ANEXO 09
FICHA TÉCNICA

OBJETO:
PRESTAR SERVICIOS DE MONITOREO Y ATENCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ID: OTIC-756)

ALCANCE:

ITEM	SERVICIO
1	SERVICIO SOC

ESPECIFICACIONES TÉCNICAS GENERALES

- Se deben prestar los servicios en el idioma español, para la interacción de las áreas de operación.
- Se deberá contar con una capacidad operativa 7x24, durante toda la ejecución del contrato.
- El contratista deberá realizar mensualmente, según lo establezcan las mejores prácticas de seguridad, análisis de tendencias sobre los eventos y plataformas monitoreadas por el servicio SOC.
- El contratista deberá proporcionar reportes bajo solicitud de la SuperSubsidio, por demanda, para el servicio SOC, según lo indicado en el ITEM Tabla general Plataforma Tecnológica.
- El contratista deberá generar y entregar boletines sobre alertas de seguridad que afecten la infraestructura.
- El contratista deberá entregar un informe mensual detallado sobre alertas mundiales que puedan afectar la seguridad sobre la infraestructura de sus clientes, dentro del servicio SOC.
- El contratista deberá monitorear los componentes de la infraestructura tecnológica indicada en la Tabla general Plataforma Tecnológica de forma proactiva.
- En caso de que el contratista comparta información con la SuperSubsidio por medio de un repositorio de información, este deberá garantizar los controles de acceso a dicho repositorio de información que sean necesarios y evitar el acceso no autorizado.
- El contratista deberá contar con procesos documentados para la eliminación segura de la información que ya no se requiera.
- El contratista deberá tener un SOC propio el cual debe contar con la certificación ISO/IEC 27001:2022 obligatoria.

- El contratista deberá contar con personal certificado en las herramientas con la que el SOC presta el servicio de monitoreo, correlación y demás.
- El contratista deberá tener los roles y responsabilidades del grupo de operaciones del SOC, claramente definido y documentado, en lo que respecta al monitoreo, correlación, análisis y de tendencias de seguridad y atención de requerimientos, manejo y contención de incidentes de seguridad, inteligencia de la amenaza y Hunting.
- Especificaciones técnicas del SIEM: Se requiere que el servicio sea prestado con una plataforma SIEM que sea del tipo Security Information and Event Manager que permita colectar, retener y correlacionar los eventos de seguridad de la infraestructura IT de la entidad. Se requiere que la solución de SIEM tenga integración de CMDB, a nivel de security mesh, customización de playbooks y reportes con SOAR.
- El contratista deberá detallar los procesos de:
    - Puesta a punto y auditoria del servicio de monitoreo y alertamiento.
    - Eliminación segura de la información que ya no se requiera, Gestión y Respuesta a incidentes,
    - Priorización de incidentes
    - Detección, categorización y alertamiento temprano y oportuno de incidentes de seguridad,
    - Priorización de atención de incidentes, Atención y escalamiento de requerimientos, Mejora Continua del servicio,
    - Gestión de cambio sobre la plataforma que soporta el servicio.
    - Controles de acceso a los repositorios de información que sean necesarios y de esta forma evitar el acceso no autorizado.
    - Modelo de Seguridad predictivo.

1. SERVICIO SECURITY OPERATION CENTER (SOC)

1.1 Especificaciones Técnicas Generales del Servicio SOC

Para la ejecución del contrato y el cumplimiento de los niveles de servicio solicitados, el contratista dispondrá del talento humano que él considere necesario, sin embargo, debeincluir mínimo lo siguiente:

Rol	Profesión en Colombia (Carreras Afines según SNIES)

Gerente de proyecto	Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. Posgrado: posgrado en Gerencia de Proyectos o Gerencia de Proyectos en Ingeniería de Telecomunicaciones o Administración de Empresas con Especialidad en Dirección de Proyectos. Certificaciones: PMP - Project Management Professional o Prince. Experiencia mínima: 10 años como profesional ejecutando proyectos y/o labores como director o gerente de proyectos en el sector de tecnología Experiencia especifica: 5 años en Ciberseguridad, Seguridad informática, Seguridad de la Informacióny.
	Certificaciones: Auditor Lider ISO 27001:2022, Cobit 5 o ITIL v4, CISM Certified Information Security Manager o CISSP Certified Information Systems Segurity Professional, Scrum Master
Consultor Senior despliegue	Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. Posgrado: Posgrado en Seguridad de la información o Seguridad informática o Seguridad de Redes Telemáticas o Seguridad Física y de la informática, Certificaciones: Certificación dada por el fabricante de la herramienta SIEM propuesta. Auditor Líder ISO 27001:2013 Auditor Lider ISO 27001:2022, CEH - Certified Ethical Hacker o CISM - Certified Information Security Manager o CISSP - Certified Information Systems Segurity Professional, Lead Cybersegurity Manager ISO/IEC 27032:2012 o Lead Cybersegurity Professional Certificate (LCSPC), Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC Experiencia mínima: 5 años como profesional ejecutando proyectos y/o labores consultor especialista en seguridad de la información o Ciberseguridad Experiencia especifica: 4 proyectos en Despliegue de la herramienta propuesta para SIEM y uno de estos contratos que contenga despliegue de mínimo 2 de las siguientes herramientas SOAR, HONEYPOT, PROTECCION DE MARCA, GESTION DE VULNERABILIDADES para el sector gobierno
Líder SOC	Profesión: título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines Posgrado: Posgrado en seguridad de la información o Seguridad de Redes Telemáticas o Seguridad Física y de la informática o Seguridad informática Certificaciones: CHFI - Computer Hacking Forensic Investigator, Auditor Interno ISO 27001:2013 o Auditor Líder ISO 27001:2013, Auditor Lider ISO 27001:2022, CEH - Certified Ethical Hacker, ITIL v3 o superior, Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC

