Supersubsidio

CONTRATO DE PRESTACIÓN DE SERVICIOS No. 429 DE 2024 SUSCRITO ENTRE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR Y UT RC SOC SSF 2024

Entre los suscritos **KATERIN GÓMEZ OLAYA**, mayor de edad, identificada con cédula de ciudadanía No. 1.024.479.097., obrando en su calidad de Secretaria General, de la **SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR**, con NIT. 860.503.600-9, entidad del Orden Nacional, creada mediante la Ley 25 del 24 de febrero de 1981, adscrita al Ministerio del Trabajo y Seguridad Social, hoy Ministerio del Trabajo, en uso de las atribuciones que le confiere la Ley 80 de 1993, la Ley 1150 de 2007, el Decreto 1082 de 2015 y demás normas reglamentarias, actuando de conformidad con la Resolución No. 0719 del 21 de octubre de 2024 y posesionada a través del acta 020 del 21 de octubre de 2024, actuando de conformidad con la delegación contenida en la Resolución No. 0426 del 30 de mayo del 2014., quien en adelante se denominará la **SUPERINTENDENCIA**, de una parte, y por la otra **UT RC SOC SSF 2024** con **NIT**. No. 901894091-4, Integrada por REALTIME CONSULTING & SERVICES SAS con Nit. 900.127.417-9, domiciliada en la ciudad de Bogotá D.C. REALTIME C & S SAS con Nit. 900.527.088-5, domiciliada en la ciudad de Bogotá D.C CONVIEST SAS con Nit. 900.915.742-9 representada por **ANA MILENA MORALES LÓPEZ,** identificada con la Cedula de Ciudadanía No. 52.705.962 quien afirma no encontrarse incurso, ni ella ni su representada, en ninguna de las causales de inhabilidad e incompatibilidad, prohibición o conflicto de interés, del orden constitucional y legal y en especial las señaladas en los artículos 8 y 9 de la Ley 80 de 1993, Ley 1474 de 2011 y demás disposiciones vigentes sobre la materia, ni ser responsable fiscalmente en virtud de lo señalado en la Ley 610 de 2000 e igualmente declara estar al día con sus empleados en el pago de los aportes al Sistema de Seguridad Social Integral en salud, pensiones y riesgos laborales, así como en el pago de aportes parafiscales (caja de compensación familiar, SENA e ICBF), según certificaciones expedidas de fecha trece (13) de noviembre de 2024 por los representantes legales y la contadores de la empresa REALTIME CONSULTING & SERVICES SAS REALTIME C & S SAS y D.C CONVIEST SAS, hemos acordado celebrar el presente contrato de prestación de servicios, previas las siguientes consideraciones

1. Que, mediante Resolución No. 0753 del 31 de octubre de 2024, se ordenó ordena la apertura de la Selección Abreviada Subasta Inversa SSF-SASI 003 DE 2024 en la página del SECOP II, portal único de contratación, https://www.colombiacompra.gov.co/secop/secop-II, contemplada en el Plan de Adquisiciones de la entidad, cuyo objeto es “PRESTAR SERVICIOS DE MONITOREO Y ATENCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ID: OTIC-756)”,

2. Que conforme el cronograma del proceso el 13/11/2024, se realizó el cierre de la Selección Abreviada subasta inversa SASI 003 DE 2024 y se recibieron dos (2) ofertas, de conformidad con la información que reposa en la plataforma SECOP II, así:

CONTRATO DE PRESTACIÓN DE SERVICIOS No. 429 DE 2024 SUSCRITO ENTRE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR Y UT RC SOC SSF 2024

	OFERENTES	INTEGRANTES	NIT
1	B2B TIC SAS	conformada por B2B TIC SAS (70%) y por INNOVA TECH IT SAS (30%)	NIT 901.003.982-1 NIT 900.860.807-0
2	UT RC SOC SSF 2024	conformada por REALTIME CONSULTING & SERVICES SAS(8%), REALTIME C & S SAS (42%), CONVIEST SAS (50%).	Nit. 900.127.417-9 NIT. 900.527.088-5 NIT. 900.915.742-9,

3. Que, Una vez concluida la evaluación preliminar de las ofertas presentadas, dentro del proceso de SELECCIÓN ABREVIADA SUBASTA INVERSA SSF SASI-003 DE 2024, los Miembros del Comité Evaluador, recomiendan publicar el presente consolidado preliminar junto con la verificación jurídica, técnica y financiera para que el proponente conforme el parágrafo 1° del artículo 5 de la ley 1150 de 2007, parágrafo 1 del artículo 5º de la Ley 1882 de 2018 y artículo 2.2.1.2.1.2.20. numeral 4 del Decreto 1082 de 2015, presenten observaciones al informe preliminar de evaluación y subsane lo requerido, si hay lugar a ello, por lo anterior, se corre traslado por un término de tres (03) días hábiles, correspondiente a los días 19, 20 y 21 de noviembre de 2024.

