Código de la dependencia productora

Bogotá D.C.,

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="3">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 colspan="2">DESCRIPCIÓN</td></tr>
<tr><td>43233200</td><td colspan="2">Software de Seguridad y Protección</td></tr>
<tr><td>43222500</td><td colspan="2">Equipo de seguridad de red</td></tr>
<tr><td>81111800</td><td colspan="2">Servicios de sistemas y administración de componentes de sistemas</td></tr>
<tr><td>81112200</td><td colspan="2">Mantenimiento y Soporte de Software</td></tr>
<tr><td>81118001</td><td colspan="2">Seguridad de los computadores, redes o internet</td></tr>
<tr><td>81161500</td><td colspan="2">Servicios de administración de acceso</td></tr>
<tr><td colspan="3">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 colspan="2">ESPECIFICACIONES TÉCNICAS MÍNIMAS</td><td>COTIZACIÓN ALTERNATIVA</td></tr>
<tr><td colspan="2">Ver anexo. No. 1</td><td>En caso de que aplique o se requieran</td></tr>
<tr><td>PLAZO PARA EJECUCIÓN-</td><td colspan="3">El plazo de ejecución será hasta el 16 de agosto de 2025 contado a partir de la aprobación de la garantía única que debe constituir el Contratista y previa expedición del correspondiente registro presupuestal</td></tr>
<tr><td>PLAZO PARA LA ENTREGA DE LOS BIENES Y/O SERVICIOS</td><td colspan="3">NA</td></tr>
<tr><td>LUGAR DE EJECUCIÓN</td><td colspan="3">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.</td></tr>
</table>

FORMA DE PAGO	• El valor del contrato a suscribir se pagará, por intermedio de la Coordinación de Pagaduría de la Subdirección Financiera de este Ministerio, al CONTRATISTA, con sujeción a la disponibilidad del P.A.C. (Programa anual mensualizado de Caja), en 12 pagos mensuales o fracción de mes de acuerdo con el servicio efectivamente prestado según acta firmada por parte del contratista y el supervisor del contrato. Dichos pagos se efectuarán **con sujeción a la disponibilidad del PAC**, dentro de los diez (10) días hábiles siguientes a la radicación en la Subdirección Financiera y la debida presentación de la factura y del cumplido expedido por el supervisor designado, la certificación de pago de aportes parafiscales y de seguridad social por parte del contratista y registro de carga de dichos soportes en SECOP II.
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)	

NOTA: Si el cotizante encuentra que algo falta, no es procedente o es diferente a lo consignado en la descripción técnica de la necesidad, es importante que lo manifieste, justificando la razón que sustenta el cambio, para que el ministerio, previo análisis, determine la procedencia de la sugerencia. Para tal fin deberá determinar los costos de la cotización alternativa.

Agradecemos se sirva remitir la información respectiva a más tardar el día 7 de junio de 2023**,** a través de correo electrónico invtecnologia@minhacienda.gov.co o gparra@minhacienda.gov.co

Cordialmente,
RICARDO FERNELIX RIOS ROSALES
Director de Tecnología

Anexo No.1: **REQUERIMIENTOS TÉCNICOS Y OBLIGACIONES MÍNIMAS**

* Si el cotizante desea presentar una cotización alternativa a la solicitada por el Ministerio, debe cumplir con las condiciones técnicas mínimas de la cotización básica.

ANEXO No.1
REQUERIMIENTOS TÉCNICOS Y OBLIGACIONES MÍNIMAS

1	**TERCERIZACIÓN DE SERVICIOS DE SEGURIDAD** **1.1 DESCRIPCION DEL SERVICIO** Los servicios por contratar comprenden los siguientes: 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: A. 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. B. 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 C. 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 D. 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. E. 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. F. 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. G. Se deben entregar informes periódicos (por lo menos mensual) con los reportes históricos de monitoreo y gestión de alarmas realizadas. H. Debe tener la posibilidad de integrarse o exportar información de incidentes a la herramienta gestión de incidentes, requerimientos y cambios utilizada por el Ministerio. I. 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. 2. Apoyar al Ministerio en la revisión, identificación y aplicación adecuada de las diferentes metodologías que requiere la entidad, en temas de seguridad y ciberseguridad, enfocado en cumplimiento de políticas y lineamientos de Estado. Se deben revisar como mínimo las siguientes metodologías: OSSTMM, CEH, OFFENSIVE SECURITY, ISSAF, NIST, OWASP, OWISAM 3. Gestión y Análisis de Vulnerabilidades. Comprende: a) Análisis de Vulnerabilidades: se debe realizar periódicamente (por lo menos cada tres meses), sobre una cantidad de 1000 IP´s correspondientes a componentes de la infraestructura computacional del Ministerio. Sobre los activos que el Ministerio considere críticos o que soporten servicios esenciales de la entidad, el análisis debe realizarse de forma permanente y persistente. b) Ethical Hacking: se debe realizar periódicamente (por lo menos dos veces al año), 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

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

1.2 CARACTERISTICAS DEL SOFTWARE DE LA ENTIDAD

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

1. **VARONIS:** Herramienta de administración y gestión de componentes de información y datos (gobernabilidad de datos). Licenciamiento para 500 usuarios y versión (8.5.34.31)

2. **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)

3. **IMPERVA:** Herramienta de auditoría de bases de datos, IMPERVA Securesphere. Licenciamiento para 500 bases de datos y versión Enterprise Edition (13.2.0.20).
4. **VISION ONE**: Trend Micro Vision One recopila y correlaciona datos de actividad profunda en múltiples vectores de XDR. Licenciamiento para 2.100 usuarios, versión 2022.