	Experiencia mínima: 7 años como profesional ejecutando proyectos y/o labores consultor especialista en seguridad de la información o Ciberseguridad Experiencia especifica: 3 años como Líder SOC
Consultor Técnico SOC	Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines Certificaciones: Auditor Lider ISO 27001:2022, Seguridad en BGP con RPKI e IRR LACNIC. Curso o Certificación dada por el fabricante de la herramienta SIEM propuesta, Auditor Lider ISO 27001:2013, Cybersecurity Manager ISO/IEC 27032:2012 o Cyber Security Foundation Professional Certificate (CSFPC) Experiencia mínima: 4 años como profesional ejecutando proyectos y/o labores como consultor en Seguridad o Ciberseguridad Experiencia especifica: 3 proyectos en Ciberseguridad, Seguridad informática, Seguridad de la Información o SOC
Analista Nivel 2 de SOC	Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines Certificaciones: Certificación vigente como profesional, analista, especialista y arquitecto de seguridad de redes o su equivalente en la solución ofertada. Emitida por el fabricante. Experiencia mínima: 5 años como profesional ejecutando proyectos y/o labores como consultor en Seguridad o Ciberseguridad Experiencia especifica: 5 años en implementación y/o administración de soluciones de seguridad

1.2. Requisitos Generales del servicio

El contratista deberá tener un SOC propio, y este deberá estar ubicado en el territorio nacional

1.3. Especificaciones Técnicas Generales del SOC

- El SOC deberá tener la capacidad de integrarse con el SIEM de propiedad de la Superintendencia del Subsidio Familiar, el cual es ArcSight (logger y ArcMC) del fabricante MicroFocus el cual tendrá funcionamiento hasta el 31 de diciembre del 2024, así mismo deberá contar con la capacidad de configurar, parametrizar y gestionar dicho SIEM, o el SOC deberá poder utilizar herramientas de su propiedad o contar con la respectiva autorización de uso con terceros, para colectar, procesar, monitorear y correlacionar

como mínimo 4500 EPS (Eventos por segundo) sin costos adicionales para la entidad. Se deberá adjuntar los documentos vigentes necesarios que demuestren que el proveedor del servicio SOC está autorizado y cuenta con el entrenamiento de utilizar dichas herramientas.

- El servicio de SOC debe poder detectar amenazas para encontrar riesgos o brechas de seguridad desconocidas.
- El servicio de SOC debe estar en la capacidad de realizar monitoreo de disponibilidad e integridad de los dispositivos al servicio de monitoreo de Seguridad.
- El servicio de SOC debe tener la capacidad en tiempo real para detectar, recolectar, cruzar y consolidar patrones sobre la información recolectada, para poder alertar tempranamente los problemas, priorizando los activos más importantes.
- El SOC deberá realizar análisis del comportamiento de la infraestructura monitoreada para correlacionar incidentes y determinar proactivamente problemas en la operación.
- Las instalaciones del SOC deben contar con procedimientos, políticas de seguridad física para oficinas, recintos e instalaciones donde se encuentran los equipos con los cuales prestan el servicio, garantizando el esquema de seguridad sobre todos los componentes que lo integren, en el caso de utilizar herramientas basadas en nube deberán estar soportadas y garantizar el modo de alta disponibilidad.
- Debe garantizar la disponibilidad, confidencialidad, integridad, autenticación, autorización, no repudio, auditoría y privacidad de los datos y servicios soportados.
- El SOC deberá contar con un grupo interno con especialidad en atención de incidentes de seguridad, bajo un procedimiento claro y definido.
- El servicio debe permitir la integración del envío de alarmas automáticas vía correo electrónico.
- El servicio SOC, debe estar en capacidad de integrarse con otras herramientas relacionadas a este tipo de servicio, además el proponente debe estar en la capacidad de desarrollar las integraciones o los conectores y/o API necesarios para las distintas fuentes de datos, sin generar costos adicionales para la SuperSubsidio.
- El Servicio SOC deberá contar con tecnologías cognitivas para acelerar el proceso de investigación de potenciales incidentes de seguridad, dicha inteligencia artificial deberá analizar fuentes como: mensajes de X, información de foros, boletines de seguridad, artículos, Wikis, presentaciones de conferencias, reportes de analistas y bases de conocimiento.
- El servicio SOC deberá contar con una capacidad de retención de información mínima de seis (6) meses, para extracción de información de forma segura y generación de reportes.
- En caso de ser necesarios software de agentes en la infraestructura de la

