Código de la dependencia productora

Bogotá D.C., 09 de septiembre de 2025

SEÑORES

PROVEEDORES

Asunto: SOLICITUD DE INFORMACIÓN PARA ESTUDIO DE MERCADO

Respetados señores:

Atentamente solicito su colaboración, a efectos de obtener información para consolidar estudios de mercado sobre los bienes, obras y/o servicios que se citan a continuación:

<table>
<tr><td>OBJETO</td><td colspan="2">Contratar los servicios de un Centro de Operaciones de Seguridad (SOC) para el monitoreo, alertamiento y gestión de la seguridad de la información de la plataforma tecnológica del Ministerio de Hacienda y Crédito Público.</td></tr>
<tr><td rowspan="8">UNSPSC</td><td>CÓDIGO UNSPSC</td><td>DESCRIPCIÓN</td></tr>
<tr><td>43233200</td><td>Software de Seguridad y Protección</td></tr>
<tr><td>43222500</td><td>Equipo de seguridad de red</td></tr>
<tr><td>81111800</td><td>Servicios de sistemas y administración de componentes de sistemas</td></tr>
<tr><td>81112200</td><td>Mantenimiento y Soporte de Software</td></tr>
<tr><td>81161500</td><td>Servicios de administración de acceso</td></tr>
<tr><td colspan="2">Nota: Por favor indicar el código en el cual está clasificado el bien o servicio a contratar.</td></tr>
<tr><td rowspan="2">DESCRIPCIÓN Y/O ALCANCE</td><td>ESPECIFICACIONES TÉCNICAS MÍNIMAS</td><td>COTIZACIÓN ALTERNATIVA</td></tr>
<tr><td>Ver anexo. No. 1</td><td>En caso de que aplique o se requieran</td></tr>
<tr><td>DURACION DEL CONTRATO</td><td colspan="2">El plazo de duración del contrato será hasta el 31 de julio de 2026, contados a partir de la fecha de activación del servicio Centro de Operaciones de Seguridad (SOC), previa aprobación de la(s)</td></tr>
</table>

	garantía(s) que debe constituir el contratista y expedición del registro presupuestal.
PLAZO PARA LA ENTREGA DE LOS BIENES Y/O SERVICIOS	N/A
LUGAR DE EJECUCIÓN	Para todos los efectos, el lugar de ejecución del contrato será en la ciudad de Bogotá, D.C. en las sedes del Ministerio de Hacienda y Crédito Público y de manera virtual en el evento de requerirse, previa autorización del Supervisor del contrato, bajo herramientas tecnológicas autorizadas por el Ministerio de Hacienda y Crédito Público.
FORMA DE PAGO	El MINISTERIO pagará al CONTRATISTA, una vez se encuentre aprobado el P.A.C. (Programa anual mensualizado de caja), como se informa a continuación: a. Por el servicio de Monitoreo, diagnostico, generación de alertas y recomendaciones se realizarán pagos mensuales o fracción de mes, durante la ejecución del contrato. b. Por el servicio de Gestión y Análisis de Vulnerabilidades se realizarán pagos mensuales o fracción de mes, durante la ejecución del contrato. c. Un pago en la vigencia 2026 por el servicio de análisis de vulnerabilidades y ethical hacking (un evento durante la ejecución del contrato). d. Para las Horas de Servicio de análisis forense de incidentes de seguridad de la información, se efectuarán pagos acordes al número de horas utilizadas durante las vigencias 2025 y 2026 hasta 200 horas máximo. Dichos pagos se efectuará dentro de los diez (10) días hábiles siguientes a la radicación en la Subdirección Financiera del cumplido a satisfacción por parte del supervisor designado para el efecto, el informe respectivo sobre la ejecución del contrato, la certificación de los pagos a los sistemas de seguridad social integral por parte del CONTRATISTA, la factura correspondiente y los demás documentos que se requieran para tal efecto, así

	como el registro del cargue de dichos soportes en SECOP II, conforme al procedimiento e instructivos para la recepción y trámite de documentos para pago establecido por el MINISTERIO.
VALIDEZ DE LA COTIZACIÓN	90 días calendario

COTIZACIÓN ALTERNATIVA *	
Detallar: CUANDO COMPRENDA VARIOS ÍTEMS, SE DEBE COTIZAR INDIVIDUALMENTE CADA UNO	**VALOR UNITARIO**
VALOR TOTAL (incluido IVA)	

Agradecemos se sirva remitir la información respectiva a más tardar el día **12 DE SEPTIEMBRE DE 2025**, a través de correo electrónico **invtecnologia@minhacienda.gov.co o claudia.grisales@minhacienda.gov.co** a la siguiente dirección: Carrera 8 No. 6C-38 de la ciudad de Bogotá a nombre de la Dirección de Tecnología del Ministerio de Hacienda y Crédito Público.

La presente solicitud de información a cotizar fue elaborada por la Dirección de Tecnología del Ministerio de Hacienda y Crédito Público.

HUERTAS ORTIZ DIEGO FERNANDO
Firmado digitalmente por HUERTAS ORTIZ DIEGO FERNANDO
Fecha: 2025.09.10 11:08:54 -05'00'

DIEGO FERNANDO HUERTAS ORTIZ
Director de Tecnología

Anexos:

Anexo No. 1 REQUERIMIENTOS TECNICOS Y OBLIGACIONES MINIMAS
Anexo No. 2 COTIZACION ECONÓMICA
Anexo No. 3 INFORMACIÓN ADICIONAL

Proyectó	Claudia Marcela Grisales Mateus – Técnico Operativo – Dirección de Tecnología	
	Luis Orlando Arenas Ruiz – Asesor Despacho Dirección de Tecnología	
Revisó	Laura Duran – Despacho ¨Dirección de Tecnología	
Asesoría jurídica contractual por:	Julio Nelson Valderrama	Aprobado vía correo electrónico el 23 de julio de 2025.

ANEXO No.1

REQUERIMIENTOS TÉCNICOS Y OBLIGACIONES MÍNIMAS

1	**TERCERIZACIÓN DE SERVICIOS DE SEGURIDAD** **1.1 DESCRIPCION DEL SERVICIO** **1.1.1 Servicios tercerizados de SOC (Security Operation Center por su sigla en inglés o Centro de operaciones de seguridad):** Incluye los servicios de monitoreo, diagnostico, generación de alertas y recomendaciones ante un evento de seguridad o un posible evento de seguridad. Comprende: Monitoreo y correlación de eventos sobre la infraestructura definida por la entidad, haciendo uso de plataformas de correlación de última generación que permita por medio de tecnologías escalables que puedan ofrecer análisis de seguridad inteligente e inteligencia frente a amenazas, de forma que proporcione una solución para la detección de alertas, la visibilidad de amenazas, la búsqueda proactiva y la respuesta amenazas, hacer analítica y explotación de Datos con la finalidad de tener escenarios predictivos de amenazas que permitan a la entidad ser proactivo ante un incidente de seguridad. Abarca: • Debe prestarse 7x24x365 (Siete días a la semana, veinticuatro horas al día, trescientos sesenta y cinco días al año), incluye días festivos, y fines de semana, con analistas de seguridad y un líder de servicios SOC, con un esquema de escalamiento de incidentes. • Deben gestionarse las **alertas** e **incidentes**, 7x24x365, a través del SOC y articulada con el Centro de Servicios Tecnológicos de la entidad, disponiendo de una herramienta de gestión de servicios, donde se utilice para dar de alta incidentes y realizar un seguimiento sobre ellos, permitiendo la recepción y registro de eventos e incidentes, realizando un análisis preliminar de los mismos, consistente, como mínimo, de las siguientes actividades: a) Investigación: Quién, Qué, Cómo, Cuándo, Dónde y Por

Qué
b) Clasificación: Evento, Incidente
c) Categorización: Ataque Informático, Código Malicioso, Falla,
d) Vulnerabilidad
e) Correlación: Hosts, Red
f) Valoración: Alto, Medio, Bajo
g) Elaboración, entrega y seguimiento del plan de trabajo para
h) Investigación, Contención, Erradicación, Recuperación, Prevención y Comunicados a eventos e incidentes
i) Seguimiento de Eventos e incidentes desde la creación hasta el cierre

- Debe monitorear, identificar y notificar alertas de vulnerabilidades que puedan derivar en incidentes de seguridad que afecten a la infraestructura de sistemas, redes o servicios del Ministerio de Hacienda. Lo anterior de acuerdo con esquema de escalamiento definido por el Ministerio.

- Debe soportar la toma de decisiones en caso de identificarse que la infraestructura del Ministerio de Hacienda pueda estar sujeta a una amenaza, vulnerabilidad o ataque.

- Gestión avanzada de incidentes, medición de impacto, generación de planes de acción que debe ser utilizada por el personal interno del SOC para establecer un sistema experto de tratamiento de los incidentes, donde se realiza la caracterización, se cataloga por taxonomía interna y se diseña el plan de acción adecuado.

- Se debe proveer la visualización del inventario de activos con la información detallada tanto en formato texto como en grafo, aportando una visión global del inventario y sus relaciones. El inventario de activos será monitoreado de manera automática y continua, de forma tal que en caso de detectarse una modificación de un activo, esta será alertada para verificarse si es un cambio autorizado.

- Se deben entregar informes periódicos (por lo menos mensual) con los reportes históricos de monitoreo y gestión de alarmas realizadas.

- Debe tener la posibilidad de integrarse o exportar información de incidentes a la herramienta gestión de incidentes, requerimientos y cambios utilizada por el Ministerio.

- El proveedor de los servicios de SOC deberá contar con mínimo DOS (2) centros de datos, el principal de los cuales debe estar ubicado en la ciudad de Bogotá; el otro debe ser de contingencia y puede estar ubicado en otra ciudad de Colombia o en otro país.

  Cabe aclararle que excepcionalmente se acepta el centro en otro país siempre que se garanticen el cumplimiento de la normatividad colombiana en materia de seguridad, disponibilidad y protección de la información, así como la posibilidad de realizar auditorías y controles por parte de la Entidad.