	5. 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 2022.
2	Realizar activación del servicio SOC de la solución descrita en el numeral 1 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	**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 de garantía única, previo registro presupuestal. **a. 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. El contratista deberá realizar las siguientes actividades dentro de los dos primeros meses de ejecución del contrato, una vez aprobada la póliza de garantía única. **b. 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. **c. 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. **d. 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. **e. 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	**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 Las plataformas del SOC deben proveer los siguientes servicios a la infraestructura de seguridad:** a) Automatismos tanto en la identificación como en la respuesta, creando así un sistema inmunitario adaptativo de alta eficacia. b) Fortaleza ya que se tratan las tecnologías como parte de un sistema global interconectado, generando una suma de capacidades. c) Inteligencia cada uno de estos componentes debe estar complementado por motores de inteligencia artificial para el enriquecimiento de la información de amenazas, generación de patrones, defensas y optimización de la seguridad de las infraestructuras d) Se deberá prestar el servicio con base en una plataforma tecnológica que soporte todos los servicios incluidos con componentes tecnológicos provistos en un modelo cloud SaaS teniendo en especial consideración las necesidades presentes y futuras del servicio en cuanto a la escalabilidad, elasticidad, resiliencia y capacidades de integración. e) Cada elemento de esta plataforma deberá soportar uno o varios procesos de los servicios que se realizan y estar integrados en su mayor parte mediante conectores nativos out-of-the-box, lo que garantice un funcionamiento sin fricciones y con los mayores estándares de calidad y disponibilidad. f) Se deberán agregar los concentradores de eventos de la arquitectura actual de seguridad del Ministerio de Hacienda, al sistema de monitorización para que forme parte de los servicios centralizados de identificación, análisis y respuesta a amenazas, así como todos aquellos componentes que aporten información de contexto y enriquecimiento, quedando cubiertos con todas las capacidades del centro de operaciones de seguridad descritas en otros puntos del presente documento. " **4.2 Especificaciones Técnicas Generales Contratista** a) El contratista deberá prestar el servicio en el idioma español, para la interacción de las áreas de operación.

	b) El contratista deberá contar con certificación ISO 27001 con antigüedad mínima de 7 años para el ámbito de Gestión de Seguridad de la información. Adicional, el proveedor debe ser miembro activo de FIRST. c) 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, elementos de hardware y demás requeridos para soportar el correcto funcionamiento de los servicios de monitoreo de los dispositivos informáticos de la infraestructura tecnológica del MHCP d) El contratista deberá contar con una capacidad operativa y de soporte de fabricantes 7x24x365, durante toda la ejecución del contrato. e) El contratista deberá certificar la evaluación de antecedentes para los contratistas o usuarios de terceras partes que interactúen con el SOC. f) El contratista deberá realizar periódicamente, según lo establezcan las mejores prácticas, análisis de tendencias sobre los eventos y plataformas monitoreadas. g) El contratista deberá proporcionar reportes bajo solicitud del Ministerio de Hacienda y Crédito Público, por demanda. h) El contratista deberá contar con un informe detallado sobre alertas mundiales que puedan afectar la seguridad sobre la infraestructura. i) El contratista deberá suministrar el servicio de administración, operación y soporte de toda la infraestructura de hardware y software implementada para el servicio. j) El contratista **a** deberá monitorear los componentes de la infraestructura tecnológica implementada para el servicio de forma proactiva mediante herramientas de gestión. k) El contratista deberá realizar los mantenimientos preventivos y correctivos adecuados para asegurar la continua disponibilidad e integridad de la infraestructura del servicio. l) El contratista deberá garantizar 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. m) El contratista deberá contar con procesos de eliminación segura de la información que ya no se requiera. n) El contratista deberá tener un SOC propietario, en la ciudad de Bogotá. o) 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. p) 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 siguientes certificaciones: CISSP, CISM, OSCP, CISA, ISO27032. q) El contratista deberá contar con personal certificado en la herramienta SIEM con que el SOC presta el servicio de monitoreo, correlación y demás. r) 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. s) El contratista deberá detallar los procesos de: Gestión y Respuesta a incidentes, atención y escalamiento de requerimientos, Mejora Continua del servicio. **4.3 Especificaciones Técnicas Generales del SOC**

	a) 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. b) El servicio de SOC debe contar con capacidades de HUNTING con el fin de encontrar amenazas desconocidas. c) 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. d) 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. e) El SOC deberá realizar análisis del comportamiento de la infraestructura administrada y monitoreada para correlacionar incidentes y determinar proactivamente problemas en la operación. f) El SOC deberá garantizar la disponibilidad, confidencialidad, integridad, autenticación, autorización, no repudio, auditoría y privacidad de los datos y servicios soportados. g) El SOC deberá contar con un grupo interdisciplinario interno para la atención de incidentes, bajo un procedimiento claro y definido. h) El servicio de SOC deberá contar con la alianza de un CERT. i) El servicio del SOC deberá permitir la integración del envío de alarmas automáticas vía correo electrónico. j) 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. k) 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. l) El servicio de SOC deberá integrase con LDAP (Protocolo Ligero de Acceso a Directorios). m) El SOC deberá contar con la capacidad de asegurar la generación, almacenamiento mínimo de doce (12) meses y potencial recuperación de respaldos de las configuraciones de todas las plataformas involucradas en el servicio. n) El servicio de SOC deberá ser compatible con los métodos de recopilación de logs de la industria (Syslog, WMI, JDBC y SNMP). o) Los componentes que realizan la recolección de eventos deberán tener la capacidad de enviar los datos a múltiples destinos primarios de forma simultánea. p) El servicio de SOC deberá estar en capacidad de realizar el análisis de la infraestructura del MHCP en tiempo real de los eventos. q) 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. r) 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. s) 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.

t) El servicio de SOC deberá estar en capacidad de gestionar procesos automatizados de respuesta a incidentes y revisión de actividades anómalas.
u) El servicio de SOC deberá estar en capacidad de gestionar procesos automatizados de primer nivel en análisis de phishing y malware.
v) 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.
w) 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.
x) 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.
y) 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

4.3.1. 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 la competencia. **4.3.2** 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. **4.3.3**. 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). **4.3.4**. 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

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.