4. Que, publicado el informe preliminar de evaluación conforme el parágrafo 1° del artículo 5 de la ley 1150 de 2007, parágrafo 1 del artículo 5º de la Ley 1882 de 2018 y artículo 2.2.1.2.1.2.20. Numeral 4 del Decreto 1082 de 2015, se corrió traslado de este por el término señalado en la ley, plazo dentro del cual se recibieron las subsanaciones de UT RC SOC SSF 2024, además, se dio respuesta a la observación presentada al informe preliminar por parte de los oferentes.

5. Que, el proponente B2B TIC SAS, dentro del término estableció para tal fin NO envió los DOCUMENTOS DE SUBSANACION, no cumpliendo con el requerimiento de subsanación de la evaluación técnica., debido a esto, se encuentran inmersa dentro de la causal de rechazo No. 3.7.12 del pliego de condiciones, que señala:

3.7.12. Cuando el proponente, no allegue los documentos, las aclaraciones y/o explicaciones, en el término concedido para tal evento.

Que teniendo en cuenta las subsanaciones allegadas en la plataforma transaccional SECOP II, dentro del término concedido para tal fin, el Comité

designado procedió a emitir el informe definitivo de evaluación el cual se consolida de la siguiente manera:

Nº	NOMBRE DEL PROPONENTE	REQUISITOS JURÍDICOS	REQUISITOS TÉCNICOS	REQUISITOS FINANCIEROS	RESULTADO
1	B2B TIC SAS	**NO CUMPLE**	**NO CUMPLE**	CUMPLE	**RECHAZADA**
2	UT RC SOC SSF 2024	CUMPLE	CUMPLE	CUMPLE	**HABILITADO**

Que al resultar un solo Oferente hábil se tiene en cuenta el numeral 1.19 del Pliego de condiciones.

1.19. UN SOLO OFERENTE HÁBIL La entidad podrá adjudicar el contrato cuando sólo se haya presentado una propuesta y esta cumpla con los requisitos habilitantes exigidos, y siempre que la oferta satisfaga los requerimientos contenidos en el pliego de condiciones, de conformidad con el artículo 2.2.1.1.2.2.6 del Decreto 1082 de 2015.

6. Que en consecuencia los miembros del Comité Asesor en Contratación recomendaron al Ordenador del Gasto (E), adjudicar el proceso de Selección Abreviada por Subasta Inversa Electrónica SSF-SASI-003 de 2024, cuyo objeto es “PRESTAR SERVICIOS DE MONITOREO Y ATENCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ID: OTIC-756)”, al proponente **UT RC SOC SSF 2024 con NIT. No. 901894091-4,** Integrada por REALTIME CONSULTING & SERVICES SAS con Nit. 900.127.417-9, domiciliada en la ciudad de Bogotá D.C. REALTIME C & S SAS con Nit. 900.527.088-5, domiciliada en la ciudad de Bogotá D.C CONVIEST SAS con Nit. 900.915.742-9 representada por **ANA MILENA MORALES LÓPEZ,** identificada con la Cedula de Ciudadanía No. 52.705.962, por el valor total de **QUINIENTOS SETENTA Y CUATRO MILLONES QUINIENTOS TREINTA MIL PESOS ($574.530.000)** incluido IVA, y todos los costos directos e indirectos, los impuestos, tasas y contribuciones a que haya lugar que conlleve la celebración y ejecución total del contrato

7. Que la empresa UT RC SOC SSF 2024 con NIT. No. 901894091-4, Integrada por REALTIME CONSULTING & SERVICES SAS con Nit. 900.127.417-9, domiciliada en la ciudad de Bogotá D.C. REALTIME C & S SAS con Nit. 900.527.088-5, domiciliada en la ciudad de Bogotá D.C CONVIEST SAS con Nit. 900.915.742-9 ha cumplido con el pago de aportes a seguridad social integral y parafiscal, conforme a la certificación aportada durante el proceso de selección.

8. Que, según certificación de la Contraloría Delegada para Responsabilidad Fiscal, Intervención Judicial y Cobro Coactivo de la Contraloría General de la Republica,

una vez consultado el Sistema de Información del Boletín de Responsabilidades Fiscales -SIBOR de fecha 02 de diciembre de 2024, ni la persona jurídica ni el representante legal aparecen reportados como responsables fiscales.

9. Que según certificación del sistema SIRI, de la Procuraduría General de la Nación, de fecha 02 de diciembre de 2024, ni la persona jurídica ni el representante legal aparecen reportados con antecedentes disciplinarios.

10. Que una vez revisado el certificado de antecedentes y requerimiento Judicial de la fecha 02 de diciembre de 2024, expedido por la Policía Nacional de Colombia, la ciudadana ANA MILENA MORALES LÓPEZ, identificada con la Cedula de Ciudadanía No. 52.705.962, representante legal de UT RC SOC SSF 2024, Sociedad Comercial con domicilio principal en la Ciudad de Bogotá, no tiene asuntos pendientes con las autoridades judiciales.