1.1.2 GESTIÓN Y ANÁLISIS DE VULNERABILIDADES, COMPRENDE:

a. **Análisis de Vulnerabilidades:** Se debe realizar de acuerdo con las necesidades del MHCP durante la vigencia del contrato sobre una cantidad de 1000 IP´s correspondientes a componentes de la infraestructura computacional y sobre los activos que el Ministerio considere críticos y/o que soporten servicios esenciales de la entidad; el análisis debe realizarse de forma permanente y persistente.

   Se aclara que el análisis de vulnerabilidades y los activos críticos definidos por la entidad podrá ejecutarse de manera **remota** o **presencial**, de acuerdo con las necesidades, condiciones técnicas y políticas de seguridad que establezca la entidad durante la vigencia del contrato.

b. Red Team: se debe realizar periódicamente (por lo menos una vez durante la ejecución del contrato), sobre una cantidad de 10 aplicaciones y/o IP correspondientes a componentes de la

	infraestructura del Ministerio. Sobre los activos que el Ministerio considere críticos o que soporten servicios esenciales de la entidad c. Realizar análisis en profundidad de incidentes, ataques, las tácticas, técnicas y procedimientos generando defensas mientras se lleva a cabo el análisis, lo cual permite una protección continua para toda la arquitectura en tiempos mínimos. Se debe contar con indicadores de Compromisos (IOC´s), actualizados diariamente. d. Servicios de inteligencia avanzado que cuente con Indicadores de Compromisos (IOC´s), actualizados diariamente**.** Debe generar acciones para prevenir ataques, apoyándose en la generación de PLAYBOOKs para incidentes de categoría Global. e. Tener la funcionalidad de Análisis Inteligente de Vulnerabilidades integrado con referencias como CVE, CPE y exploits, donde realice auditoria de vulnerabilidades de forma pasiva. f. Tener la capacidad de realizar escaneos a diferentes niveles y con diferente impacto (pasivo y activo), el cual se encargará de establecer las plantillas de sistemas autorizados y sobre la misma detectar intrusos y/o modificaciones estructurales sobre el activo, como cambio de puertos abiertos, etc. y la capacidad de examinar si existen exploits públicos, privados, pruebas de concepto o desarrollo de evaluación que puedan materializar la amenaza de una forma aplicada y sencilla. g. Se deben entregar informes periódicos (mínimo una vez por mes), o sobre demanda a través del supervisor del contrato, con la descripción del trabajo realizado, metodologías y lineamientos utilizados, resumen de las actividades realizadas, matriz de vulnerabilidades y hallazgos, recomendaciones y conclusiones h. Se debe entregar la capacidad crítica del SOC, tras tener desplegadas las capacidades de visión estratégica de seguridad, descubrimiento de amenazas y vulnerabilidades, y gestión centralizada de seguridad a través de la gestión de eventos de seguridad, se deberá incluir la capa de respuesta ante incidentes, donde un grupo de expertos del proponente tendrá que analizar todos aquellos eventos escalados como incidentes, realizando actividades de análisis, como forense, reversing de malware,

análisis de tráfico entre otras, para el correcto modelado de la amenaza y el diseño de los planes de tratamiento, que serán los que marcarán las pautas y acciones a seguir para responder ante la amenaza gestionada, estos planes tendrán que estar englobados en las siguientes categorías, planes de identificación, prevención, contención, remediación y recuperación

i. Disponer de un servicio CSIRT que permita disponer de expertos de seguridad y ciberseguridad en caso de requerirlo.

1.1.3 ETHICAL HACKING Y SERVICIO DE ANÁLISIS DE VULNERABILIDADES

Se debe realizar de acuerdo con las necesidades del MHCP un (1) evento durante la vigencia del contrato sobre una cantidad de 10 aplicaciones y/o IP correspondientes a componentes de la infraestructura y sobre los activos que el Ministerio considere críticos o que soporten servicios esenciales de la entidad.

1.1.4 SERVICIO DE ANÁLISIS FORENSE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Este servicio deberá ser ejecutado de forma integral y bajo un modelo metodológico reconocido internacionalmente que deberá ser presentado y aprobado por el MHCP.

El servicio de análisis forense de incidentes de seguridad de la información deberá estar en capacidad de reconstruir lo que haya sucedido tras un incidente de seguridad, determinando quien, desde donde, cómo, cuándo y que acciones ha llevado a cabo el intruso en los sistemas afectados por el incidente de seguridad.

1.2 CARACTERISTICAS DEL SOFTWARE DE LA ENTIDAD

El proveedor deberá integrar las herramientas que actualmente tienen licenciadas por el MHCP, y que se encuentran en servicio a saber:

1. **PAM:** (Privileged Access Management) - CyberArt es una solución para la gestión de accesos con privilegios. Permite proporcionar privilegios muy delimitados para los perfiles de usuario que se definan. Licenciamiento: 93 cuentas y versión: (12.2.2)

	2. **VISION ONE**: Trend Micro Vision One recopila y correlaciona datos de actividad profunda en múltiples vectores de XDR. Licenciamiento para 2.100 usuarios, versión 2025. 3. Solución para aseguramiento de la plataforma de comunicación corporativa (solución de protección para Gsuite, Office365, One Drive y SharePoint On Line), marca Trend Micro versión 2025.
2	**2.1 ACTIVACION DEL SOC:** El contratista deberá realizar la activación (por 9 meses) del servicio SOC de la solución descrita en el numeral 1 (ADMINISTRACION Y OPERACIÓN SERVICIO DEL SOC) y realizar la implementación inicial de la plataforma. De lo anterior se generará un certificado de activación del soporte, el cual deben ser entregado al supervisor del contrato, en los primeros diez (10) días siguientes a la aprobación de la garantía.
3	**3.1 ACTIVIDADES DE INICIO DEL CONTRATO:** Con el objetivo de implementar el servicio de SOC, el contratista deberá realizar el levantamiento de la información requerida para la configuración, implementación y funcionamiento de la solución SIEM y/o los dispositivos recolectores (sensores), para lo cual el MHCP brindará la colaboración y la asesoría respectiva. El contratista deberá realizar las siguientes actividades dentro de los diez (10) primeros días siguientes a la aprobación de la póliza: **3.1.1 Actividades del Servicio** • Inicio del contrato - Kick Off • Entrega de la documentación de los procesos solicitados del servicio del SOC • Entrega de la documentación del equipo de trabajo • Personalización de la arquitectura propuesta. • Plan de trabajo y autorización de la implementación por parte del MHCP. **3.1.2 Integración y Puesta en Marcha (actividades)** • Configuración y conexión de dispositivos, ajustes técnicos, estabilización de la plataforma tecnológica.

	• Definición de la integración de logs de los equipos, dispositivos y bases de datos definidas por el MHCP, que incluya prueba, configuración y conexión. • Creación, prueba y afinamiento de las tareas requeridas por el MHCP. **3.1.3 Monitoreo (actividades)** • Generación de alertas, notificaciones, reportes. Indicadores de gestión de incidentes y escalamientos. • Configuración del tiempo máximo de notificación de alertas, incidentes de seguridad o actividades sospechosas (severidad alta, media y baja) • Definición y configuración de los medios de notificación: teléfono, celular, herramienta de mesa de ayuda, chat, correo electrónico. • Definición y configuración del tiempo máximo de generación y envío de informes de servicio mensual o los periodos acordados para la entrega de los mismos según las necesidades del MHCP. **3.1.4 Mantenimiento (actividades)** • Revisión del control de cambios, mejoras, actualizaciones y soporte. • Integración de nuevos dispositivos • Generación de reportes técnicos con recomendaciones de mejoramiento de la infraestructura tecnológica del MHCP. **3.1.5 Entrega de Configuración al MHCP** • El proveedor deberá entregar al MHCP todas las configuraciones realizadas en la infraestructura tecnológica durante la implementación del servicio de SOC Una vez finalizadas las actividades de inicio del contrato, entregar al supervisor del contrato un informe que consolide las actividades y resultados de las acciones ejecutadas.
4	**4.1 SERVICIO:** El servicio de gestión de SOC consiste en el tratamiento de eventos, identificación y atención de incidentes, los cuales contaran con un conjunto de metodologías y procesos que permitirá brindar respuesta oportuna a los riesgos y amenazas que afrontan el MHCP.

Por incidente se entenderá todas las eventualidades que generen problemas técnicos como fallas, daños, degradación del desempeño, mal funcionamiento o anomalías que se presentan en la plataforma y que impidan que esta cumpla con su óptimo desempeño.

4.1.1 Especificaciones Técnicas Generales para la prestación de servicio.

- El contratista deberá prestar el servicio en el idioma español, para la interacción de las áreas de operación.
- El contratista deberá contar con certificación ISO 27001 con antigüedad mínima de 7 años, esta certificación debe incluir dentro de su alcance los servicios asociados a este proceso y como mínimo debe estar certificado en procesos de monitoreo de activos y/o eventos de seguridad y/o correlación de eventos y/o monitorización de eventos de seguridad.
- El contratista debe ser miembro activo de FIRST con una antigüedad mínima de 5 años, para esto debe presentar certificado de afiliación a FIRST.
- El contratista deberá estar en la capacidad para el servicio de SOC de desarrollar los conectores y/o API necesarios para las integraciones con las fuentes de datos. Desarrollando un máximo de 10 conectores.
- El contratista suministrará al Ministerio de Hacienda y Crédito Público, mediante la modalidad de servicio, la totalidad de elementos de software, motores de bases de datos y demás requeridos para soportar el correcto funcionamiento de los servicios de monitoreo de los dispositivos informáticos de la infraestructura tecnológica del MHCP.
- El contratista deberá contar con una capacidad operativa y de soporte de fabricantes 7x24x365, durante toda la ejecución del contrato.