4.3.5. 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

4.3.6. 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

4.4 Requerimientos Específicos – Correlación y Alertamiento de Eventos de Seguridad

a) 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.
b) 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. c) 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. d) 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. e) El contratista deberá establecer el protocolo para informar, reportar y/o escalar los eventos, alertas e incidentes que se detecten. f) 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. g) 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 h) 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. i) 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. j) El enlace o canal de comunicación entre el MHCP y el proveedor será por canal de internet dedicado y deberá disponer de ancho de banda suficiente para realizar las actividades de acuerdo al dimensionamiento del servicio contratado. El costo del canal dedicado a internet lo asume el proveedor. k) 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. l) El servicio de SOC deberá estar en capacidad de ofrecer a través de sus herramientas, las siguientes funciones: • Análisis de comportamiento • Análisis de vulnerabilidades • SIEM • Detección de Amenazas m) 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. n) 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. o) 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. **Definición caso de uso** Todo el conocimiento generado dentro del SOC debe retroalimentar los casos existentes, como la creación de nuevos casos, permitiendo afinar la detección y reduciendo los falsos positivos. **Identificación** La Identificación de los eventos de seguridad a ser tratados por el equipo SOC se basa en los casos de uso definidos y monitorizados por el proponente para el Ministerio de Hacienda. **Triage** Durante el Triage se lleva a cabo la categorización y el análisis del impacto del evento detectado, estableciendo la categoría de la alerta, criticidad y prioridad correspondiente. **Investigación** En la etapa de Investigación los equipos de Nivel 2 y Nivel 3 del proponente llevan a cabo un análisis en mayor profundidad del incidente. **Remediación** En la etapa de Remediación se pone en práctica el plan de contención y remediación para mitigar el incidente con base en los planes de actuación definidos en el Playbook asociado al caso de uso materializado. **Post-Incidente** Durante el Post-Incidente se incluye el final de la investigación, documentando toda la información obtenida y realizando un reporte del incidente Se requiere el servicio de Monitorización y Análisis del Incidente dentro del proceso de análisis de

incidentes, la clasificación de las alertas detectadas es el elemento inicial que permite un rápido tratamiento de cada evento y priorización adecuada de la gestión del incidente, por lo tanto, se requiere:

Catalogación de eventos de seguridad: Todo evento debe ser clasificado dentro del catálogo de tipologías de incidentes, bien sea el del proponente o el proporcionado por el Ministerio de Hacienda.

Clasificación de la fase y patrón del incidente: Atendiendo al "Kill Chain" el framework en el cual se puedan definir criterios de clasificación para identificar la fase en la que se encuentra el ataque y sus patrones según las Técnicas y Tácticas utilizadas, a través del framework ATT&CK MITRE.

Clasificación del nivel de comunicación: A través del protocolo TLP, se propone una clasificación para facilitar el intercambio de información con en base a la criticidad e intervinientes para garantizar la protección de la información confidencial y la rápida coordinación de los actores del tratamiento para una respuesta, contención y remediación adecuada.

Clasificación del nivel de criticidad: La criticidad de un evento va a permitir la priorización y toma de decisiones en relación con las acciones de respuesta; valorando la criticidad del evento, del contexto y la combinación de ambas para identificar un incidente **modelable, un incidente operable o una crisis.**

Catalogación del nivel de crisis: En caso de que un incidente se considere crítico, El proponente deberá mantener un nivel de alerta para la crisis (DEFCON) que permite gestionar de manera sistemática la evolución y situación de esta, así como las implicaciones de cada nivel de crisis (intervinientes, medidas, comunicación, etc.) habilitando inmediatamente una estructura completa de tratamiento liderada desde una war-room.

4.5 Servicio de Threat Hunting

El Ministerio de Hacienda requiere como objetivo principal en el servicio de Threat Hunting actuar de manera proactiva en la infraestructura del Ministerio de Hacienda para identificar amenazas que no fueron detectadas por las soluciones implementadas en la actualidad. De igual manera, es posible la identificación de incidentes que se han llevado a cabo en la infraestructura y de los cuales no se tenía conocimiento.

El servicio se debe desarrollar basado en misiones de hunting, los analistas del proponente deben priorizar la búsqueda de amenazas con base a las técnicas que más están siendo usadas estadísticamente por los cibercriminales. Gracias a este modelo de trabajo, se irán cubriendo técnicas basadas en la matriz de ATT&CK de MITRE para poder ir centrando esfuerzos en aquellas que no se hayan implementado y sobre las que se desarrollan las principales actividades.

Cada misión de hunting que se vaya terminando, se irá automatizando en formato de "identificación preventiva" para poder hacer foco en las nuevas misiones, consiguiendo así que los analistas no tengan que volver a perder tiempo en intentar detectar comportamientos pasados, ya que estos serán detectados automáticamente.

