



...

CONTRATO N° SSF SASI 429 de 2024 UT RC SOC	
DATOS BÁSICOS DEL CONTRATO	
OBJETO DEL CONTRATO	PRESTAR SERVICIOS DE MONITOREO Y ATENCION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION
VALOR TOTAL DEL CONTRATO	\$ 574.530.000
FECHA ACTA DE INICIO	DICIEMBRE 09 DE 2024
FECHA PREVISTA DE TERMINACIÓN	ENERO 09 DE 2026

...

OBLIGACIONES ESPECIFICAS	ACTIVIDAD	MEDIO DE VERIFICACIÓN
OBLIGACIÓN ESPECIFICA 1: Dar cumplimiento al, objeto contractual, así como a todas y cada una de las especificaciones técnicas y entregables, definidas en el ANEXO - Ficha Técnica.	<ul style="list-style-type: none"> Se elaboró y entregó Plan de Trabajo Implementación SOC. Se realizó conexión de los equipos indicados por la SSF al SOC de Realtime. Se elaboró y entregó Informe de Implementación SOC SSF Se realizó el escaneo de vulnerabilidades y Ethical Hacking a los servicios expuestos supersubsidio.gov.co y ssf.gov.co Se elaboró y entregó el documento Informe de Escaneo de Vulnerabilidades y Ethical Hacking. Se realizó el monitoreo de eventos Se elaboró y entregó el informe de monitoreo mensual realizado Informe mensual SSF. 	<ul style="list-style-type: none"> Plan de Trabajo Implementación SOC Informe de Implementación SOC SSF. Informe de escaneo de vulnerabilidades y Ethical Hacking SSF. Informe mensual SSF. Actas de Reunion
OBLIGACIÓN ESPECIFICA 2: Allegar dentro de los cinco (5) días hábiles siguientes a la firma del acta de inicio las hojas de vida del equipo de trabajo para validación y aprobación del Supervisor del contrato, así como el cronograma de trabajo que se desarrollara durante la ejecución del contrato.	<p>Se entregaron hojas de vida de las siguientes personas el día:</p> <ul style="list-style-type: none"> Cesar Dario Cordoba – Gerente de Proyectos Eduard Mendez – Consultor Senior de Despliegue. Jensy Martinez – Líder SOC Rafael Morales – Consultor Técnico SOC Ronald Vargas – Analista Nivel 2 SOC <p>Así mismo, se elaboró y entregó el documento Plan de Trabajo Implementación SOC que contiene el cronograma a desarrollar para la implementación.</p>	<ul style="list-style-type: none"> Hojas de Vida del equipo SOC Plan de Trabajo Implementación SOC (Cronograma)
OBLIGACIÓN ESPECIFICA 3: Activar, configurar y poner en funcionamiento oportunamente las herramientas tecnológicas según sea el caso, de acuerdo con las especificaciones indicadas, de acuerdo con las buenas prácticas dadas por el fabricante.	<p>Se realizó la activación, configuración y puesta en funcionamiento del SOC para los dispositivos indicados por la SSF, de acuerdo con las buenas prácticas del fabricante.</p> <p>Se elaboró y entregó Informe de Implementación SOC SSF en donde se evidencia la actividad.</p>	<ul style="list-style-type: none"> Informe de Implementación SOC SSF

...

OBLIGACIONES ESPECIFICAS	ACTIVIDAD	MEDIO DE VERIFICACIÓN
OBLIGACIÓN ESPECIFICA 4: Una vez implementadas las herramientas tecnológicas utilizadas en el servicio de acuerdo con los lineamientos establecidos, deberá realizar sesiones de mínimo 8 horas en transferencia de conocimiento al equipo de trabajo de la SSF, por cada herramienta y servicio implementado.	Se entregó y aprobó el Plan de Trabajo Implementación SOC , que contiene la programación de la transferencia de conocimiento. Las sesiones de transferencia de conocimiento están programadas en sesiones de dos horas los días 21, 22, 23 y 24 de enero de 2024. Carta de Compromiso de Transferencia de Conocimiento.	<ul style="list-style-type: none"> Plan de Trabajo Implementación SOC (Programación Transferencia) Carta de Compromiso de Transferencia de Conocimiento
OBLIGACIÓN ESPECIFICA 5: Utilizar una metodología de gestión de proyectos de amplio uso en el mercado para el control de este y aplicar las mejores prácticas de administración como es ITIL V3 o superior, NIST, FIRST.6.	Se elaboró, entregó y explicó en la reunión de inició, el documento Plan de Trabajo Implementación SOC que contiene la WBS del alcance y el cronograma a seguir para lograr los requerimientos del proyecto, usando la metodología de gestión de proyectos del PMI.	<ul style="list-style-type: none"> Plan de Trabajo Implementación SOC
OBLIGACIÓN ESPECIFICA 6: Adelantar las actividades de integración de las herramientas tecnológicas definidas, en el caso que aplique.	Se configuró la herramienta SOC y se integró a esta los dispositivos definidos por la SSF, estas integraciones quedan descritas en el documento Informe de Implementación SOC para SSF.	<ul style="list-style-type: none"> Informe de Implementación SOC SSF.
OBLIGACIÓN ESPECIFICA 7: El CONTRATISTA deberá entregar dentro de los siguientes diez (10) días hábiles siguientes a la firma del acta de inicio el procedimiento integral para la gestión de incidentes de seguridad y evaluación de vulnerabilidades,	Se elaboró y entregó el procedimiento de gestión de incidentes y el procedimiento de Gestión de Vulnerabilidades y Ethical Hacking que contiene los requisitos establecidos en este numeral.	<ul style="list-style-type: none"> Procedimiento de Gestión de Incidentes. Procedimiento de Gestión de Vulnerabilidades y Ethical Hacking.