	• El contratista deberá certificar la evaluación de antecedentes para los contratistas o usuarios de terceras partes que interactúen con el SOC. • El contratista deberá realizar periódicamente, según lo establezcan las mejores prácticas, análisis de tendencias sobre los eventos y plataformas monitoreadas. • El contratista deberá proporcionar reportes bajo solicitud del Ministerio de Hacienda y Crédito Público, por demanda. • El contratista deberá contar con un informe detallado sobre alertas mundiales que puedan afectar la seguridad sobre la infraestructura. • El contratista deberá prestar el servicio de administración, operación y soporte de toda la infraestructura de hardware y software implementada para el servicio. • El contratista deberá monitorear los componentes de la infraestructura tecnológica implementada para el servicio de forma proactiva mediante herramientas de gestión. • El contratista deberá realizar los mantenimientos preventivos y correctivos adecuados para asegurar la continua disponibilidad e integridad de la infraestructura del servicio. • El contratista deberá garantizar y contar con controles de acceso a los repositorios de información que sean necesarios para el Ministerio de Hacienda y Crédito Público gestionados y evitar el acceso no autorizado. • El contratista deberá contar con procesos de eliminación segura de la información que ya no se requiera. • El contratista deberá tener un SOC propietario, en la ciudad de Bogotá. • El contratista deberá prestar su servicio con la solución de Security Information and Event Management SIEM la cual deberá estar como líder en el cuadrante Mágico de Gartner.

- Para la ejecución del contrato y el cumplimiento de los niveles de servicio solicitados, el contratista dispondrá del talento humano que el considere necesario; sin embargo, debe incluir un profesional que certificado de entrenamiento en la herramienta SIEM con que el SOC presta el servicio y además un profesional que cuente con alguna de las certificaciones:

  - ✓ Especialización en Auditorías de Sistemas o
  - ✓ Lead auditor ISO 22301:2019 o
  - ✓ ISO 27001:2022 Certified Lead Implementer o
  - ✓ Auditor Interno ISO 27001:2022 o
  - ✓ Lead Risk Manager ISO 31000:2018+ISO 27005:2022.

- El contratista deberá contar con personal certificado en la herramienta SIEM con que el SOC presta el servicio de monitoreo, correlación y demás.

- El contratista deberá tener los roles y responsabilidades del grupo de operaciones del SOC, claramente definido, en lo que respecta al monitoreo, correlación, análisis y tendencias de seguridad y atención de requerimientos, manejo y contención de incidentes de seguridad, inteligencia de la amenaza y hunting.

- El contratista deberá detallar los procesos de: Gestión y Respuesta a incidentes, atención y escalamiento de requerimientos, Mejora Continua del servicio.

4.2 Especificaciones Técnicas Generales del SOC

- El SOC debe estar en capacidad de colectar, procesar, monitorear y correlacionar los eventos para el escalamiento y determinar si corresponde a un evento de seguridad, tendencias, falsos positivos, patrones o firmas de intruso las cuales deberán ser notificadas y documentadas.
- El servicio de SOC debe contar con capacidades de HUNTING con el fin de encontrar amenazas desconocidas.
- El servicio de SOC debe estar en la capacidad de realizar

	monitoreo de disponibilidad y estado de los dispositivos integrados al servicio de monitoreo de seguridad. • El servicio de SOC deberá tener la capacidad en tiempo real para detectar, recolectar, cruzar y consolidar patrones sobre la información recolectada, con el objeto de poder tener una alerta temprana de los problemas, brindando priorización a los activos más importantes. • El SOC deberá realizar análisis del comportamiento de la infraestructura administrada y monitoreada para correlacionar incidentes y determinar proactivamente problemas en la operación. • El SOC deberá garantizar la disponibilidad, confidencialidad, integridad, autenticación, autorización, no repudio, auditoría y privacidad de los datos y servicios soportados. • El SOC deberá contar con un grupo interdisciplinario interno para la atención de incidentes, bajo un procedimiento claro y definido. • El servicio de SOC deberá contar con la alianza de un CERT. • El servicio del SOC deberá permitir la integración del envío de alarmas automáticas vía correo electrónico. • El servicio SOC deberá contar con tecnologías cognitivas como inteligencia artificial para realizar el proceso de investigación de potenciales incidentes de seguridad, dicha inteligencia artificial deberá analizar mensajes de Twitter, información de foros, boletines de seguridad, artículos, wikis, presentaciones de conferencias, reportes de analistas y bases de conocimiento. El proveedor deberá explicar cómo se cumple este punto y si está integrado a la solución y/o requiere de consolas de gestión adicionales. • El servicio de SOC deberá integrase con LDAP (Protocolo Ligero de Acceso a Directorios). • El SOC deberá contar con la capacidad de asegurar la generación, almacenamiento mínimo de nueve (9) meses y potencial recuperación de respaldos de las configuraciones de todas las plataformas involucradas en el servicio. • El servicio de SOC deberá ser compatible con los métodos de recopilación de logs de la industria (Syslog, WMI, JDBC y SNMP). • Los componentes que realizan la recolección de eventos deberán tener la capacidad de enviar los datos a múltiples destinos primarios de forma simultánea.

	• El servicio de SOC deberá estar en capacidad de realizar el análisis de la infraestructura del MHCP en tiempo real de los eventos. • El servicio de SOC deberá estar en capacidad de almacenar y conservar tanto los eventos normalizados como el original en bruto para fines forense mínimo por un periodo de seis 6 meses. • El servicio de SOC deberá estar en la capacidad de soportar la configuración en alta disponibilidad en un modo integrado y sin la necesidad de software adicional de terceros. • El servicio de SOC deberá contar con un portal web que le permita al MHCP tener una visualización de la información relevante respecto a amenazas emergentes, vulnerabilidades en su infraestructura e incidentes de seguridad detectados. Dicha información deberá mostrar la información a nivel de monitoreo, investigación, atención de incidentes y gestión de requerimientos y permitir descargar la información. • El servicio de SOC deberá estar en capacidad de gestionar procesos automatizados de respuesta a incidentes y revisión de actividades anómalas. • El servicio de SOC deberá estar en capacidad de gestionar procesos automatizados de primer nivel en análisis de phishing y malware. • El servicio de SOC debe estar en la capacidad de identificar un evento de seguridad cuando ocurra o está en suceso y relacionarlo en forma directa o indirecta con otros eventos de seguridad asociados. Estos, constituyen el conjunto de eventos que permite determinar el patrón de ataque, conformando eventos correlacionados. • Se requiere que el servicio evalúe la exposición y riesgo digital del Ministerio de Hacienda y emitir un rating dinámico (KPI) que permita conocer, en tiempo real, el estado de seguridad digital. El rating (Score) deberá ser multivector y contener los elementos clave de afectación, evaluando desde todos los puntos de vista. • Adicional se requiere que permita la elaboración de planes estratégicos de actuación en cada uno de los puntos para elevar la madurez de la seguridad. El Score y su desglose pueden ser presentado en comités de dirección para mostrar el estado de los planes estratégicos de mejora en la seguridad de la información y su impacto real sobre la misma. • Debe ser dinámico y realizar la evaluación periódicamente

	conforme se desarrollan las medidas de mejora con lo cual se puede evaluar y demostrar su eficacia. Identificar potenciales amenazas de seguridad y la capacidad del Ministerio de Hacienda de prevenirlas o limitar su impacto, evitando de esta manera ataques que puedan comprometer el funcionamiento de los servicios del Ministerio de Hacienda. Para esto, el contratista debe abordar diferentes trabajos en paralelo con base a tres perspectivas de riesgo: estratégico, táctico y operativo. El resultado de las tres líneas de acción se deberá agregar para determinar los gaps de cumplimiento entre el estado actual y el objetivo deseado, en relación con el apetito al riesgo del Ministerio de Hacienda, el alineamiento con entidades similares y/o del sector y las tendencias de misionalidad. Se deben realizar actividades de inteligencia "actual" y "prospectiva", esta última con la intención de prever posibles amenazas y neutralizarlas de forma preventiva. El Ministerio de Hacienda requiere que el servicio pueda contar como mínimo con las siguientes actividades: • Análisis de prospectiva que combinen el análisis de inteligencia con la metodología de gestión de riesgos. • Uso de herramientas propias de investigación y metodología de inteligencia. • Informes teniendo en cuenta la estrategia e intereses del Ministerio de Hacienda. • Enfoque de los escenarios que aporta un componente diferencial de aspectos geopolíticos y estratégicos según criterios del proponente. • Durante el servicio se deberán aportar modelos y patrones de detección preventiva que protegerán la infraestructura y sus activos de las amenazas descubiertas y analizadas **4.2.1**. Los objetivos planteados por el Ministerio de Hacienda para este servicio es la proporción de la información disponible sobre la entidad que pueda resultar en un evento de ciberseguridad. Por esto, el principal objetivo es contar con la notificación en el tiempo y forma oportuna para la identificación de amenazas, respuesta ante incidentes y protección de los recursos digitales más expuestos. Para la consecución de este objetivo principal, se han establecido los

	siguientes objetivos específicos: • Identificación y parametrización de los activos a monitorizar. • Monitorización y selección de las amenazas que afectan al Ministerio de Hacienda • Generación de alertas de incidentes en caso de detección de fuga de datos, exposición de credenciales o manipulación de dominios asociados a el Ministerio de Hacienda • Análisis de las amenazas más complejas y de la totalidad de las amenazas identificadas para mejor entendimiento del panorama de seguridad. • Priorización de las amenazas de mayor riesgo (impacto + probabilidad) hacia el Ministerio de Hacienda • Evaluación geográfica y sectorial del panorama de amenazas para mejor comprensión del posicionamiento del Ministerio de Hacienda en términos de ciberseguridad con respecto a otras entidades gubernamentales. **4.2.2** El servicio deberá contar con una base metodológica del Ciclo de Inteligencia desplegada en sus cuatro fases Planificación, Obtención, Análisis y Difusión, que permita al Ministerio de Hacienda: • Generar inteligencia regional específica. • Traducir la inteligencia global en inteligencia operable. **4.2.3**. Para la operación del servicio el proponente deberá aportar como mínimo las siguientes fuentes según su categoría: • Más de 300 fuentes OSINT. • Más de 500 fuentes Darknet/ Deep Web. • Fuentes de ciberamenazas (APT, Malware, IOC, etc.) de un sector a nivel mundial. • Fuentes de intercambio privilegiado con artefactos de incidentes. • Fuentes de inteligencia agregada (Cyber Threat Alliance). **4.2.4**. El Ministerio de Hacienda requiere en el servicio capacidades en vigilancia digital con el siguiente alcance: El servicio de vigilancia digital deberá desarrollar un proceso activo de identificación y seguimiento a las posibles amenazas, y/o de incidentes