entidad, se deberán suministrar los medios de instalación de los agentes que se requieran. Una vez se realice la Instalación, el contratista deberá realizar la respectiva configuración y certificación de que se está recibiendo eventos y alertas de monitoreo de los dispositivos informáticos de la infraestructura tecnológica relacionada en la Tabla general Plataforma Tecnológica

- Sólo deberá recibir los eventos que se requieran monitorear.
- El servicio SOC debe ser compatible con los métodos de recopilación de logs de la industria (Syslog, WMI, JDBC y SNMPv3).
- El servicio SOC debe vigilar y alertar cuando hay una interrupción en la recopilación de registros de un dispositivo. En otras palabras, si los registros no se ven desde un dispositivo en minutos determinados, generará una alerta.
- El servicio SOC deberá permitir el desarrollo de conectores personalizados sin la necesidad de editar archivos de configuración.
- El servicio SOC debe realizar un análisis en tiempo real de los eventos.
- El servicio SOC debe ser capaz de correlacionar los eventos y fuentes de datos de flujos de red en tiempo real.
- El servicio SOC debe contar con un portal web con comunicación segura que permita a la SSF tener una visualización de la información relevante respecto a amenazas emergentes, vulnerabilidades en su plataforma e incidentes de seguridad detectados por el servicio de SOC. Los contenidos de este portal web deberán estar orientados a mostrar la información del estado de la operación a nivel de monitoreo, investigación, atención de incidentes y gestión de requerimientos, para lo cual el servicio ofertado debe permitir la personalización del dashboard.
- El portal Web del servicio debe permitir descargar información de requerimientos de servicio, así como, publicaciones de seguridad y alertas generadas.
- El servicio SOC debe contar con un modelo de seguridad predictiva segmentada en fases, se debe indicar el detalle de estas fases.
- El servicio SOC debe contar con procesos automatizados de respuesta a incidentes y revisión de actividades anómalas.

1.4. Especificaciones Técnicas Generales del Servicio de Gestión de Vulnerabilidades.

- Gestión, atención y análisis de Incidentes: En el momento de detectar actividades sospechosas, se deberá realizar un análisis exhaustivo que permita determinar la naturaleza y el alcance del incidente, incluida la identificación de la causa raíz y el impacto potencial.
- Gestión y análisis de Vulnerabilidades: Realizar evaluaciones regulares de vulnerabilidades en la infraestructura de la organización y coordinar la aplicación de parches y actualizaciones de seguridad para mitigar posibles riesgos.
- Gestión y atención de incidentes de Seguridad: Coordinar y gestionar todos los aspectos relacionados con los incidentes de seguridad, incluyendo la comunicación

con las partes interesadas internas y externas, la documentación de los incidentes y la realización de informes 'post-mortem' para mejorar los procesos de seguridad.

- Gestión de alertas: Deberá gestionar los diferentes eventos, alertas o incidentes de seguridad informática y ciberseguridad.
- El proveedor deberá poner a servicio de la Superintendencia del Subsidio Familiar, al menos dos usuarios para poder realizar test de vulnerabilidades a demanda para los activos de información tanto a nivel externo aquellos expuestos a internet como interno aquellos expuesto únicamente en la red local de entidad.
- Se deberá renovar la suscripción del servicio Tenable IO por un año, actualmente se cuenta con vigencia hasta el 06 de diciembre de 2024, para la Superintendencia del Subsidio Familiar esto con el fin de garantizar de manera correcta las actividades de seguimiento a demanda de las vulnerabilidades.
- **Tipo de amenazas a analizar:** se enlistan a continuación sin embargo se aclara que no se deben limitar a las mencionadas a continuación:
    - Malware y ransomware.
    - Phishing.
    - Ataques DDoS.
    - Violencia de datos.
    - Vulnerabilidades y parches: Seguimiento de sistemas que no están actualizados y que pueden ser objetivos fáciles para atacantes
    - Tendencias en amenazas emergentes

  En general las nuevas tácticas, técnicas y procedimientos (TTP) utilizados por atacantes, y los incidentes relacionados con la falta de cumplimiento de regulaciones y su impacto en la seguridad.
- Las herramientas dispuestas para realizar el análisis podrán ser establecidas por el contratista según considere.
- El análisis deberá permitir realizar comparativos mensuales que permitan identificar patrones en el tiempo.