...

OBLIGACIONES ESPECIFICAS	ACTIVIDAD	MEDIO DE VERIFICACIÓN
<p>incluyendo técnicas de Ethical Hacking, en el cual se establezca la periodicidad de los informes y reportes que soporten la gestión y operación del SOC y de los servicios contratados, los cuales deberán contener como mínimo la siguiente información:</p> <ul style="list-style-type: none">• Informe de eventos de actividad sospechosa atendidos durante el periodo.• Informes del estado de los equipos o dispositivos monitoreados.• Informe de alertas, ataques, incidentes y tendencias.• Información de las amenazas identificados provenientes del ciberespacio.• Informes de comportamientos más relevantes según la correlación realizada por el proponente.• Informe de los incidentes de seguridad presentados.• Cumplimiento de los Acuerdos de Niveles de Servicio.• Información de la gestión realizada sobre los requerimientos, casos, eventos o situaciones reportadas por la entidad.• Estadística de la información procesada.• Hallazgos realizados sobre la plataforma tecnológica.• Análisis y recomendaciones sobre los resultados.		

...

OBLIGACIONES ESPECIFICAS	ACTIVIDAD	MEDIO DE VERIFICACIÓN
OBLIGACIÓN ESPECIFICA 8: Prever el plan de recuperación y contingencia del servicio contratado ante los eventos que puedan afectar el cumplimiento de la ejecución de este tecnológicas.	Se elaboró y entregó un Plan de Recuperación y Contingencia de la Plataforma del SOC	<ul style="list-style-type: none"> Plan de Recuperación y Contingencia Plataforma SOC.
OBLIGACIÓN ESPECIFICA 9: Informar a la SSF sobre las amenazas identificadas y que puedan generar la interrupción del servicio contratado.	Se elaboró y entregó Informe mensual SOC en la cual se informaron las amenazas identificadas, las cuales puede impactar a la SSF.	<ul style="list-style-type: none"> Informe mensual SSF.
OBLIGACIÓN ESPECIFICA 10: Identificar e implementar las estrategias de recuperación apropiadas para restablecer el servicio contratado dentro de las franjas de tiempo pactadas.	Se elaboró y entregó un Plan de Recuperación y Contingencia de la Plataforma del SOC	<ul style="list-style-type: none"> Plan de Recuperación y Contingencia Plataforma SOC.
OBLIGACIÓN ESPECIFICA 11: Establecer, juntamente con la SSF, la responsabilidad por los controles que deben implementarse tanto por SSF como por el contratista para garantizar el funcionamiento de las estrategias de continuidad del servicio objeto del contrato.	Se elaboró y entregó un Plan de Recuperación y Contingencia de la Plataforma del SOC , en el cual quedaron definidas las responsabilidades de la UT para la continuidad del servicio.	<ul style="list-style-type: none"> Plan de Recuperación y Contingencia Plataforma SOC.
OBLIGACIÓN ESPECIFICA 12: Socializar o divulgar, al inicio y durante la ejecución del contrato, con el equipo de trabajo que realiza las actividades, las políticas de seguridad y privacidad de la información y políticas de tratamiento de datos personales.	Se socializaron con el equipo de trabajo la socialización de las políticas de seguridad y privacidad de la información y las políticas de tratamiento de datos personales.	<ul style="list-style-type: none"> Acta de asistencia Presentación de Políticas de Seguridad y Privacidad de la Información y las Políticas de Tratamiento de Datos Personales.

...