	concretos de ciberseguridad que se originan en los entornos digitales de internet la pública y la denominada "internet profunda", como una estrategia efectiva para anticipar posibles acciones que pueden afectar los intereses del Ministerio de Hacienda. Se requiere un servicio de monitorización sobre los contenidos públicos, ocultos y sobre aquellos que no sean legítimos, con un enfoque claro y orientado a la detección de amenazas incluido Phishing. A continuación, se detallan los tipos de activos incluidos en el servicio: • Tipos de activos: • Dominios corporativos (Ministerio de Hacienda) • Marcas • Apps / productos digitales de la organización • Identidades digitales y VIP's • Información confidencial digital El servicio de vigilancia Digital debe contar con un número ilimitado de Takedowns - eliminación de dominios maliciosos y de phishing sin importar su ubicación. Ejemplos de activos a monitorizar: Usuarios, Marcas, Dominios, Productos, Servicios, Páginas web, Aplicaciones móviles, Servidores/Servicios, Direcciones de correo, Personal VIP, Redes sociales, Portales de empleo, Distribuidores y puntos de venta autorizados, Grupos de interés conocidos. **4.2.5.** El servicio deberá contar con una Plataforma de ámbito Global con fuentes de Información y disponer de un amplio conjunto de fuentes de información (>10.000) entre las que se encuentran: fuentes abiertas (fabricantes, comunicaciones de amenazas públicas, etc.) como fuentes específicas y sectoriales (banca, talcos, industria), las herramientas también deberán realizan búsquedas en la deep web y DarkNet (en foros, markets, etc.) permitiendo tener una visión agregada de la exposición de la entidad a nivel global **4.2.6**. Los servicios de Cyber Threat Intelligence deberán ofrecer un conjunto de beneficios basados en la prevención y detección, reputación e inteligencia. La finalidad principal es la investigación de incidentes que afecten a el Ministerio de Hacienda, bien por la exfiltración de información y/o por ser target de algún ciberataque.

	Prevención / detección / respuesta a fugas de información: • Credenciales de empleados y usuarios del entorno digital. • Información confidencial / propiedad intelectual. • Detección de planes de robo / ciberataques (phishing) • Protección de la Marca / Reputación: • Detección (en fuentes digitales públicas) de falsificaciones, piratería, comercialización ilegal, etc. • Detección de contenidos publicados en las redes sociales sobre marcas, productos o colaboradores VIP, que pudiesen generar situaciones de crisis o erosión del negocio. • Inteligencia y Seguridad Corporativa: • Identificación (en fuentes digitales públicas) de amenazas generales sobre la compañía, empleados o sus operaciones físicas. • Priorización y adaptación • Identificación de las principales amenazas • Claridad y concisión a la hora de transmitir las prioridades para una mejor toma de decisiones • Adaptación a las necesidades del Ministerio de Hacienda en cuanto al servicio **4.3 Requerimientos Específicos – Correlación y Alertamiento de Eventos de Seguridad** • El contratista deberá basado en su experiencia y bases de conocimiento diseñar el modelo de recolección de LOGs y arquitectura del servicio, con el objetivo de ser monitoreados y se tenga en cuenta al menos los eventos más relevantes de seguridad y no impacte la infraestructura del Ministerio de Hacienda y Crédito Público. • El contratista y el Ministerio de Hacienda y Crédito Público deberán definir una serie de reglas, alertas y notificaciones clasificadas y priorizadas para detectar eventos e incidentes sobre la infraestructura tecnológica que se está monitoreando y reportarlas al MHCP cada vez que se encuentre en riesgo los principios de integridad, disponibilidad o confidencialidad de los activos tecnológicos. • El servicio de SOC deberá analizar, detectar y reportar ataques reales y potenciales a la infraestructura del MHCP y mantener la trazabilidad y detectar los comportamientos anómalos.

	• El servicio de SOC deberá estar en la capacidad de generar alertas identificadas en los reportes de análisis de tendencia de centros internacionales SIRT/CERT o en bases de datos de conocimiento del proveedor, basado en los casos detectados a otros clientes que tenga el servicio ofrecido.
	• El contratista deberá establecer el protocolo para informar, reportar y/o escalar los eventos, alertas e incidentes que se detecten.
	• El contratista deberá informar al MHCP de manera prioritaria y alertar sobre los cambios de seguridad, de configuración y críticos que se generen en la infraestructura del MHCP estableciendo para ello una tabla de alertas, prioridad, tiempos y escalamiento.
	• El contratista y el MHCP deberán definir los tipos de reglas, alertas y notificaciones enfocados a los eventos relevantes de seguridad. Las alertas mínimas requeridas deberán monitorear eventos como:
	  • Actividades asociadas a la administración de cuentas de usuario final (UserID)
	  • Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores (root, sa, administrator).
	  • Ejecución de comandos especiales sobre los sistemas operativos
	  • Ejecución de comandos especiales sobre las bases de datos (dump, drop, delete, insert, update).
	  • Cambios de parámetros técnicos, de configuración o de seguridad.
	  • Cambios de configuración horaria.
	  • Cambios no autorizados en recursos tecnológicos críticos
	  • Actividades de conexión de cuentas de usuario final o administradores.
	  • Actividades asociadas a manipulación de bitácoras técnicas (LOGs) o interrupciones en el envío de los LOGs.
	  • Actividades asociadas a conexión de acceso remoto.
	  • Actividades asociadas a la no efectividad de controles en el ejercicio del monitoreo transaccional
	• Los canales de comunicación se centralizarán en la ciudad de Bogotá y el proveedor será el encargado de dimensionar, diseñar, adquirir, instalar, configurar, operar y administrar la arquitectura tecnológica del servicio de monitoreo.

	• El contratista con la aprobación del MHCP deberá definir el modelo de conexión de los dispositivos que serán monitoreados; especificando los requerimientos técnicos para cumplir con el servicio a contratar; apoyar y soportar al MHCP en la conexión, configuración y activación de las conexiones técnicas de los dispositivos a monitorear. • El enlace o canal de comunicación entre el MHCP y el contratista será por una conexión por VPN (Red Privada Virtual) cifrada y segura de acuerdo con el dimensionamiento del servicio contratado. • La arquitectura de la solución SOC propuesta por el proveedor no deberá impactar la disponibilidad de los activos tecnológicos CORE del MHCP, no de la infraestructura crítica que lo soporta. Por lo tanto, el servicio de monitoreo y respuesta a eventos de seguridad de la infraestructura informática deberá estar basado en soluciones SIEM internacionalmente reconocidas, separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática para no impactar la normal operación del MHCP. • El servicio de SOC deberá estar en capacidad de ofrecer a través de sus herramientas, las siguientes funciones: a. Análisis de comportamiento b. Análisis de vulnerabilidades c. SIEM d. Detección de Amenazas • El servicio de SOC deberá mantener sincronizados todos los relojes de las herramientas de monitoreo con la hora legal para Colombia, suministrada por la Superintendencia de Industria y Comercio. • El contratista deberá realizar un monitoreo a los análisis de tendencia de amenazas y riesgos disponibles en internet o en centros de respuesta a incidentes (COLCERT) que permita informar al MHCP alertas, tendencias, ataques y amenazas provenientes desde el ciberespacio y pueda afectar la infraestructura tecnología o los servicios del MHCP. Así mismo, el proveedor deberá disponer de servicios de inteligencia ante Ciber Amenazas. A continuación, se detalla la visión de actividades por desarrollar por parte del proponente en el proceso establecido de las capacidades de Monitorización y Respuesta Ante Incidentes.

4.4 Especificaciones Técnicas Generales Herramienta SIEM con Inteligencia Artificial.

La Entidad tiene como objetivo adquirir como servicio una plataforma integrada de próxima generación especializada en la detección, investigación y respuesta ante amenazas de seguridad cibernética.

Las funciones principales y capacidades mínimas esperadas de la plataforma son:

a) Recopilación de Datos Amplia: Capacidad de recopilar datos de diversas fuentes, tanto en entornos locales (on-premise) como en la nube.
b) Análisis Eficiente de Datos: Habilidad para analizar los datos recopilados de manera eficiente, extrayendo inteligencia de seguridad relevante.
c) Almacenamiento Seguro de Datos: Garantía de almacenamiento seguro de la información, protegiendo su integridad y confidencialidad.
d) Búsquedas de Alta Velocidad: Ofrecer capacidades de búsqueda rápidas sobre los datos almacenados.
e) Lenguaje de Búsqueda Flexible: Utilizar un lenguaje de búsqueda natural y no propietario, facilitando la interacción de los usuarios.
f) Generación de Informes de Cumplimiento: Permitir la creación de informes detallados orientados al cumplimiento normativo y regulatorio.
g) Paneles de Control (Dashboards): Proporcionar paneles de control personalizables y fáciles de usar para facilitar la supervisión, el monitoreo continuo y la toma de decisiones estratégicas y operativas.