1.5. Especificaciones Técnicas Generales del Servicio de Ethical Hacking

- Deberá incluir un (1) Ethical Hacking, análisis de vulnerabilidades y retest, que permita validar las brechas de seguridad tanto internas como externas de la entidad.

- Las pruebas de Ethical Hacking se deberá realiza mediante las siguientes características técnicas:
    - Prueba de penetración externa: Evaluación de seguridad desde fuera del entorno de la empresa sin tener conocimiento previo de los sistemas.
    - Prueba de penetración interna: Evaluación de seguridad que simula a un atacante interno, como un visitante que cuenta solo con acceso físico a su oficina o un contratista con acceso limitado a determinados sistemas.

  En ambos casos se deberá validar como mínimo:
    a. Movimientos Laterales
    b. Escalamiento de privilegios
    c. SQL Injection
    d. Cross Site Scripting
    e. Ataques de directorio transversal
    f. Ataques por referencia directa a objetos

g. Ingeniería social
h. Informe del Ethical hacking
i. Plan de remediación y apoyo a la remediación.

Los activos de información de la entidad son aproximadamente 300.

1.6. Requerimientos Específicos - Correlación y Alertamiento de Eventos deSeguridad

- Los dispositivos tecnológicos de la SSF generan eventos que quedan registrados en los LOGs, los cuales deben ser monitoreados por el contratista. El contratista debe (basado en su experiencia y bases de conocimiento) diseñar el modelo de recolección de LOGs y arquitectura del servicio, con el fin de que se correlacionen y tengan en cuenta al menos los eventos relevantes de seguridad y alertamiento para que no impacte la normal ejecución de los servicios tecnológicos que apoyan los procesos de la SSF.
- El contratista y la SSF, al momento de la puesta en marcha del servicio, deben definir y configurar una serie de reglas, alertas y notificaciones clasificadas y priorizadas para detectar eventos e incidentes sobre la plataforma tecnológica que se estará monitoreando y reportarlas a la SSF cada vez que se encuentre en riesgo los principios de integridad, disponibilidad o confidencialidad de los activos tecnológicos.
- El contratista debe analizar, detectar y reportar ataques reales y potenciales a sistemas de información y bases de datos, mantener la trazabilidad y detectar comportamientos anómalos.
- Adicionalmente, se debe generar alertas de otras amenazas que puedan impactar a la SSF, como las identificadas en los reportes de análisis de tendencia de centros internacionales CSIRT/CERT o en las bases de datos de conocimiento del contratista, basado en los casos detectados a otros clientes que tenga el servicio ofrecido.
- El contratista debe establecer el protocolo para informar, reportar y/o escalar los eventos, alertas e incidentes que se detecten. Estos deberán ser reportados conforme a la categorización establecida por la entidad.
- El contratista debe informar de manera prioritaria y alertar sobre los cambios de seguridad, de configuración y críticos que se generen en las plataformas tecnológicas que se están monitoreando. Para esto se debe hacer una tabla de alertas, prioridad, tiempos y escalamiento.
- Los tipos de reglas, alertas y notificaciones deben enfocarse en eventos relevantes de seguridad. Las alertas mínimas requeridas deben 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 sistemas operativos. Ejecución de comandos especiales sobre bases de datos (dump,drop, delete, insert, update).
  - Cambios de parámetros técnicos, de configuración o de seguridad.
  - Cambios de configuración horaria.
  - Cambios no autorizados en recursos tecnológicos críticos. Actividades de conexión de cuentas de usuario final o administradores.
  - Actividades asociadas a manipulación de bitácoras técnicas.
  - (LOGs) o interrupciones en el envío de los LOGs. Actividades asociadas a conexión de acceso remoto.
  - Actividades asociadas a la no efectividad de controles en el ejercicio del monitoreo transaccional.
- Los canales de comunicación (red de datos) se centralizan en la ciudad de Bogotá y el contratista será encargado de dimensionar, diseñar, adquirir, instalar, configurar, operar y administrar la arquitectura tecnológica del servicio de monitoreo.
- El contratista debe definir el modelo de conexión de los dispositivos que serán monitoreados; especificar los requerimientos técnicos para cumplir con el servicio a contratar; apoyar y soportar a la SSF en la conexión, configuración y activación de las conexiones técnicas de los dispositivos a monitorear.
- El enlace o canal de comunicación entre la SSF y el contratista será por canal de internet dedicado y deberá disponer de ancho de banda suficiente para realizar las actividades de acuerdo al dimensionamiento del servicio hecho por el contratista.
- El contratista debe realizar las conexiones físicas y/o configuraciones lógicas entre los dispositivos que soportan el servicio y los elementos activos de red, sin que esto genere costos adicionales para la entidad.
- La arquitectura de la solución debe tener en cuenta que no se puede impactar la disponibilidad de los activos tecnológicos CORE de la SSF, ni de la infraestructura crítica que lo soporta. Por lo tanto, el servicio de monitoreo y respuesta a eventos de seguridad de la infraestructura informática debe 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 de la SSF.
- Asimismo, el SOC debe estar en capacidad de ofrecer a través de sus herramientas, las siguientes funciones:
  - Correlación de eventos.
  - Gestión de vulnerabilidades.
  - Monitoreo de integridad de archivos.
  - Detección de Amenazas/exposiciones mediante correlación y validación de postura de seguridad.