Aplicar este modelo de trabajo le permitirá al Ministerio de Hacienda que, con el paso del tiempo,

	consiga ir cubriendo una gran cantidad de técnicas utilizadas en intrusiones por los principales grupos de cibercriminales. Automatizando y permitiendo por lo tanto hacer foco en las nuevas técnicas que vayan descubriéndose, enriqueciendo por lo tanto de manera indirecta otros servicios ofertados. Bajo las actividades anteriormente descritas, se deberá elaborar contenido diferente para cada una de ellas. Todo este contenido tendrá que verse reflejado en los reportes generados por el equipo de threat hunting para el Ministerio de Hacienda. **Contenido:** • Hipótesis/Escenario sobre el que se sustenta la operación llevada a cabo dentro de la infraestructura. • Actor/es que están relacionados con la hipótesis. • Tácticas y técnicas que se pretenden identificar durante el ejercicio de hunting. • Malware, herramientas legítimas y LOLBAS que puede generar esas técnicas y tácticas que se tratan de identificar en la red. • Indicadores de compromiso detectados en las misiones de hunting. • Comandos ejecutados cuando aplique. • Objetivo de identificación por parte del equipo de Threat Hunting. • Generación de operables que puedan identificar el uso de la hipótesis sobre la que se ha trabajado (reglas SIGMA, consultas de Elastic, Eventos de Windows, Sysmon, etc.) • Periodicidad de nuevos Hunts: entregables periódicos que serán automatizados y enriquecidos durante el servicio. • Notificación de Hunts monitoreados en 24X7. El servicio deberá llevar la actualización de un cuadro de mandos basado en la matriz de ATT&CK donde quedará registrada la siguiente información. • Técnicas abordadas y sin mecanismos de detección desarrollados: Son aquellas técnicas que se han llevado a cabo en alguna misión de hunting pero que aún no se han automatizado contramedidas de detección y/o mitigación. • Técnicas abordadas y con mecanismos de detección desarrollados: Todas aquellas técnicas que han sido abordadas en misiones de hunting y ya existen contramedidas de detección y/o mitigación • Técnicas con gaps de visibilidad (no existe ningún data Source que permita detectarla): Se trata de aquellas técnicas que se ha llevado a cabo una misión de hunting pero que es posible identificar su explotación debido a que no existe ninguna fuente de logs o data Source que cubra dicha información. En este apartado el equipo de threat hunting y threat management trabajarán en conjunto para solventar el problema. **a. Especificaciones Técnicas Generales Herramienta SIEM.** a) El proveedor deberá ofrecer un servicio integral de SOC, el cual contemple durante la etapa de operación, la ejecución del afinamiento y estabilización respectivo de la plataforma SIEM que cuenta la entidad b) El proveedor deberá estar en la capacidad de suscribir las actualizaciones de firmas, URLs y demás funcionalidades de seguridad ante las cuales pueda proteger el (los) dispositivo(s)

	que hagan parte de la solución SIEM instalada. c) La herramienta SIEM especializada en monitoreo y correlación de eventos de seguridad de la información ofrecida por el proveedor deberá estar actualizada y en la última versión liberada en el mercado. d) La herramienta SIEM especializada en monitoreo y correlación de eventos de seguridad de la información ofrecida por el proveedor deberá estar en capacidad de almacenar y conservar los logs de seguridad para fines forenses e investigación y los correspondientes eventos por el periodo definido por el MHCP. e) La herramienta SIEM especializada en monitoreo y correlación de eventos de seguridad de la información ofrecida por el proveedor deberá estar en capacidad de ser alimentada por fuentes de inteligencia externas de amenazas que contengan listas de reputación (IP) y/o dominios catalogados como sospechosos para la generación de indicadores de compromiso. f) El Correlacionador de Eventos utilizado por el SOC debe garantizar el manejo de protocolos seguros, así como la protección adecuada de la información a transmitir para la prestación y uso del servicio (SSL/TLS, VPN, canales dedicados). g) El Correlacionador de Eventos utilizado por el SOC debe conectarse con sistemas de inteligencia basados en intercambio colaborativo y machine learning para descubrir ataques ocultos, entre otros. h) El Correlacionador de Eventos utilizado por el SOC debe contar con un panel de control de seguridad fácil de utilizar que destaca las amenazas más importantes y apoya un flujo de trabajo rápido y eficaz para la investigación y remediación i) El Correlacionador de Eventos utilizado por el SOC debe estar en la capacidad de integrarse a través de estándares STIX o TAXII hacia los motores de correlación del Ministerio de Hacienda para intercambiar Indicadores de Compromiso (IOC). j) El Correlacionador de Eventos utilizado por el SOC debe ser compatible con los métodos de recopilación de logs de la industria (syslog, WMI, JDBC, SNMP, OPSEC, ALE, registros de FTP, SCP, SFTP, entre otros). k) La nube de inteligencia que alimente el Correlacionador de Eventos a nivel de indicadores de compromiso (IOC) debe consumir mínimo diez (10) fuentes externas. **4.6 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: **4.6.1. 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 **4.6.2 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 **4.6.3. 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 **4.6.4. 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

4.7 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, correlar y entrega 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.

4.7.4. 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.

4.7.3 Tecnología de Análisis de Inteligencia y Ciber investigación

El Ministerio de Hacienda requiere que el proponente cuente y ponga a disposición del servicio una

plataforma enfocada a la ciber investigación para la prevención de riesgos procedentes del entorno digital, debe contar con una funcionalidad amplia, incluyendo una significativa capacidad de obtención, integración, procesamiento y visualización de altos volúmenes de información. Los requisitos mínimos y estructurales serán:

- Vigilancia/monitorización del entorno, atendiendo a criterios temáticos definidos por la organización. Debe incluirse la capacidad de generar alertas automáticas en función de criterios predefinidos por la organización.