4.5 Funcionalidades Mínimas Requeridas

- La plataforma debe implementarse como un servicio (SaaS) proporcionando desde el origen el envío seguro, la compresión y el cifrado de datos. La entidad no aceptará soluciones basadas en software libre que carezcan de respaldo y soporte por parte de un fabricante reconocido en el mercado. Además, se requiere que los proveedores estén posicionados como líderes en el

	Cuadrante Mágico de Gartner para SIEM durante al menos 4 años consecutivos. • La plataforma deberá facilitar la documentación dentro de los incidentes, recreando de manera automática cadenas de ataques completas y reconstruyendo el comportamiento de usuarios y dispositivos. Además, deberá utilizar el marco de trabajo internacionalmente reconocido MITRE ATT&CK para identificar de forma proactiva las amenazas. • La plataforma debe tener la capacidad de tener casos de uso requeridos mediante el uso de analítica de seguridad incluirán: Malware, Phishing, Ataque de Fuerza Bruta, Ransomware, Cryptomining, Credenciales Comprometidas, Movimiento Lateral, Escalación de Privilegios, Actividad Privilegiada, Manipulación de Cuentas, Exfiltración de Datos, Evasión, Fuga de Datos, Abuso de Acceso Privilegiado, Manipulación de Auditoría, Destrucción de Datos, Seguridad Física, Protección de la Fuerza Laboral, Autenticación y Acceso Anormal. Estos casos deben estar preconfigurados y disponibles sin necesidad de desarrollo adicional. • La plataforma debe tener la capacidad de respuesta automatizada a incidentes de seguridad debe incluir 'playbooks' llave en mano que permitan la automatización de incidentes relacionados con phishing, malware, indicadores de compromiso (IoC) y desvinculación de empleados. • La plataforma deberá integrarse con productos líderes en seguridad y ofrecer al menos 600 acciones de respuesta automáticas o semiautomáticas. Esto permitirá a los analistas emplear acciones repetibles, reduciendo así el tiempo de respuesta y mejorando la eficiencia. **4.5.1 Características Requeridas e Indispensables** • La plataforma debe estar certificada por lo menos en SOC 2 tipo II, ISO 27001, 27017, 27018 y GDPR para asegurar que los controles de seguridad mantendrán la información almacenada de forma segura y manteniendo la privacidad. • La plataforma debe garantizar por lo menos un nivel de servicio de 99.9% en carga de datos a la nube y 99.5% en disponibilidad de acceso al producto y en caso de no ser cumplidos se deberán de asignar créditos a la solicitante. • La consola deberá desplegarse de manera segura mediante

	protocolo HTTPS y deberá tener un acceso centralizado a todos los componentes de la plataforma. • La plataforma debe tener la capacidad de mostrar el estado de salud y licenciamiento dentro de la misma interfaz web. • La plataforma debe ofrecer informes visuales sobre el estado de la licencia para controlar la ingesta de datos y facilitar la toma de decisiones basadas en la capacidad contratada. • La plataforma debe contar con actualizaciones por parte del fabricante, con la finalidad de para mantener tanto el contenido, como las capacidades en la última versión, estas actualizaciones no requerirán involucramiento del equipo del solicitante. • La plataforma debe crear alertas sobre el estado de salud en el que se encuentran sus componentes siendo capaz de enviarlas vía mail. • La plataforma debe notificar y resolver cualquier falla del sistema de manera independiente sin involucramiento del equipo solicitante. • La plataforma debe permitir la creación de usuarios locales y externos utilizando una solución de SSO a través de SAML 2.0, y deberá soportar control acceso basado en roles (RBAC). • La plataforma deberá contar con la función de restringir datos a usuarios y roles específicos para mantener el control de la información que cada uno de ellos puede visualizar y acceder. • La plataforma debe tener control de acceso basado en roles (RBAC) no debe permitir IdP-initiated SAML para evitar ataques tipo Man-In- The-Middle. • La plataforma debe contar con controles de seguridad que permitan el cifrado AES-256 para los datos en reposo y forzando cifrado TLS en tránsito con TLS versión 1.2 o 1.3. • La plataforma se debe mantener actualizada constantemente en cuanto a contenido, incluyendo la normalización de eventos, acciones, integraciones, reportes, etc. • La plataforma debe contar con un módulo que proporcione visibilidad de la ingesta y procesamiento de los datos permitiendo ver los datos que llegan a la solución con el fin de asegurar que se están procesando, categorizando y enriqueciendo adecuadamente en tiempo real desde la interfaz Web. • La plataforma debe proporcionar informes sobre el estado de cobertura para identificar la eficiencia de las reglas y fuentes integradas en relación con los casos de uso y las técnicas y

	tácticas de Mitre ATT&CK. • La plataforma debe contar con al menos los siguientes logs de auditoría sobre las acciones realizadas sobre la plataforma: • Creación o Modificación de Alertas y Casos • Creación, Modificación y eliminación de APIs. • Autenticación en la plataforma • Nueva fuente de datos creada, habilitada, modificada o eliminada. • Creación, Modificación y Eliminación de tablas de contexto. • Creación, Habilitamiento, Deshabilitamiento, Modificación y eliminación de reglas. • Creación, Modificación y Eliminación de roles de usuario. • Auditoria de búsquedas realizadas, descargadas o exportadas. • Auditoria de usuarios creados, activados, desactivados, modificados, reinicio de passwords, eliminados, etc. • Dichos logs deberán ser almacenados en la misma base de datos para poder ser utilizados en búsquedas, visualizaciones, reportes, etc. • El fabricante debe contar con un portal que permita la gestión de casos de soporte de la plataforma. • El fabricante debe contar con una comunidad web que permita discutir y compartir temas de interés, tener acceso a documentación de la plataforma, webinars y material educativo. • La plataforma debe permitir la colección de eventos utilizando una máquina virtual o física de forma centralizada o distribuida geográficamente sin costo. • La plataforma debe contar con la opción para filtrar los eventos que son enviados y procesados con la finalidad de reducir la ingesta y evitar la superación del licenciamiento. • La plataforma propuesta debe colectar datos por medio de diferentes métodos, por lo menos archivos, bases de datos (JDBC/OBDC), APIs, eStreamer y syslog. • Los colectores de la plataforma deben tener la capacidad de realizar actualizaciones de forma centralizada desde la interfaz web en cuanto estás se encuentren disponibles. • La plataforma debe soporta la ingesta de syslog y en el supuesto de que los dispositivos no tengan la capacidad de enviar eventos de forma directa, deberá contar con agentes

	para Servidores Windows y/o Linux que ejecutándose de manera local pueda recopilar datos operativos y métricas del sistema. • La plataforma debe permitir la colección de datos de forma segura usando protocolos SSL, TLS para el syslog. • La plataforma debe permitir un máximo de 3.000 EPS o una ingesta diaria de 250 GB y soportar picos máximos de 3.500 EPS por 2 horas al día diarios, donde se han integrado las siguientes fuentes (sin limitarse). • La plataforma debe retener la información en la nube de 3 meses en caliente y 6 meses en frio. • La plataforma deberá contar con la capacidad de recolectar logs de soluciones IaaS, PaaS y SaaS de nube a nube, mediante colectores basados en API. • La plataforma debe ofrecer al menos 500 fuentes de datos predefinidas, como controladores de dominio, directorio activo, VPNs, alertas de seguridad, DLP, SIEMs existentes, infraestructura en nube y SaaS. • La plataforma debe de contar con normalizaciones (parseo) predefinidos para los fabricantes más importantes del mercado, estos deberán de contar con soporte para no depender de desarrollos de terceros o tiendas. • La plataforma debe contar con capacidad para la integración de nuevos dispositivos no soportados nativamente para la normalización de bitácoras a través de • una interfaz web fácil de utilizar y que cuente con un paso a paso del proceso para facilitar las tareas a los administradores. • La plataforma debe contar con una lista de indicadores de compromiso (IOC) provenientes de un proveedor líder en la industria. • La plataforma debe ser capaz de utilizar tablas de contexto personalizadas para identificar indicadores de compromiso (IOCs) que puedan ser utilizados en el contenido desarrollado. • La plataforma debe estar nativamente alineada con la matriz de ataque de MITRE (MITRE ATT&CK), lo que permitirá a los investigadores ejecutar cazas de amenazas basadas en esas técnicas. • La plataforma debe permitir la definición de los tiempos de retención desde la interfaz web.

	• La plataforma debe contar con una interfaz web que permita la consulta de la información en tiempo real, con el fin de realizar investigaciones forenses, así como identificar patrones en los datos recolectados mostrando tendencias. • La plataforma debe permitir consultas simples mediante operadores lógicos, condicionales, comodines, rangos y términos negativos sin necesidad de utilizar lenguaje complejo. • La plataforma debe permitir un método de búsqueda avanzado para usuarios con mayor manejo y conocimiento de la plataforma, incluyendo operadores de WildCards y Expresiones Regulares. • La plataforma debe permitir la construcción de búsquedas complejas mediante el uso de lenguaje natural en castellano. Por ejemplo: "Muestra el top 10 de usuarios que más veces se autenticaron en el último día en Windows, o el top 10 de las páginas más visitadas en el UTM/Proxy". Esto deberá permitir a los analistas construir búsquedas rápidas y enfocarse en posibles amenazas. • La plataforma debe de contar con la capacidad llevar al usuario entre búsquedas, reglas de correlación o tableros de control para poder generar contenido utilizando la misma consulta. • La plataforma debe contar, sumar, obtener mínimos, promedios y máximos de los eventos que se estén buscando sin necesidad de cambiar de pantalla o interfaz con la intención de hacer investigaciones numéricas y de volumen. • La plataforma debe ser capaz de exportar los datos almacenados en formato crudo o seleccionando los campos deseados, en archivos CSV. • La consola debe poder guardar búsquedas para su uso posterior y permita acceder a los eventos (logs) originales, siempre que así se requiera. Además de contar con la información previamente interpretada por la plataforma como lo son: eventos, alertas e incidentes. • La plataforma debe permitir mostrar u ocultar campos específicos cuando estamos realizando búsquedas para permitir la identificación de la amenaza. • La plataforma debe analizar y mostrar los errores en las consultas antes de ejecutarlas, para permitir a los analistas

	corregirlas fácilmente. • La plataforma debe permitir realizar búsquedas de los eventos identificados como anómalos, enriqueciéndolos con casos de uso, razones de reglas que se dispararon y las TTPs de MITRE ATT&CK. • La plataforma debe contar con un API que permita automatizar las búsquedas y la modificación de contexto. • La plataforma debe contar con tableros o dashboards que deben ser configurados sin necesidad de tener un lenguaje o código especial. • La consola de administración debe permitir contenidos de visualización basados en filtros configurables, los cuales podrán ser exportados, almacenados y compartidos con cualquier usuario cuyo perfil lo permita. • La plataforma debe permitir agregar filtros que apliquen a todas las visualizaciones del panel de control. • La plataforma debe de contar con paneles de control pre-construidos de: • Anomalías por caso de uso • Conteo de anomalías por día • Conteo de anomalías por regla • Casos abiertos por severidad • Equipo de trabajo y tipo de incidente • Métricas de desempeño de gestión de los casos y cumplimiento de al menos las siguientes normativas: NIST, HIPAA, PCI, SOX y GDPR. • La plataforma debe tener la capacidad de agrupar los tableros o dashboards para que los usuarios puedan acceder de forma sencilla a los que ellos han generado y los que han marcado como favoritos. • La plataforma debe permitir la asignación de permisos y roles a cada uno de los tableros o dashboards para restringir el acceso a la información almacenada. • La plataforma debe presentar la información en los tableros o dashboards en gráficos tipo barra, columna, línea, área, torta, burbujas, embudo, valores únicos, diagrama sankey, mapas, mapas de calor, mitre y tablas. • La plataforma debe contar con la capacidad de combinar la información recolectada con información de contexto de los usuarios y entidades, con el propósito de asignar una puntuación de riesgo, priorizar e investigar de forma