- El contratista debe mantener sincronizados todos los relojes de las herramientas de monitoreo con la hora legal para Colombia.
- El contratista debe realizar un monitoreo a los análisis de tendencia de amenazas y riesgos disponibles en Internet o en centros de respuesta a incidentes (CSIRT) que permita informar a la SSF alertas, tendencias, ataques y amenazas provenientes desde el ciberespacio y puedan afectar la infraestructura o los servicios que la SSF presta. Asimismo, el contratista debe disponer de servicios de Inteligencia ante Ciberamenazas.

1.7. Requerimientos Específicos – Almacenamiento de Logs

- El contratistadeberá asegurar el almacenamiento, disponibilidad y recuperación de los LOGs y la información generada en la ejecución del servicio contratado.
- El tiempo de custodia de la información técnica de LOGs será de seis (6) meses.
- El tiempo de custodia de los reportes, estadísticas, análisis de Tendencia, métricas e indicadores será por la duración del contrato.
- Es importante que el contratista defina un plan de respaldo en caso de borrados accidentales o provocados y presentarlo, una vez se firme el acta de inicio.

1.8. Requerimientos Específicos – Gestión de Incidentes de Seguridad

- El contratista deberá establecer un procedimiento apoyado con una metodología para la detección, alertamiento, notificación y seguimiento de eventos o incidentes de seguridad; también para informar puntos débiles de seguridad; definir responsabilidades que se deberían asignar para la gestión de incidentes y proponer mejoras de seguridad de la infraestructura tecnológica.
- Se debe contar con un experto para apoyo en respuesta a incidentes. En caso de tener un incidente informático deberán disponer el Personal SOC para apoyo en análisis forense.
- Se deben definir los medios de comunicación apropiados para la agilidad en la comunicación de los eventos e incidentes de seguridad, como:
  - Contacto telefónico
  - Correo electrónico
  - Mensajes vía celular y/o chat de contacto
- También debe contar con una herramienta para el seguimiento del estado de alertas e incidentes y establecer las responsabilidades, roles y los procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información. Para esto debe disponer de una herramienta de manejo de incidentes de seguridad y asegurar

los accesos a dicho servicio mediante el uso de protocolos seguros y autenticación de usuarios por medio de doble factor. El contratista debe proveer acceso a un 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.

- Los incidentes reaccionan ante las alertas generadas por el servicio de monitoreo y realizan todas las acciones necesarias para la detección, priorización, alerta, notificación y seguimiento de estado del incidente. Las actividades relacionadas con el manejo de incidentes serán:
    - Clasificar y priorizar las diferentes alertas generadas por el proceso de monitorización basado en un esquema de emergencia (triage) de acuerdo a la metodología CSIRT/CERT.
    - Alertar eventos detectados de acuerdo con los procedimientos establecidos con la SSF.
    - Notificar mediante los canales establecidos a los interlocutores que formen parte del proceso de escalado y toma de decisiones que establezca la SSF.
    - 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 (APT) y así definir reglas para detectar, reaccionar y contener ataques dirigidos.
- El contratista realizará 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 de la SSF; realizando recomendaciones a los administradores de la infraestructura y seguridad en la SSF a nivel de acciones a realizar y mejores prácticas.