OBLIGACIONES ESPECIFICAS	ACTIVIDAD	MEDIO DE VERIFICACIÓN
OBLIGACIÓN ESPECIFICA 13: Entregar a la finalización del contrato las copias de seguridad y los casos de uso realizados durante el contrato para cada uno de los componentes.	Se elaboró y entregó el documento Plan de Trabajo Implementación SOC que contiene la actividad de entrega de copias de seguridad y casos de uso al finalizar el contrato.	<ul style="list-style-type: none"> Plan de Trabajo Implementación SOC (Entrega de Copias de Seguridad y Casos de Uso)
OBLIGACIÓN ESPECIFICA 14: Desarrollar capacidades predictivas para anticipar posibles amenazas cibernéticas y actuar de manera proactiva en su prevención.	Se realizó monitoreo de eventos en la cual se involucran actividades de análisis de comportamiento y correlación de eventos. Se elabora y entrega Informe mensual SSF en la cual se informaron las amenazas identificadas, las cuales puede impactar a la SSF.	<ul style="list-style-type: none"> Informe mensual SSF.
OBLIGACIÓN ESPECIFICA 15: El contratista deberá Establecer un sistema eficiente de alerta temprana que permita notificar de manera inmediata sobre amenazas latentes y posibles incidentes de seguridad.	Se acordó el sistema de alertamiento temprano en el documento Procedimiento de Gestión de Incidentes.	<ul style="list-style-type: none"> Procedimiento de Gestión de Incidentes.
OBLIGACIÓN ESPECIFICA 16: El contratista deberá Establecer y promover la adopción de estándares y buenas prácticas en seguridad digital, en línea con el marco normativo existente.	Se elaboró, entregó y explicó en la reunión de inicio, el documento Plan de Trabajo Implementación SOC que contiene los roles y responsabilidades del equipo de trabajo del SOC, además contiene la WBS del alcance y el cronograma a seguir para lograr los requerimientos del proyecto, usando la metodología de gestión de proyectos del PMI. El Plan de trabajo contempla las capacidades de recursos humanos para la seguridad de acuerdo con SOMM-Security Operations Model, la gestión de IT para proveer el servicio de acuerdo	<ul style="list-style-type: none"> Plan de Trabajo Implementación SOC.

...

OBLIGACIONES ESPECIFICAS	ACTIVIDAD	MEDIO DE VERIFICACIÓN
	con las buenas prácticas de la ISO 20000-1 y el cumplimiento de monitoreo de acuerdo con la ISO 27001.	
OBLIGACIÓN ESPECIFICA 17: El contratista deberá Implementar un enfoque integral de gestión de riesgos e incidentes de seguridad digital, determinando roles y responsabilidades en la entidad.	Se elaboró, entregó y explicó en la reunión de inicio, el documento Plan de Trabajo Implementación SOC que contiene los roles y responsabilidades del equipo de trabajo del SOC, además contiene la WBS del alcance y el cronograma a seguir para lograr los requerimientos del proyecto, usando la metodología de gestión de proyectos del PMI.	<ul style="list-style-type: none"> Plan de Trabajo Implementación SOC
OBLIGACIÓN ESPECIFICA 18: El contratista deberá Establecer programas de capacitación continua para el personal la SSF de la OTIC, manteniéndolos actualizados sobre las últimas tendencias y técnicas en ciberseguridad	Se entregó y aprobó el Plan de Trabajo Implementación SOC , que contiene la programación de la transferencia de conocimiento. Las sesiones de transferencia de conocimiento están programadas en sesiones de dos horas los días 21, 22, 23 y 24 de enero de 2024. Otras capacitaciones serán acordadas en las fechas y temas acordadas. Carta de Compromiso de Transferencia de Conocimiento.	<ul style="list-style-type: none"> Plan de Trabajo Implementación SOC (Programación Transferencia) Carta de Compromiso de Transferencia de Conocimiento
OBLIGACIÓN ESPECIFICA 19: El objeto contractual se desarrollará bajo las directrices e instrucciones de los estándares mínimos a los que se refiere la ISO 20000-1, ISO 27001, SOMM-Security Operations Model.	Se elaboró, entregó y explicó en la reunión de inicio, el documento Plan de Trabajo Implementación SOC que contiene los roles y responsabilidades del equipo de trabajo del SOC, además contiene la WBS del alcance y el cronograma a seguir para lograr los requerimientos del proyecto, usando la metodología de gestión de proyectos del PMI. El Plan de trabajo contempla las capacidades de recursos humanos para la seguridad, la gestión de IT para proveer el servicio y el cumplimiento de monitoreo de acuerdo con la ISO 27001.	<ul style="list-style-type: none"> Plan de Trabajo Implementación SOC
OBLIGACIÓN ESPECIFICA 20: Todos los documentos o información que se produzcan en desarrollo del contrato serán de uso exclusivo de la Superintendencia del Subsidio Familiar y	Se firmó la clausula de confidencialidad en el contrato, la cual asegura que los documentos e información no serán utilizados en otros escenarios y no se divulgará dicha información.	<ul style="list-style-type: none"> Contrato firmado entre las partes.



...

OBLIGACIONES ESPECIFICAS	ACTIVIDAD	MEDIO DE VERIFICACIÓN
EL CONTRATISTA se obliga a no utilizarlos para fines distintos a los previstos en el contrato, ni divulgar la información que se le suministre, ni los resultados de su trabajo, obligándose a mantener confidencialidad de los mismos de conformidad con la ley, so pena de las acciones civiles, administrativas o penales a que haya lugar.		