	efectiva. • La plataforma debe proporcionar acceso a los diferentes modelos de datos generados por la actividad de los usuarios y dispositivos. • La plataforma debe ser capaz de crear reglas basadas en un histograma para determinar actividades anómalas. • La plataforma debe ser capaz de modelar la información recibida en al menos 3 tipos de modelos de datos: categórico, número y "día de la semana" con el fin de crear una línea base de comportamiento tanto de usuarios como de entidades. • La consola de administración debe contar con la opción de crear listas de observación para monitorear usuarios y entidades específicos, como ejecutivos, cuentas de servicio o personal externo. Además, deberá tener la capacidad de exportar los logs a un archivo CSV cuando sea necesario. • La plataforma debe permitir una respuesta rápida y eficiente a los incidentes, proporcionando una única consola para automatizar los flujos de trabajo. • La plataforma debe contar con un componente que identifique las alertas de seguridad de otros componentes en la organización y las priorice utilizando técnicas de inteligencia artificial y aprendizaje de máquina. • La plataforma debe tener la capacidad de administrar incidentes e investigaciones de seguridad generados automáticamente o creados manualmente, proporcionando guías con acciones establecidas por los analistas de acuerdo con el caso de uso que se esté trabajando. • La plataforma debe contar con un sistema de gestión de incidentes totalmente personalizable y una interfaz intuitiva y fácil de usar para los analistas de nivel básico. • La plataforma debe permitir documentar las acciones ejecutadas durante el incidente, así como proporcionar recomendaciones posteriores. • La plataforma debe incluir el manejo de casos para responder rápidamente a los incidentes, ya sea mediante acciones puntuales por parte del analista de seguridad y a través de la automatización y orquestación de procedimientos predefinidos o "playbooks". • La plataforma debe contar con "Playbooks" predefinidos para la automatización de los incidentes más comunes de la

	organización, como alertas de malware, incidentes de phishing, inteligencia de amenazas, enriquecimiento y clasificación automática de incidentes. • La plataforma debe contar con al menos 16 plantillas prefabricadas las cuales puedan ser utilizadas para generar un playbook. • La plataforma debe tener la capacidad de crear nuevos "Playbooks" y flujos de trabajo, clonar o modificar los existentes, para que estos sean modificados según las necesidades específicas de la organización. • La plataforma debe ser capaz de conectarse a herramientas de terceros mediante un API, lo que permitirá la automatización de acciones en diferentes equipos de seguridad. Algunas de las herramientas de terceros a las que debe poder conectarse son: Email Management, Email Protection, Firewall, Geolocation, Identity and Access Management, ITSM, Malware Scanning, Messenger, Sandbox y Threat Intelligence. • La plataforma debe tener la capacidad de crear y ejecutar un número ilimitado de acciones y "playbooks". • La plataforma debe permitir la creación de acciones y "Playbooks" con la capacidad de ejecutarse manual o automáticamente cuando ocurran eventos y/o condiciones específicas. • La plataforma debe permitir aplicar acciones sobre componentes en sitio (Centro de Datos) o directamente en la nube. • Cuando la plataforma de respuesta realice acciones sobre servicios en nube no deberá de utilizar recursos de red o hardware del centro de datos del solicitante. • La plataforma debe proporcionar las herramientas necesarias para generar conexiones y desarrollar servicios personalizados que no estén disponibles por defecto, y el desarrollo deberá realizarse mediante un lenguaje de programación estándar ejemplo: Python. • La plataforma debe permitir centralizar todas las detecciones, alertas y casos en una única interfaz de usuario, permitiendo detectar, investigar y responder ante las amenazas (TDIR). • La plataforma debe permitir agrupar todas las detecciones, alertas y casos de acuerdo con sus características, como, por

ejemplo: IP, dispositivo, usuario, regla, caso de uso, MITRE TTPs o una etiqueta personalizada, facilitando el entendimiento de la amenaza.

- La plataforma debe permitir automatizar flujos de trabajo cuando se cumplan ciertas condiciones específicas, reduciendo los tiempos de respuesta al realizar acciones secuenciales, automatizando tareas complejas, repetitivas y manuales.
- La plataforma deberá estar basada en Data Lakes de Big Query y permitirá su desplegué a través de colectores en sitio virtuales o físicos.

4.5.2 Plataforma de Inteligencia de Amenazas (TIP)

El Ministerio de Hacienda requiere que La plataforma de inteligencia de amenazas (TIP) con la cual el proponente preste el servicio se integre de forma nativa con el resto de los elementos tecnológicos de la plataforma de servicio para detener las amenazas de una manera efectiva y eficiente, permitiendo acelerar las operaciones de seguridad.

Asimismo, debe permitir consolidar en una única visión todas las amenazas internas y externas a la organización, así como priorizarlas, automatizar su tratamiento y la colaboración con terceras partes.
La plataforma debe recoger, analizar y extraer en su caso la información relativa a las amenazas detectadas por distintos medios y unifica la información de amenazas proveniente de:

- Feeds comerciales incluidos en el servicio de terceros
- El resto de Feeds OSINT disponibles en el mercado relevantes para el servicio
- Información de incidentes detectados en el SIEM de la plataforma
- Información de incidentes documentados en el Service desk del servicio
- Información de vulnerabilidades detectadas en los procesos de auditoría de los activos internos.
- Información de las amenazas detectadas en el servicio de vigilancia digital

La plataforma deberá contar como mínimo con los módulos:

4.5.3 Library: La biblioteca de amenazas de forma automática puntúa y prioriza la inteligencia de amenazas basado en los parámetros propios definidos en el servicio de forma específica.

La priorización se calcula a través de múltiples fuentes internas y externas para obtener una evaluación común utilizando la inteligencia de contexto agregada, lo cual elimina falsos positivos y actividad superflua

Características principales:

- Contexto desde una perspectiva interna y externa
- Auto ajustable
- Importación de datos estructurados y no estructurados
- Priorización automática basada en todas las fuentes
- Enriquecimiento de fuentes a medida para sistemas existentes

4.5.4 Workbench

Debe contar con un banco de trabajo adaptativo que permita combinar la inteligencia humana y la automatización para proporcionar una detección y respuesta proactiva y una configuración específica por el Ministerio de Hacienda y las múltiples integraciones trabajan de forma conjunta con los procesos y el resto de las herramientas de la Plataforma para mejorar la efectividad de estos.

Características principales

- Visión consolidada de amenazas y valoración unificada
- Evaluación continua de amenazas
- Operaciones automatizadas para el resto de los elementos de la plataforma tecnológica
- Cuadros de mando customizables orientados a cada caso de uso

4.5.5. Open Exchange

Una arquitectura extensible que permita al Ministerio de Hacienda contar con un robusto ecosistema de información de amenazas que permita importarla desde fuentes externas e internas, enriquecerla y

exportar la información de inteligencia para operativizar la en el resto de las operaciones de seguridad. Con un amplio Marketplace de integraciones, permite también la integración mediante componentes propios usando SDK/API. Así como el soporte standard de STIX/TAXII

4.5.6. Investigations

Un módulo de investigaciones da solución al desafío que suponen los silos de información y elimine las ineficiencias entre los equipos de operaciones para acelerar los procesos de detección y respuesta proporcionando un modelo de colaboración activa entre todos los equipos.

Características principales:

- Fusionar datos de las amenazas, evidencias y usuarios
- Acelerar la investigación, el análisis y la comprensión de las amenazas para mejorar la postura de seguridad de forma proactiva
- Reducir los tiempos medios de detección y respuesta (MTTD y MTTR)
- Permita obtener una visión alineada en el tiempo de los incidentes, actores y campañas.

4.6 Plataforma de Observabilidad Analítica Avanzada y Minería de Datos con Inteligencia Artificial.

4.6.1 Capacidades Generales

1. La solución requerida debe tener la capacidad de consolidar y mejorar las capacidades de analítica de datos y reforzar la inteligencia operativa mediante la integración de funcionalidades clave en una plataforma unificada.
2. La solución debe contar con un cuadro de mando transversal y unificado.
3. La solución debe contar con capas funcionales integradas como Almacenamiento de Logs, analítica avanzada e inteligencia de negocio.
4. La solución debe tener la capacidad de tener independencia de las fuentes de datos, de los fabricantes de los sistemas de

origen y de los mecanismos de extracción utilizados.

5. La solución se debe soportar un máximo de 100 dispositivos y tener la capacidad de soportar 10 GB diarias.
6. La solución debe contar con una interfaz de recolección de logs abierta y potente (Smart Data Broker), flexible y de alto rendimiento.
7. La solución deberá proporcionar las siguientes funcionalidades complementarias:
   - Ofrecer paneles de control que consoliden información de diversas fuentes.
   - Capacidad para integrar y gestionar datos provenientes de múltiples orígenes simultáneamente.
   - Funcionalidad para crear y distribuir reportes de manera programada y automática.
   - Permitir que múltiples usuarios y/o grupos de usuarios accedan a la plataforma con roles, permisos y vistas personalizadas y segregadas.
   - Habilidad para crear y recolectar eventos relevantes dentro de la plataforma.
   - Proporcionar mecanismos para definir alarmas basadas en umbrales o condiciones, y sistemas de notificación para alertar a los usuarios pertinentes.
8. La solución debe contar con una interfaz API que permita la exportación o integración de la información con otros sistemas de analítica avanzada, portales Web, o sistemas de Business Intelligence de terceros.