1.9. Requerimientos Específicos – Informes, Métricas y Tendencias

- El contratista deberá elaborar reportes de monitoreo, cambios, alertas, tendencias, gestión, métricas, estadísticas que se entregarán de manera periódica (diario, semanal, mensual, semestral) según requerimiento.
- El contratista deberá 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. Además, debe quedar registros de cuándo, dónde y cómo se presentan los incidentes, así como definir nuevos reportes acorde a las necesidades de la SSF.
- El contratista emitirá con periodicidad mensual, el informe de seguimiento del servicio contratado, con los siguientes mínimos requeridos:
    - Informe de eventos de actividad sospechosa atendidos durante el periodo.
    - Informe de los cambios realizados sobre la infraestructura
    - Informes periódicos monitoreo, métricas y tendencias

- Informes del estado de los equipos o dispositivos de ciberseguridad monitoreados.
- Informes de alertas, ataques, incidentes y tendencias.
- Informes de comportamientos más relevantes según la correlación realizada por el contratista.
- Informe de los incidentes de seguridad presentados.
- Estadísticas de la información procesada
- Hallazgos realizados sobre la plataforma tecnológica
- Análisis y recomendaciones sobre los resultados

- Características y detalles técnicos mínimos requeridos que deben contener los informes:
  - Estado de la implantación. Se expone el estado actual en que se encuentra la implantación detallando las tecnologías integradas, las que no están integradas y las acciones adicionales para resolver conflictos con la integración.
  - Eventos procesados. Se presentan los datos referentes a los eventos procesados, las tecnologías que envían eventos e históricos con los datos previamente recopilados.
  - Alertas generadas. Se presentan todas las alertas generadas agrupadas por categoría y criticidad, junto con un historial de servicio.
  - Alertas procesadas. Se reflejan las tareas investigadas, categorizadas por criticidad, realizando un filtrado previo para eliminar falsos positivos.
  - Nivel de riesgo de seguridad de la información de los activos tecnológicos que se monitorean.
- Además de generar informes técnicos y de seguimiento, los cuales se podrán crear de forma automática y bajo petición Informes periódicos, manual, con los logs recopilados, correlacionados y métricas y tendencias de análisis, también se buscar generar indicadores y métricas ciberseguridad del servicio, como los mínimos siguientes:
  - Alertas/Incidentes por tipo
  - Alertas/Incidentes nuevos y resuelto
  - Tiempo medio de creación de alertas/incidentes
  - Tiempo medio de solución
  - Tendencias y top de alertas/incidentes
  - Cumplimiento de acuerdos de servicio
  - Nivel de disponibilidad del servicio
  - Los reportes deben ser generados en formato PDF o HTML o MS Word y otros que sean compatibles con las herramientas de ofimática.
  - El contratista debe estar disponible para crear otros reportes, según la necesidad de análisis de los datos recopilados en el servicio de monitoreo.
  - El contratista debe contar con un portal de informes, métricas e indicadores que usará la SSF para seguimiento, en el cual se deben entregar perfiles de usuarios al supervisor y los que autorice el mismo.

Se deben considerar las siguientes categorías como eventos mínimos a monitorear.

CATEGORÍAS MÍNIMAS DE EVENTOS DE SEGURIDAD A MONITOREAR	
ASPECTO	**ESPECIFICACIÓN**
Cuentas (Directorio activo, correo electrónico y sistemas de información)	Autenticación exitosa
	Autenticación fallida
	Usuario agregado a grupo especial local (cambio de privilegios)
	Usuario eliminado de grupo especial local (cambio deprivilegios)
	Usuario agregado a grupo especial global (cambio de privilegios)
	Usuario eliminado de grupo especial global (cambio deprivilegios)
	Usuario agregado a grupo especial universal (cambio deprivilegios)
	Usuario eliminado de grupo especial universal (cambio deprivilegios)
	Cuenta bloqueada
	Cuenta desbloqueada
	Contraseña cambiada
	Cambios de perfiles y permisos de cuentas privilegiadas
	Elevación de privilegios a usuarios
Bases de Datos	Autenticación exitosa - cuenta ordinaria
	Autenticación fallida - cuenta ordinaria
	Autenticación exitosa – SA
	Autenticación fallida – SA
	Cuenta bloqueada

	Cuenta desbloqueada
	Usuario agregado al grupo de SA
	Ejecución de instrucciones DML (Insert, Update y Delete) sobretablas en producción por usuarios no autorizados
	Ejecución de instrucciones DDL (Copia, (dump), Create, Drop,Alter) sobre tablas en producción por usuarios no autorizados
	Acceso de desarrolladores
	Update de cuentas
Cambios sobre plataformas	Software instalado en Servidor Windows y Linux
	Software desinstalado en Servidor Windows y linux
	Archivo crítico modificado (control de integridad)
	Cambio en políticas del Directorio Activo
	Eliminación de logs de auditoría
Conexiones	Acceso remoto RDP
Entorno Cloud	Deberá integrarse con la tecnología de evaluación de posturade seguridad en nube
	Deberá alertar riesgos identificados en la herramienta y permitir correlación para alertamiento por el SOC
Auditoría	Cambios de parámetros de seguridad
	Archivos críticos del sistema operativo modificados
	Cambios de políticas en Directorios Activos
	Eliminación de logs de auditoría
	Modificación de winlogon.exe
Sistema operativo	Intentos exitosos de conexión
	Intentos fallidos de conexión

	Cambios críticos de seguridad o configuración
	Actividades de administración de cuentas (creación, eliminacióncambio de perfiles)
	Actividades de cuentas de altos privilegios

1.10. Requerimientos Específicos de Captura, Integración y Análisis de LOGs

CAPTURA, INTEGRACIÓN Y ANÁLISIS DE ARCHIVOS DE AUDITORÍA O BITÁCORAS TÉCNICAS (LOGS).