- Motores de análisis de patrones e identificación de amenazas basados en Inteligencia artificial y Machine Learning.

- Estructura de operación basada en Big Data con colas abiertas para la interrelación de fuentes internas y correlación de otras soluciones de forma nativa.

- Explotación automática de fuentes específicas de información. Conexión a BBDD corporativas, redes sociales, foros y blogs, etc. Supone poder capturar previamente grandes cantidades de datos, tanto estructurados como no estructurados (tratamiento masivo).

- Homogeneización e integración de la información recopilada. Dado que los datos recopilados pueden venir en formatos de muy diversa naturaleza, las plataformas deben ser capaces de homogeneizar los datos recopilados e integrarlos en un contexto unificado que permita el posterior análisis conjunto. Esta recopilación de información debe ser completa (datos y metadatos), con el fin de proporcionar una trazabilidad suficiente a los datos recopilados (por ejemplo, para su presentación en el ámbito judicial).

- Interpretación de las piezas de información recopiladas. Uso de técnicas de análisis semántico / inteligencia artificial para una comprensión básica del contenido de la evidencia (identificación de idioma, análisis de sentimiento, extracción de entidades, etc.)

- Análisis básicos del conjunto de evidencias recopiladas y visualización de estas: Geoposicionamiento, secuenciación temporal, mapa de relaciones y estadísticas.

- Gestión del caso. Seguimiento control de las piezas de información utilizadas, esquemas de investigación, gráficos elaborados tras los análisis, publicación de resultados, etc.

- Gestión de perfiles de usuario. Definición y control de quién puede hacer qué (aspecto clave por la naturaleza de algunas de las informaciones que eventualmente puedan ser recopiladas).

El Ministerio de Hacienda requiere que la plataforma pueda crear casos de investigación, emitiendo su planificación y ejecución según el ciclo de Inteligencia, identificando de forma clara cada una de sus fases, las tareas que se pueden realizar en ellas y los procesos de relación y cambio de fase.

4.7.4. Componente de Obtención.

La plataforma deberá estar preparada para poder obtener y recibir información de medios

totalmente heterogéneos (redes sociales, foros, blogs, noticias, fuentes RSS, repositorios internos, logs de dispositivos, etc.). Los procesos de recolección e importación podrán ser desarrollados en diferentes tecnologías y con aproximaciones diferentes, debido a que cada fuente que se pretenda investigar podría tener unos requisitos específicos de captura. Todos los procesos de obtención de información se deberán monitorizar para comprobar su actividad, y gestionar de forma dinámica y automática el número de instancias requeridas de cada uno, para que puedan acometer todos los trabajos que les solicite la plataforma.

4.7.5. Componente de Transformación.

Debe de concentrar los principales procesos automáticos, algoritmos de inteligencia artificial y aprendizaje automático. A partir de la información proveniente de medios diversos, deberá obtener un cuerpo de evidencias documentales homogéneo, clasificado, válido y enriquecido. La información recibida pasará por diferentes procesos hasta que esté preparada para su almacenamiento y análisis.

Cada mensaje de información pasará por una secuencia de transformación donde algoritmos específicos se encargarán de realizar, como mínimo, las siguientes tareas de forma automática:

- Clasificación del elemento en base a términos.
- Identificación de entidades dentro del contenido.
- Geolocalización.
- Control de no repetición.
- Identificación del Idioma.
- Aplicar expresiones regulares.

Análisis de sentimiento. En el componente de transformación además de estos procesos automáticos desencadenados con la recolección de la información mediante el componente de obtención, existirán otros procesos o algoritmos encargados de realizar análisis automático referente a:

- Correlación de entidades. Una vez identificadas las entidades en cada elemento, sobre la información validada, el sistema, deberá trabajar sobre las entidades de todos los elementos relacionando aquellos elementos con entidades comunes.
- Generar imágenes del contenido.
- Similitud. Algoritmo que identifique elementos muy parecidos en base a un umbral de aceptación definido.
- Sistema de recomendaciones. Algoritmo de aprendizaje automático que con base en las acciones de validación de información del usuario aprenda y sugiera al analista la validación de conjuntos de información pendiente de revisar.

4.7.6. Componente de Gestión.

Tanto el componente de Obtención, como el componente de Transformación estarán compuestos por una serie de procesos específicos encargados de realizar tareas independientes y concretas, por ello, la plataforma deberá de tener un componente

encargado de la gestión y orquestación de todos los procesos que se ejecutan en el sistema. Este componente deberá cubrir los siguientes objetivos:

- Recepción de tareas e instanciación de procesos.
- Coordinación y priorización de tareas.
- Permitir flujos paralelos y secuenciales de tareas.
- Poder definir secuencias de tareas diferentes.
- Realizar tareas puntuales, periódicas o de Background.
- Mantener una trazabilidad de datos.

4.7.7. Componente de Almacenamiento.

El componente de almacenamiento estará planteado con base en la utilización de sistemas gestores que permitan el almacenamiento y recuperación eficaz de grandes volúmenes de información. Debido a que la plataforma debe manejar información de diversa naturaleza se deberá poder diseñar esquemas de bases de datos sobre motores acordes a cada una de las necesidades.

La plataforma deberá disponer de tres tipos de sistemas de almacenamiento:

- Base de datos Big Data: Para mantener todas las estructuras de información de las aplicaciones referentes a la organización, gestión, tareas, escalabilidad y configuración de la plataforma.