4.7 Plataforma Vigilancia Digital

El Ministerio de Hacienda requiere que la plataforma para el servicio de Vigilancia Digital del proponente sea una solución modular, y se adecue a las necesidades del Ministerio de Hacienda utilizando los módulos necesarios que proveen la inteligencia de amenazas y las actividades de vigilancia digital en los servicios propuestos.

La plataforma debe realizar caza de amenazas fuera de la red corporativa y monitorizar la actividad maliciosa, incidentes y actores

	antes de que puedan causar daño a los servicios e infraestructura. La plataforma debe automáticamente recolectar, analizar, correlacionar y entregar datos de amenazas enriquecidos de una amplia variedad de categorías que puede impactar al negocio, desde la identificación de Botnets y servidores C&C a variantes de malware específicas para la organización, desde credenciales comprometidas a la capacidad de encontrar aplicaciones móviles fantasma, actividades de hacktivistas y campañas de phishing que tienen como objetivo la organización y sus procesos. Asimismo, mediante la integración directa y nativa con la plataforma TIP, debe ser capaz de enviar toda la información de inteligencia necesaria para que a través de esta se pueda obtener una visión global de amenazas. **4.7.1 La plataforma deberá contar con mínimos los siguientes módulos:** **Dark Web:** Mejora el conocimiento de lo que está pasando en la Dark Web, permite observar actividades maliciosas que tienen como objetivo la organización y permite prevenir ataques futuros. Permite encontrar credenciales de usuario robadas y activos en tiempo real. **Credential:** Permite obtener información de inteligencia sobre credenciales exfiltradas, robadas y vendidas, así como información del malware usado para el robo de estas. Los sensores, Honeypot y buscadores buscan de forma continua esta información. **Data Leakage:** Permite descubrir si los documentos y el código fuente de la organización se han filtrado en internet, deep web o en redes P2P de forma intencionada o no. **Malware:** Permite detectar malware que busque robar información sensible o cometer fraude o ataques "Man in the browser" específicos a la organización. A través de un análisis continuo y robusto de millones de muestras cada mes, permite obtener un reporte exhaustivo de malware que tiene como objetivo la organización. **Hacktivism:** Monitoriza de forma global la actividad de hacktivismo en redes sociales y en la web abierta o en la Dark web que pueda

	afectar a la infraestructura de la organización usando un avanzado sistema de alerta temprana y geolocalización. **Mobile Apps**: Monitoriza las aplicaciones ilegales y maliciosas con apariencia legal en los Marketplace de aplicaciones. Permite descubrir aplicaciones que pretenden ser legítimas y relacionadas con la organización con objetivos ilegales. **Social Media:** Monitoriza la huella digital de la organización en redes sociales, encontrando sitios web no autorizados a utilizar los logos, marcas, activos que pretender ser legítimos de la organización para poder tomar medidas para su eliminación. **Domain Protection:** Permite monitorizar y detectar dominios fraudulentos establecidos con el fin de robar información de la organización o dañar la imagen de esta. Permite combatir el phishing y el Cybersquatting detectando los ataques y permitiendo tomar medidas proactivas. **4.7.2 MISP (Malware Sharing Information Platform)** El Ministerio de Hacienda requiere que el proponente cuente con la plataforma MISP (Malware Sharing Information Platform), que es una herramienta de inteligencia de amenazas que se ha convertido en el standard de facto para la compartición de información de inteligencia de amenazas a nivel global con otros grupos de interés como organizaciones CERT y CSIRT u otras organizaciones nacionales, regionales o globales. El rol que tendrá esta herramienta en el servicio es la recepción mediante su conector nativo con la plataforma de inteligencia de amenazas (TIP) y la publicación de dichas amenazas con los grupos de interés seleccionados y la recepción y consolidación de las amenazas compartidas desde estos grupos en la plataforma TIP. Las principales funcionalidades de la plataforma son: • Almacenar información tanto técnica como no técnica sobre malware y ataques ya detectados. • Crear automáticamente relaciones entre eventos y sus atributos, identificando amenazas relacionadas.

- Generar reglas para la detección o prevención de amenazas a partir de indicadores para sistemas NIDS (Network Intrusion Detection System).
- Almacenar datos en un formato estructurado, permitiendo así un uso automatizado de la base de datos para alimentar sistemas de detección o herramientas forenses.
- Compartir los atributos de eventos maliciosos, malware y amenazas con otras organizaciones y grupos de confianza.
- Modelado y estructuración de eventos y amenazas según estándares de intercambio de incidentes, ejemplo STIX.
- Establecer una arquitectura federada entre comunidades para intercambiar información entre comunidades de forma segura y controlada.
- Conexión y compatibilidad con la mayoría de las plataformas de inteligencia de amenazas y soluciones de seguridad.

4.8 Requerimientos Específicos – Almacenamiento de Logs.

- El servicio de SOC deberá asegurar el almacenamiento, disponibilidad y recuperación de los LOGs y la información generada durante la ejecución del servicio contratado y 6 meses adicionales.
- El tiempo de custodia de la información técnica de LOGs será por la vigencia del contrato. El proveedor podrá hacer uso del almacenamiento del MHCP para guardar los LOGs durante los meses solicitados.
- El tiempo de custodia de los reportes, estadísticas, análisis de tendencia, métricas e indicadores será por la duración del contrato y 6 meses adicionales.
- El servicio de SOC deberá estar en la capacidad de contar con un plan de respaldo en caso de borrados accidentales o provocados.
- El proveedor deberá disponer del recurso humano con el fin de garantizar la gestión, configuración, instalación de agentes y/o desarrollos para la integración de logs y eventos hacia la solución entregada.

Nota: Una vez cumplido el periodo anteriormente establecido, podrá transferir dicha información al almacenamiento que disponga el MHCP.

4.9 Requerimientos Específicos – Servicio de Análisis Forense de Incidentes de seguridad de la Información

- El servicio de SOC deberá estar en capacidad de realizar el análisis forense digital de forma integral y bajo un modelo metodológico reconocido internacionalmente que deberá ser presentado y aprobado por el MHCP.
- El análisis forense deberá contemplar por lo menos las siguientes fases
  - Contexto: Verificación del escenario
  - Identificación de la infraestructura
  - Recolección de evidencia
  - Análisis de evidencia
  - Presentación del informe técnico e informe gerencial
- El servicio del SOC deberá estar en capacidad de reconstruir lo que haya sucedido tras un incidente de seguridad, determinando quien, desde donde, cómo, cuándo y que acciones ha llevado a cabo el intruso en los sistemas afectados por el incidente de seguridad.
- El proveedor deberá garantizar que tiene las certificaciones requeridas por las entidades de control respectivas para presentar y soportar el análisis forense de un incidente de seguridad.

4.10 Requerimientos Específicos – Gestión de Incidentes de Seguridad.

- El proveedor deberá contar con un procedimiento apoyado en una metodología CIRT/CERT para la detección, alertamiento, notificación y seguimiento de eventos o incidentes de seguridad; de igual manera para informar puntos débiles de seguridad; definir responsabilidades que se deberían asignar para la gestión de incidentes y proponer mejoras de seguridad a la infraestructura tecnología del MHCP.
- El proveedor en coordinación con el MHCP deberá definir los medios de comunicación apropiados para la agilizar la comunicación, análisis, tratamiento y gestión de los eventos e incidentes de seguridad, como contacto telefónico, correo electrónico, mensajes vía celular y/o chat de contacto.
- El servicio de SOC deberá contar con una herramienta para el seguimiento del estado de alertas e incidentes, establecer las

	responsabilidades, roles y los procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de la información. Para ello debe disponer de una herramienta de manejo de incidentes de seguridad y asegurar los accesos a dicha solución mediante el uso de protocolos seguros y autenticación de usuarios.
	• El proveedor deberá otorgar acceso al sistema en línea para seguimiento de incidentes, registro de casos, seguimiento a niveles de servicio, reportes, seguimiento al rendimiento de las plataformas, gráficos y estado de incidentes.
	• El proveedor deberá estar en la capacidad de implementar una interfase de comunicación entre la herramienta del contratista y la herramienta de gestión de incidentes, requerimientos y gestión de cambios del MHCP.
	• El servicio de SOC deberá estar en la capacidad de gestionar las siguientes actividades relacionadas con el manejo de incidentes, así:
	  • Clasificar y priorizar las diferentes alertas generadas por el proceso de monitorización basado en un esquema de emergencia (triage) de acuerdo con la metodología SIRT/CERT.
	  • Alertar eventos detectados de acuerdo con los procedimientos establecidos por el MHCP
	  • Notificar mediante los canales establecidos a los interlocutores que formen parte del proceso de escalado y toma de decisiones que establezca el MHCP.
	  • Seguimiento del estado del incidente y soporte metodológico para la contención o neutralización de los posibles ataques.
	  • Definición de escenarios de crisis para preparación ante amenazas avanzadas (ATP) y así definir reglas para detectar, reaccionar y contener ataques dirigidos.
	• El proveedor deberá realizar los análisis de los eventos o incidentes de seguridad para proponer medidas de protección adicionales o identificar oportunidades de mejora en la seguridad de la infraestructura tecnológica del MHCP.

	• El proveedor otorgará acceso al servicio de SOC a tres (3) funcionarios designados por el Ministerio de Hacienda y Crédito Público.
	