- Para la prestación del servicio, el contratista debe contar con tecnología y herramientas especializadas en captura, integración y cumplir las condiciones técnicas necesarias para realizar la recopilación, correlación y análisis de eventos de seguridad sobre la plataforma tecnológica que la SSF defina.
- El contratista realizará la integración y monitoreo de los dispositivos y activos tecnológicos que conforman la infraestructura y activos tecnológicos priorizados por la SSF, entre los cuales se incluyen sistemas operativos (servidores y computadores personales), bases de datos, dispositivos de comunicación (routers, switches, AP) y herramientas de seguridad (DLP, antivirus). Una vez integrada toda la plataforma tecnológica definida por la SSF el contratista establecerá el monitoreo y captura de todos los archivos de auditoría (logs) en los que se encuentran los eventos de seguridad que los dispositivos tecnológicos generan.

1.11. Otras Especificaciones del servicio SOC

El servicio de gestión de SOC se enfocará en el tratamiento de eventos, identificación y atención de incidentes, los cuales estarán respaldados por un conjunto de metodologías y procesos diseñados para proporcionar una respuesta oportuna a los riesgos y amenazas que se enfrentan diariamente en SSF. En este sentido, el personal de SOC llevará a cabo el escalamiento y las comunicaciones utilizando la matriz de comunicaciones establecida, la cual definirá claramente la priorización para el uso de correo electrónico, herramienta de recepción de solicitudes, llamadas telefónicas, entre otros medios. Esta matriz garantizará una comunicación efectiva y eficiente con el personal de la SSF, permitiendo la rápida comunicación de incidencias y la toma de medidas inmediatas correspondientes.

Adicionalmente realizará el seguimiento a los eventos hasta que estos sean

cerrados adecuada y oportunamente.

De forma permanente el SOC realizará una valoración de las amenazas existentes en la región y el mundo, determinando cuál de estos exponen a un riesgo a SSF, resumiendo los resultados en Boletines o Informes extraordinarios de SOC.

Los servicios de gestión de SOC realizarán seguimiento 7x24 a los ataques originados desde Internet al igual que los originados al interior de SSF.

El SOC, debe definir la matriz de escalamiento en común acuerdo con los responsables de seguridad en SSF clarificando el nivel de escalamiento según el tipo y nivel de incidente al igual que la ausencia de atención a las actividades sospechosas e incidentes previamente declarados.

Cuando un evento de seguridad ocurre o está en suceso, el SOC deberá identificarlo y estar en la capacidad de relacionarlo de forma directa o indirecta con otros eventos de seguridad asociados. Estos, constituyen el conjunto de eventos que permite determinar el patrón de ataque, a este conjunto de eventos finitos se les denomina eventos correlacionados.

2. Tipos de Alertas

En la siguiente tabla se muestra un ejemplo de los tipos de alertas mínimas que se deben definir, donde se incluye al menos la regla, la severidad, los tiempos y el nivel deescalamiento:

Nombre de la alerta	Descripción	Regla	Severidad	Tiempo de escalamiento	Escalamiento
A. Intentos de ingreso fallido en un día	Usuarios que registren 6 o más intentos fallidos de ingreso en un día, al autenticarse.	>=6	Baja	24 horas máximo	• Usuario • Supervisor de usuario • Administradores TI • Grupo incidentes
B. Intentos de ingreso fallido repetitivos en una semana	Usuarios que registren 6 o más intentos fallidos de ingreso en un día, en más de tres ocasiones en una semana	>=3 A (en una semana)	Media	24 horas máximo	• Usuario • Supervisor de usuario • Administradores TI • Grupo incidentes
C. Intentos de ingreso fallido repetitivos en un mes	Usuarios que registren 6 o más intentos fallidos de ingreso en un día, en más de tres ocasiones en una semana y en 2 o más ocasiones en un mes	>=2 B (en un mes)	Alta	24 horas máximo	• Usuario • Supervisor de usuario • Administradores TI • Grupo incidentes
D. Cuenta de usuario borrada	Cuenta de usuario eliminada por un usuario administrador	>=1	Muy Alta	8 horas máximo	• Usuario • Supervisor de usuario • Administradores TI • Grupo incidentes

Imagen de referencia

Dependiendo de las alertas creadas, los incidentes detectados por dichas alertas se deben clasificar en niveles alto, medio y bajo y es responsabilidad del Contratista definir los niveles de severidad para ser aprobados por la SSF, de acuerdo a la criticidad del evento o del impacto de los activos incluidos en el alcance de monitoreo técnico.