- Motor de indexación: Orientado a mantener los documentos que provengan de los procesos de recolección y que son el elemento fundamental de estudio. Para este tipo de base de datos, no solo bastará con diseñar un entorno en el que poder almacenar de manera correcta una gran cantidad de información, sino que será necesario poder disponer de un motor de búsqueda de información rápido y potente para poder realizar análisis y estadísticas sobre grandes cantidades de información en tiempo real.

- Base de datos caché: Para operaciones y recursos necesarios temporales el sistema deberá de tener una base de datos de rápido acceso, evitando realizar dichas tareas sobre sistemas más complejos reduciendo de esta forma su carga de trabajo e indexación.

4.7.8. Componente de Mensajería y Distribución.

El componente de mensajería y distribución deberá interconectar los diferentes elementos, dotando a la plataforma de una arquitectura desacoplada entre los componentes. Para la correcta comunicación entre módulos y procesos, el componente de mensajería deberá gestionar toda la problemática asociada a prioridades, entregas, gestión de colas, routing de información y almacenamiento y distribución de mensajes, todo ello contando con la necesidad de absorber y transferir gran cantidad de información.

4.7.9. Componente de Seguridad.

La plataforma estará capacitada para incluir soluciones que aseguren la hora del acceso y

transferencia de información. Para esto deberá de estar diseñada con medidas que aseguren la implantación real y operativa del principio de "Need to Know". Así, se deberá de poder definir y gestionar diferentes perfiles con distintos niveles de acceso, además de controlar las identidades en el momento de acceso a través de modelos de autenticación SSO (Single Sign On).

4.7.10. Componente de Explotación.

El componente de explotación ágil se corresponde con la capa donde se encontrará la aplicación o conjunto de aplicaciones a las que se tendrá acceso mediante la plataforma de ciberinvestigación. Este componente deberá estar orientado a un entorno web y accesible desde distintos dispositivos de forma concurrente. Se encargará de presentar a los usuarios de la plataforma todos los datos obtenidos, así como la información agregada a los mismos con inteligencia generada por la plataforma. Toda la interacción directa entre los usuarios y la plataforma se realizará a través de esta capa, a excepción del envío de alarmas a terceros sistemas que pueda realizar la plataforma. Uno de los aspectos importantes de este componente o interfaz, es que deberá de tener la posibilidad de representación de la información recolectada de varias formas. El interfaz de usuario además de representar la información con sus datos y metadatos debe posibilitar otras representaciones:

- Representación en forma de grafo, para el análisis de relaciones entre elementos, localización de vecinos y caminos mínimos.
- Representación geoespacial, plasmando en un mapa los eventos asociados a un elemento cuando estén disponibles.
- Representación con base en filtros o gráficas, permitiendo el análisis de características globales.
- Secuencias temporales. Representación de eventos asociados a los documentos en base a histogramas

El Ministerio de Hacienda requiere que la solución provea módulos que doten a los analistas de capacidades de inspección según métodos estructurados, totalmente integrados con el resto de los módulos, con paso de información y valoración cruzada, como mínimo deberá de poseer estas secciones:

- Generación de Hipótesis y valoración por pasos según analistas. Espacio dedicado al perfilado de hipótesis sobre los casos que se estén diseñando, donde cada analista podrá establecer pasos en los criterios de valoración de la hipótesis.

- Módulo de análisis de hipótesis según método ACH (Análisis de Hipótesis en Competencia). Donde los analistas deberán de poder establecer criterios de comparación según el modelo de las hipótesis y las evidencias, adquiridas de forma automática por la herramienta, para la determinación de criterios en la toma de decisión.

4.8. Plataforma On-Premise en las instalaciones del SOC que no dependa de la nube y permita la inteligencia en la detección del malware

El Ministerio de Hacienda requiere que el proponente cuente y ponga a disposición del servicio una

	plataforma para fortalecer las capacidades de inteligencia en la detección del malware. Debido a la criticidad de la actividad es necesario tener un sistema interno, con conexiones externas limitadas, donde se pueda realizar inteligencia sobre las muestras de malware de los ataques dirigidos, y poder llegar a identificar cuales pertenecen a una misma campaña, son mutaciones o modelos de falsa bandera, para que según las conclusiones se pueda aplicar una política de defensa apropiada. Para llevar a cabo estos objetivos se necesita una plataforma en las instalaciones del SOC On-Premise, con análisis autónomos, que tenga como mínimo estas características: • Panales de control con información sobre las muestras que se han analizado, cuántas de ellas se tratan de una carga final de malware y cuantas son embebidas. Gráficas diferentes que representan información sobre todas las muestras subidas en la plataforma y su principal comportamiento. • En el mismo panel de control se deberá de poder ver de forma clara una tabla que muestre las últimas muestras que han sido subidas en la plataforma, y que se pueda consultar la información sobre las mismas a través de enlaces en la propia tabla Sección de análisis comparativos de muestras según los siguientes criterios: a) Similitud: relación de muestras de malware a nivel de código, mostrando el porcentaje de similitud que existe entre todas las muestras. b) Categoría: Relación de las muestras de malware por el tipo de amenaza a la que pertenecen (trojan, bot, phishing, etc) c) Tácticas Mitre: Relación de las muestras de malware en función de las tácticas que utilizan durante su ejecución en un sistema. d) Técnicas Mitre: Relación de las muestras de malware en función de las técnicas que utilizan durante su ejecución en un sistema. e) Procesos: Relación de las muestras de malware según los procesos que llaman durante su ejecución en los sistemas. f) Conexión: Relación de las muestras de malware en base a las conexiones que establecen con direcciones IP o dominios del exterior. g) Etiquetas: Relación entre las muestras de malware en base a las etiquetas que se han establecido en las mismas. Se deberá de poder establecer un correcto etiquetado de las muestras de malware que ayude a ver muestras de malware según familias, comportamientos, patrones, etc. h) Reglas YARA: Relación de muestras de malware que tengan en común una regla YARA que detecte su comportamiento. **4.8.1.** El Ministerio de Hacienda requiere que los algoritmos mínimos de comparación de muestras a través de “Similitud” que son exigibles no excluyentes entre ellos, es decir, la plataforma deberá de mostrar una comparativa continua entre todas las muestras, podrá haber miles de ellas, o entre una selección de estas, a través de los siguientes modelos de similitud, por lo que previamente debe de realizar el proceso de inspección, siendo obligatorio la totalidad de los mismos: • SSDEEP • IMPHASH

