura actual de ciberseguridad. **2.** Análisis de la postura de ciberseguridad y definición iniciativas de fortalecimiento. **3.** Propuesta de acciones de mejora orientadas al fortalecimiento de la postura de ciberseguridad.	28

4. Definición de responsables, recursos y tiempos estimados para la implementación de las acciones. **5.** Sesión de seguimiento y actualización del plan de mejora continua antes de finalizar el contrato. **Perfil del profesional que lidera la actividad** Esta actividad debe ser liderada por un profesional con: Título profesional: Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Electrónica, Ingeniería de Software o Ingeniería de Telecomunicaciones. Título de posgrado: Especialización o maestría en áreas relacionadas con Seguridad Informática, Ciberseguridad o Seguridad de la Información. Certificaciones vigentes: Una (1) certificación vigente CEH – Certified Ethical Hacker. Una (1) certificación vigente como Lead Cybersecurity Manager en ISO/IEC 27032. Una (1) certificación vigente como Auditor Líder o Auditor Interno en ISO/IEC 27001:2022.	

Documentación para entregar

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

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