3. Acuerdos de Niveles de Servicio SLA

3.2. Implementación del Servicio

El contratista realizará el levantamiento de la información requerida para la configuración, implementación y funcionamiento de la solución SIEM y/o dispositivos recolectores (sensores), para lo cual la SSF brindará apoyo y acompañamiento.

SLA IMPLEMENTACIÓN DEL SERVICIO	
ASPECTO	**ESPECIFICACIÓN**
DISEÑO DEL SERVICIO	Actividades:
	Inicio del contrato
	Entrega de la documentación de procesos solicitados y de la documentación específica solicitada referente al equipo de trabajo.
	Personalización de la arquitectura propuesta.
	Plan de trabajo y autorización de implementación.
	Tiempo: Una (1) semana desde la firma del acta de inicio
INTEGRACIÓN Y PUESTA EN MARCHA	Configuración y conexión de dispositivos, ajustes técnicos,estabilización de plataforma tecnológica.
	Actividades: Definición de integración de logs de los equipos,dispositivos y bases de datos definidas por la SSF, que incluya prueba, configuración y conexión. Creación, prueba yafinamiento de las alertas requeridas por la SSF.
	Medio de solicitud: Correo electrónico, actas de reunión
	Responsable: el Contratista
	Tiempo: El establecido en el plan de trabajo aprobado por elsupervisor.
ENTREGA DE CONFIGURACIÓN	"Al finalizar el contrato, se debe realizar un empalme con el nuevo servicio SOC donde se deben entregar todas las configuraciones realizadas durante la ejecución del contrato. Esto debe realizarse en máximo una semana."

3.3. Disponibilidad del Servicio SOC

La Entidad deja claro que, si la disponibilidad es inferior a la establecida en este numeral, se realizará el respectivo descuento al contratista en el pago mensual del servicio.

SLA IMPLEMENTACIÓN DEL SERVICIO	
ASPECTO	**ESPECIFICACIÓN**
Dispositivo de recolección de logsubicado en la SSF	Horario: 7x24 Porcentaje de disponibilidad: 99,96%
Enlace o canal de comunicación entrela SSF y Contratista	Horario: 7x24 Porcentaje de disponibilidad: 99,7%
Sistema de monitoreo y respuesta a eventos de seguridad de la infraestructura informática ubicado eninstalaciones del contratista	Horario: 7x24 Porcentaje de disponibilidad: 99,96%
Portal de informes, métricas e indicadores que usará la SSF y el SOC para seguimiento	Horario: 7x24 Porcentaje de disponibilidad: 99.6% Se aclara que la disponibilidad requerida es para consultas de la SSF, y se entiende que si los analistas del SOC requieren su consulta, el portal debe estar habilitado.

3.4. Descuentos por menores niveles de servicio SOC

La siguiente tabla será la base para las conciliaciones mensuales que han de determinarel pago del servicio.

Indicador	**Peso Porcentual sobre el servicio**	**Forma de Medición**	**Fuente**	**Meta**	**Descuentos**		
					De <=	**A >**	**Desc.**
Dispositivos de recolección delogs	35%	Promedio de tiempo disponible de los dispositivos de recolección de logs	Herramienta de Gestión del proveedor	99,96%	100	99,96	0%
					99,95	91	10%
					90	81	20%
					80	0	100%
Enlace o canalde comunicación entre la SSF yContratista	25%	Promedio de tiempo disponible del o los Enlace(s) o canal(es) de	Herramienta de Gestión del proveedor	99,70%	100	99,7	0%
					99,6	91	10%
					90	81	20%

		comunicación entre la SSF y Contratista			80	0	100%
Sistema de Monitoreo y respuesta a eventos de seguridad de la infraestructura informática ubicado eninstalaciones del contratista	35%	Promedio de tiempo disponible del SOC Sistema de monitoreo y respuesta a eventos de seguridad de la infraestructura informática	Herramienta de Gestión del proveedor	99,96%	100	99,96	0%
					99,95	91	10%
					90	81	20%
					80	0	100%
Portal de informes, métricas e indicadores que usará la SSF y el SOC para seguimiento	5%	Promedio de tiempo disponible Portal de informes, métricas e indicadores	Herramienta de Gestión del proveedor	99,6%	100	99,6	0%
					99,5	91	10%
					90	81	20%
					80	0	100%