- TRHHASH
- TLSHHASH
- Similarity Uniform Fuzzy Hash

4.8.2. El Ministerio de Hacienda requiere que cada muestra sea analizada de forma estática y dinámica de forma automática y deberá mostrar la información de las siguientes secciones:

Información básica de la muestra: Visualizará información base de la muestra, como hashes, nombre del fichero, tamaño, entre otros.
Resumen del Comportamiento: El resultado de los análisis estáticos y dinámicos, reseñando los riesgos identificados según su criticidad.
Conexiones: En caso de que la muestra durante su ejecución realice comunicaciones con algún host externo, aparecerán todas y cada una de ellas y el protocolo usado.
Relaciones: La información que tiene vinculada una muestra de malware debe ser mostrada en modo grafo para poder tener a simple vista todo su comportamiento, tanto de análisis de similitud como estáticos y dinámicos, con el resto de las muestras seleccionadas, o entre tags elegidas, todo ello en un entorno off-line.
MITRE: Visualización de la matriz de MITRE ATT&CK Enterprise mostrando aquellas tácticas y técnicas que el malware usa durante su ejecución en el sistema.
Resultados YARA: En un entorno aislado y sin comunicación, los analistas deberán de poder incorporar reglas Yara para que se puedan pasar de forma reiterativa y automática sobre todas las muestras cargadas. Aquellas reglas YARA que hayan sido ejecutadas contra la muestra de malware para identificar si tienen cierto comportamiento, se mostrarán indicando si hubo match o no.
La solución debe permitir a los analistas seleccionar dos tipos de comparativas en una sección dedicada a la inspección.

4.8.3. **Comparativa por código**. Dentro de la comparativa de código, se debe de poder comparar muestras de malware seleccionando aquellas que el analista previamente a identificado, debiendo existir la posibilidad de comparar todas las muestras de malware que comparten un determinado tag. Comparativa por comportamiento: La otra opción de comparativa debe ser por comportamiento, la cual, debe de permitir, a través del análisis dinámico hecho previamente en la muestra de malware, ver que patrones de actividad tiene en relación con otras muestras de malware. Al igual que la anterior comparativa de código, también debe permitir comparar diferentes muestras de malware por sí mismas o por TAGs, añadiendo además opciones de filtros por comportamientos concretos.

4.9. Requerimientos Específicos – Almacenamiento de Logs.

a) 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 1 año más.
b) El tiempo de custodia de la información técnica de LOGs **será de SEIS (6)** meses. El proveedor podrá hacer uso del almacenamiento del MHCP para guardar los LOGs durante los meses solicitados.
c) El tiempo de custodia de los reportes, estadísticas, análisis de tendencia, métricas e indicadores será por la duración del contrato y 1 año más.
d) El servicio de SOC deberá estar en la capacidad de contar con un plan de respaldo en caso de borrados accidentales o provocados.

	e) El proveedor deberá disponer del recuro 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. **4.10. Requerimientos Específicos – Servicio de Análisis Forense de Incidentes de seguridad de la Información** a) 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. b) 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 c) 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. d) 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. **4.11. Requerimientos Específicos – Gestión de Incidentes de Seguridad.** a) 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. b) 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. c) 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. d) 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. e) 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. f) 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. g) El proveedor otorgará acceso al servicio de SOC a tres (3) funcionarios designados por el Ministerio de Hacienda y Crédito Público. h) 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. I) 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

4.12. Requerimientos Específicos – Informes, Métricas y Tendencias.

- El proveedor deberá elaborar reportes de monitoreo, cambios, alertas, tendencias, gestión, métricas, estadísticas que se entregarán de manera periódica (diario, semanal, mensual, semestral) según requerimiento del MHCP.
- El servicio de SOC deberá estar en la capacidad de generar reportes de eventos y de análisis de tendencias, para tomar las acciones preventivas y/o correctivas, tales como: instalación de parches, actualización de versiones, modificación de políticas y configuraciones.
- El proveedor generará y entregará al MHCP con periodicidad mensual, el informe de seguimiento del servicio contratado, con las siguientes actividades mínimas, así:
  - Informe de eventos de actividad sospechosa atendidos durante el periodo respectivo.
  - Informe de los cambios realizados sobre la infraestructura monitoreada.
  - Informes del estado de los equipos o dispositivos monitoreados.
  - Informes de alertas, ataques, incidentes y tendencias.
  - Informes de los comportamientos más relevantes según la correlación realizada por el proveedor.
  - Informe de los incidentes de seguridad presentados.
  - Estadísticas de la información procesada.
  - Hallazgos realizados sobre la infraestructura tecnológica.
  - Análisis y recomendaciones sobre los resultados.
  - Informe sobre el estado del implantación, eventos procesados, alertas generadas, alertas procesadas y nivel de riesgo de seguridad.
- El servicio de SOC deberá generar informes técnicos y de seguimiento, los cuales se podrán generar de forma automática y/o bajo petición manual, con los logs recopilados, correlacionados y analizados. Adicionalmente, deberá generar indicadores y métricas del servicio, como mínimo los siguientes:
  - Alertas/incidentes por tipo.
  - Alertas/incidentes nuevos y resueltos.
  - Tiempo medio de creación de alertas7incidenrtes.
  - Tiempo medio de solución
  - Tendencias y top de alertas/incidentes.
  - Cumplimiento de acuerdos de servicio.
  - Nivel de disponibilidad del servicio.

