ANEXO TÉCNICO

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.

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.

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.

REQUISITOS

- La vigencia de la solución de seguridad debe iniciar a partir del 1 de octubre 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	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** • **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.	1020	12	Unidad

		-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. -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	2300	12	Unidad

		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			
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)	2300	12	Unidad

		- 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).			
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 -Capacidad de evaluar en tiempo real el riesgo asociado a usuarios y sesiones, aplicando controles automáticos	2300	12	Unidad

		-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	2300	12	Unidad

		-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 -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 cualquier 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.	1	12	Unidad

		• 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 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**	1	12	Unidad

		• **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 • 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			

ACTIVIDADES A EJECUTAR POR EL CONTRATISTA:

1. Tramitar EARLY BILLING con el fabricante si aplica.

2. 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.

3. Alinear la solución de seguridad según las políticas de ciberseguridad del INDER Medellín.

4. 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.

5. Envió de campañas de Phishing y entrenamiento a usuarios final por medio de la solución por lo menos 2 veces al año.

6. 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**.**

7. 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.

REQUISITO HABILITANTE

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 y 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.**

PERSONAL TÉCNICO

- 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 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

Deberá presentar tarjeta profesional y/o certificados por los fabricantes de la marca que entregará.

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 PRESUPUESTOS DIVIDO SMMLV, 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.
j. No se aceptarán subcontratos.
k. Cuando el Proponente se trate de consorcio o unión temporal la experiencia debe ser acreditada por al menos uno de los asociados.
l. Porcentaje de participación en el Consorcio o Unión Temporal, en caso de que aplique

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

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, 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.