	• Se deberá establecer una metodología en la cual:
	
	  • N2 - Coordinación para la activación del Plan de Respuesta ante Incidentes y N3 - Respuesta experta: Los equipos de Nivel 2 y Nivel 3 del proponente trabajaran con el objetivo de recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo lo posible el impacto negativo de forma que la calidad del servicio y la disponibilidad se mantengan.
	  • Ajuste y optimización de los Playbook definidos: Con base en el conocimiento que se va generando con las investigaciones realizadas, se hace necesario el ajuste y la optimización de los Playbook y casos de uso definidos, mediante el rediseño de patrones y reglas, mejorando la detección preventiva.
	  • Propuesta de diseño de casos de uso y Playbook con base en las amenazas relacionadas con el incidente: Los equipos de Gestión de Incidentes del SOC del proponente deberán establecer medidas acumulativas y configuraciones específicas, basándose en incidentes externos e internos.
	  • Análisis especializado y evaluación de inteligencia (CTI): Cuando un incidente requiere de un análisis profundo para la determinación de las causas de este, se utilizará el nivel de Especialización y Threat Intelligence del proponente, el cual, a partir de sus especialistas y laboratorios de tráfico, forense y malware, generarán defensas, procedimientos, casos de uso y Playbook a aplicar dentro del ecosistema**.**
	• Para el control de dichos objetivos y gestión ágil del servicio, las capacidades que debe aportar el proponente a la gestión de crisis son:
	  • IR – Assessment
	  • Análisis inicial de adecuación de la arquitectura de negocio, tecnológica y procedimental para la respuesta a incidentes tecnológicos de alto impacto**.**

	• Cyber Crisis Management • Gestión estratégica y operativa de incidentes de alto impacto con criticidad y prioridad muy alta. Definición de plan general para el gobierno, la gestión, el seguimiento y cierre de crisis de origen cibernético. • Incident Intelligence • Análisis, investigación y defensa proactiva de amenazas técnicas a través del entendimiento de las motivaciones del ciber criminal, de sus técnicas y tácticas de ataque y de sus impactos operativos. • Incident Response • Gestión operativa de los incidentes y alertas escalados en servicios o desde el Ministerio. Se basa en el conocimiento previo (Incident Intelligence) para determinar la mejor estrategia de contención, mitigación y recuperación. • Digital Forensic and Experts Labs • Adquisición de evidencias forenses de sistemas y laboratorios de análisis de artefactos expertos para determinar la causa raíz, modus operandi y autoría de los incidentes por parte de un equipo altamente especializado.
5	**5.1 CONDICIONES DEL SERVICIO:** Estas condiciones aplican a las actividades de soporte técnico que afecten la disponibilidad del servicio de SOC. • Las soluciones contarán con el servicio de asistencia técnica 7 x 24 x 365, a través del cual se recibirán los incidentes y requerimientos reportados por las personas designadas por el Ministerio de Hacienda y Crédito Público. • En el momento del reporte del incidente o requerimiento se deberá hacer un registro que incluya mínimo los datos de fecha, hora, descripción y número del incidente o requerimiento. El número de incidente o requerimiento asignado se utilizará para identificar y hacer seguimiento del mismo. • El especialista de soporte dispondrá de máximo dos (2) horas de soporte remoto, contadas a partir del registro del incidente, para atender el mismo y calcular tiempo de solución. • Para incidentes de criticidad e impacto alto, que afecten operaciones del Ministerio, serán atendidos en sitio por especialistas con experiencia en soporte de problemas y a la

	vez, se debe generar el caso con el fabricante de la plataforma SOC. El especialista contará con un tiempo de dos (2) horas para el desplazamiento contadas a partir del registro del incidente. • Garantizar la recuperación estable de los servicios en máximo ocho (8) horas.
6	**6.1 CONFIDENCIALIDAD**: Toda la información correspondiente, implementaciones, configuraciones, levantamiento de información y los resultados de los mantenimientos y atención de soportes que realicen los especialistas, así como la información que sea entregada por el Ministerio de Hacienda y Crédito Público dentro de las actividades objeto del contrato serán tratados por el Contratista en forma confidencial, adhiriéndose a las políticas de seguridad y de terceros del Ministerio de Hacienda y Crédito Público.
7	**7.1 RECURSO HUMANO:** Para la ejecución del contrato el contratista deberá prestar el servicio con mínimo el recurso humano que se relaciona a continuación: **Un (1) Gerente de Proyecto:** Formación académica Profesional universitario en ingeniería de sistemas, telemática, o ingeniería electrónica, o, telecomunicaciones afines al SNIES. ✓ Especialización en Gerencia de Proyectos o ✓ Project Management Professional (PMP) o ✓ Lead Risk Manager ISO 31000:2018 o ✓ ISO 27001:2022 Lead Implementer y Experiencia de dos (2) años certificada en Gerencia de Proyectos de Tecnología y/o Seguridad de la información. **Dos (2) Ingenieros de Operación:** ➢ **Un (1) Consultor Ciberseguridad:** Formación académica Profesional universitario en ingeniería de sistemas, telemática, o ingeniería electrónica, o, telecomunicaciones afines al SNIES.

	✓ ISO 27001:2022 Certified Lead Implementer o ✓ Certified Ethical Hacker EC-Council o ✓ Ethical Hacking Professional Certification CEHPC o ✓ Cyber security Foundation Professional Certificate CSFPC o ✓ Auditor Interno ISO 27001:2022 y • Experiencia de dos (2) años en Proyectos relacionados con Centros de Operación de Seguridad (SOC). ➢ **Un (1) Consultor de Gestor de Incidentes** Formación académica Profesional universitario en ingeniería de sistemas, telemática, o ingeniería electrónica, o, telecomunicaciones y afines al SNIES ✓ Especialización en Auditorías de Sistemas o ✓ Lead auditor ISO 22301:2019 o ✓ ISO 27001:2022 Certified Lead Implementer o ✓ Auditor interno ISO 27001:2022 o ✓ Lead Risk Manager ISO 31000:2018+ISO 27005:2022 y • Experiencia de dos (2) años en Seguridad Informática y por lo menos (1) año de experiencia en actividades relacionadas en Centros de Operación de Seguridad (SOC). Para la evaluación de experiencia que se acredite por parte de ingenieros, se tendrá en cuenta la experiencia adquirida conforme a lo establecido en la Ley 842 de 2003, es decir la experiencia profesional solo se computará a partir de la fecha de expedición de la matrícula profesional o del certificado de inscripción profesional, respectivamente. La hoja de vida del recurso humano requerido para la ejecución del contrato deberá estar acompañadas con una autorización expresa y por escrito, en la cual la persona natural autorice al PROPONENTE a presentar su hoja de vida en el actual proceso de selección. Durante la ejecución del contrato es posible realizar el cambio del

	recurso humano, siempre y cuando se mantengan el perfil mínimo requerido y no se genere afectación en el desarrollo del contrato, no obstante, en caso de requerirse reemplazo, el mismo deberá ser aprobado por la Entidad, a través de la supervisión contractual, que en todo caso deberá cumplir con los requisitos mínimos requeridos para el perfil objeto de cambio.

ANEXO No. 2

COTIZACIÓN ECONÓMICA

VIGENCIAS 2025 - 2026						
ITEM	**SERVICIO**	**VIGENCIA**	**UNIDAD**	**CANTIDAD**	**VALOR UNITARIO**	**VALOR TOTAL**
1	Servicio de Monitoreo, diagnostico, generación de alertas y recomendaciones	2025	Meses	2		
		2026		7		
2	Servicio de Gestión y Análisis de Vulnerabilidades	2025	Meses	2		
		2026		7		
3	Servicio de análisis forense de incidentes de seguridad de la información	2025	Horas	50		
		2026		150		
4	Servicio de análisis de vulnerabilidades y ethical hacking de acuerdo con las necesidades del MHCP Mínimo 10 aplicaciones 1 evento durante la vigencia del contrato	2026	Global	1		
VALOR IVA						
VALOR TOTAL CON IVA						

NOTA 1: Los interesados deben tener en cuenta que al valor del contrato se le aplicara el valor del impuesto de timbre equivalente al 0.5% del valor

del contrato. Por lo anterior, deben incluir en sus cotizaciones todos los impuestos tasas y contribuciones a que haya lugar.

NOTA 2: El valor de la oferta económica debe incluir la totalidad de los costos directos e indirectos relacionados con el objeto del contrato, así como cualquier otro costo inherente al mismo. No se considerarán costos adicionales en ninguna circunstancia.

NOTA. 3: Los valores unitarios y totales se deben ajustar al peso y estar en pesos colombianos.

ANEXO No. 3

INFORMACIÓN ADICIONAL

El cotizante, corresponde a alguna de las siguientes categorías:

	SI	NO
MICRO EMPRESA		
PEQUEÑA EMPRESA		
MEDIANA EMPRESA		

Relacione contratos celebrados relacionados con el objeto cotizado, en los cinco (5) últimos años con otras Entidades Estatales y/o Privadas (número y fecha del contrato, nombre entidad contratante).

No. del Contrato	Fecha del Contrato	Objeto del Contrato	Nombre Entidad Contratante

INFORMACIÓN RELACIONADA CON EMPRENDIMIENTOS Y EMPRESAS DE MUJERES

Por favor diligenciar sí el cotizante se encuentra en alguna de las siguientes definiciones:

DEFINICIONES	SI
Cuando más del cincuenta por ciento (50%) de las acciones, partes de interés o cuotas de participación de la persona jurídica 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	

Cuando por lo menos el cincuenta por ciento (50%) de los empleos del nivel directivo de la persona jurídica sean ejercidos por mujeres y éstas hayan estado vinculadas laboralmente a la empresa durante al menos el último año anterior a la fecha de cierre del Proceso de Selección en el mismo cargo u otro del mismo nivel. Entendiéndose 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.	
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.	
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.	

INFORMACIÓN PARA EL FOMENTO DE SUJETOS EN ESPECIAL PROTECCIÓN CONSTITUCIONAL.

El cotizante cuenta con alguno de los siguientes grupos poblacionales, para la provisión de bienes o servicios para la ejecución del objeto cotizado:

GRUPOS POBLACIONALES	SI
Población en pobreza extrema	
Desplazados por la Violencia	
personas en proceso de reintegración o reincorporación	
Víctima del conflicto armado interno	
Mujeres cabeza de familia	
Adultos mayores	
Personas en condición de discapacidad	

Comunidades Indígenas, negra, afrocolombiana, raizal, palanquera, Rom o gitanas	
Otros sujetos de especial protección constitucional	

PROVEEDOR

Nombre o Razón Social del Cotizante _____
Nombre del Representante _____
Nit o Cédula de Ciudadanía No. _____ de_____
Dirección _____
Ciudad _____
Teléfono _____
Fax _____
Correo electrónico _____