	• El servicio de SOC deberá estar en la capacidad de generar los reportes en formato TXT, PDF, HTML, MS, Word y otros que sean compatibles con las herramientas de ofimática. • El proveedor deberá tener la capacidad según las necesidades del MHCP de crear otros reportes, según la necesidad de análisis de los datos recopilados en el servicio de monitoreo. • El servicio de SOC deberá contar con un portal de informes, métricas e indicadores a disposición del MHCP para efectuar el seguimiento respectivo. **4.13 Requerimientos Específicos – Integración y Análisis de LOGs.** a) El servicio de SOC deberá estar en capacidad de realizar la integración y monitoreo de los dispositivos y activos tecnológicos que conforman la infraestructura y activos tecnológicos importantes del MHCP, entre los cuales se incluyen sistemas operativos bases de datos, dispositivos de comunicaciones (routers, switches) y herramientas de seguridad (DLP, antivirus). Una vez integrada toda la plataforma tecnológica definida por el MHCP el proveedor establecerá el monitoreo y captura de todos los archivos de auditoria (logs) en los que se encuentran los eventos de seguridad que los dispositivos tecnológicos generan.
5	**CONDICIONES DEL SERVICIO:** Estas condiciones aplican a las actividades de soporte técnico que afecten la disponibilidad del servicio de SOC a. 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. b. 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. c. 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. d. 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. e. Garantizar la recuperación estable de los servicios en máximo ocho (8) horas,
6	**TRANSFERENCIA DE CONOCIMIENTO:** Durante la ejecución del contrato, se debe realizar la transferencia de conocimiento del servicio de SOC, para mínimo tres (5) funcionarios del Ministerio de Hacienda y Crédito Público con una intensidad horaria de mínimo de (8) horas, en la cual se provean conocimientos específicos de los fundamentos, administración, operación y manejo de las tecnologías y configuraciones implementadas en la plataforma, así como temas relacionados con la configuración, operación, integración y resolución de problemas. Esta transferencia de conocimiento puede ser realizada de forma presencial o virtual, de acuerdo a las condiciones de salubridad e higiene públicas.

	La planeación, programación y realización de esta actividad debe coordinarse con el supervisor del contrato.
7	**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.
8	**RECURSO HUMANO:** Para la ejecución del contrato el contratista deberá prestar el servicio de soporte y mantenimiento técnico con mínimo el recurso humano que se relaciona a continuación: **Un (1) Director de SOC-CERT:** Profesional Universitario en Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería en Telecomunicaciones. • Especialización o maestría en Administración o certificación PMP. • Certificaciones en Certified ec-council instructor y Computer hacking Forensic • Certificación CBCP • Certificación CISA • Certificación ISO 31000 Risk Manager • Certificación Certified ISO 22301 Lead Implementer • Experiencia de cinco (5) años certificada en Proyectos relacionados con Seguridad de la Información. **Un (1) Gerente de Proyecto:** Profesional Universitario en Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería en Telecomunicaciones. • Especialización o maestría en administración de empresas • Scrum Master Accredited Certification • Certificaciones en Certified ec-council instructor y Computer hacking Forensic • Certificación en ISO 27001:2013 Implementador Líder • Certificación ISO 31000:2018 Risk Manager • Certificado en PMP vigente. Experiencia de cinco (5) años certificada en Gerencia de Proyectos de Tecnología y/o Seguridad de la información **Cuatro (4) Ingenieros de Operación:** Profesional Universitario en Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería en Telecomunicaciones o carreras afines. • Experiencia de un (1) año certificado en Proyectos relacionados con Centros de Operación de Seguridad (SOC). • soporte 7x24 con operación remota.

	Nota: La hoja de vida del recurso humano deberá ser presentada con su oferta para validación, anotando que: 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 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 habilitantes señalados en los términos de referencia.

ANEXO No. 2
COTIZACIÓN ECONÓMICA

ITEM	SERVICIO	UNIDAD	CANTIDAD	VALOR 1 AÑO	VALOR 2 AÑOS	VALOR 3 AÑOS
1	Servicio Security Operation Center	Mes	12			
2	Servicio de análisis de vulnerabilidades y ethical hacking de acuerdo con las necesidades del MHCP Mínimo 10 aplicaciones 2 eventos por años	Global	2			
3	Servicio de análisis forense de incidentes de seguridad de la información	Hora	1			
	VALOR TOTAL CON IVA					

NOTA 1: El valor ofertado debe estar en pesos colombianos, y debe incluir la totalidad de actividades y recursos que sean requeridos para la realización de lo contemplado en el Anexo Técnico.

NOTA 2: Por favor incluir valores ajustados al peso de conformidad con lo establecido en la Ley 31 de 1992, la unidad monetaria y de cuenta del país es el peso colombiano, en tanto que las fracciones denominadas centavos no volvieron a ser acuñadas por dicha autoridad y por lo mismo no hacen parte de la unidad monetaria ni de cuenta en Colombia.

NOTA 3: Cotizar la totalidad de los Items con el detalle de cada uno

NOTA 4: Indicar si el servicio o el bien está exento del pago del impuesto al valor agregado – IVA

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 _____