11. Que una vez revisado el Certificado de Antecedentes y requerimientos judiciales de fecha 02 de diciembre de 2024, expedido por la Policía Nacional de Colombia, la ciudadana ANA MILENA MORALES LÓPEZ, identificada con la Cedula de Ciudadanía No. 52.705.962, representante legal de UT RC SOC SSF 2024, Sociedad Comercial con domicilio principal en la Ciudad de Bogotá, no tiene asuntos pendientes en el Registro Nacional de Medidas Correctivas.

12. Que, según certificación del 30 de octubre de 2024, Expedida por la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y Telecomunicaciones -MINTIC, El Registro de Deudores Alimentarios Morosos – REDAM, correspondiente a ANA MILENA MORALES LÓPEZ, identificada con la Cedula de Ciudadanía No. 52.705.962, representante legal de UT RC SOC SSF 2024, Sociedad Comercial con domicilio principal en la Ciudad de Bogotá, no se encuentra inscrita en el registro de deudores morosos.

13. Que, realizadas las consideraciones previas, las partes acuerdan suscribir el presente contrato, el cual está contenido en las siguientes:

CLÁUSULAS:

CONTRATO DE PRESTACIÓN DE SERVICIOS No. 429 DE 2024 SUSCRITO ENTRE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR Y UT RC SOC SSF 2024

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

CLÁUSULA SEGUNDA. CARACTERÍSTICAS TÉCNICAS DE LOS PRODUCTOS, BIENES, OBRAS O SERVICIOS: En desarrollo del objeto mencionado, se compromete a cumplir con los servicios descritos en el estudio previo, el pliego de condiciones definitivo, las adendas realizadas, y la oferta presentada por el contratista en el marco de la Selección Abreviada de Subasta Inversa SASI-003 de 2024 SOC adelantada por la Superintendencia del Subsidio Familiar y seleccionada conforme a las reglas establecidas para tal efecto, que se detallan a continuación:

El contratista deberá prestar los servicios de acuerdo con las siguientes especificaciones técnicas:

El servicio SOC corresponde a la estrategia de la Superintendencia por fortalecer su Modelo de Seguridad y Privacidad de la Información MSPI en el sentido de incorporar el monitoreo de seguridad de los incidentes que se puedan presentar de manera proactiva y para la gestión de riesgos, conforme normatividad internacional, buenas prácticas en el sector TI y los lineamientos MinTIC, asegurando así las condiciones para los servicios de TI en la Superintendencia, tales como ISO/IEC 27001, NIST SP 800-61. Así mismo se ha de emplear sistemas de detección automática de amenazas (SIEM), firewalls, herramientas de análisis de vulnerabilidades y sistemas de gestión de incidentes, incluida la integración de diferentes tecnologías para la adopción de metodologías que, en una permanente dinámica, para la correlación de eventos automática de incidentes y con base en buenas prácticas que son de adopción común en la industria de la ciberseguridad.
Para dar cumplimiento al objeto, el contratista deberá tener en cuenta las especificaciones del servicio a adquirir por parte de la Superintendencia establecidas en el ANEXO 9 FICHA TÉCNICA

La infraestructura de la SSF en la actualidad está compuesta por un total 14 servidores físicos y 60 virtuales (Hyper-V), en su mayoría está basada en Microsoft, sin embargo, actualmente se cuentan con algunos servidores de sistema operativo Linux, las bases de datos de los sistemas de información son en su mayoría Microsoft SQL Server, una base de datos MYSQL y una base de datos Postgresql. Su infraestructura se encuentra tanto en Azure como en On Premise.

CONTRATO DE PRESTACIÓN DE SERVICIOS No. 429 DE 2024 SUSCRITO ENTRE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR Y UT RC SOC SSF 2024

Servidores	Sistemas Operativos de los servidores: Windows Server 2012 R2 y/o superiores, Virtualización por Hyper-V, Linux Centos 7,0 y/o superiores, Linux Ubuntu 22 y/o superiores.
Sistemas Operativos de Estaciones de trabajo	Sistemas Operativos de los servidores: Windows Server 2012 R2 y/o superiores, Virtualización por Hyper-V, Linux Centos 7,0 y/o superiores, Linux Ubuntu 22 y/o superiores.
Bases de datos	Microsoft SQL Server 2016 y/o superiores, MySQL 11, Postgresql.
Switches	12 switches Border, 1 Switch Core
Firewall y equipos de seguridad	Firewall Nex-generation Palo Alto 3220, WAF 400E, Antivirus ESET.
Correo electrónico institucional	Microsoft Office 365 E1 y E3 Exchange Online P1
Aplicaciones	14 sistemas de información de acuerdo con el catálogo de servicios de la entidad

Tabla general Plataforma Tecnológica

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)

CONTRATO DE PRESTACIÓN DE SERVICIOS No. 429 DE 2024 SUSCRITO ENTRE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR Y UT RC SOC SSF 2024

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

I.2. Requisitos Generales del servicio

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

I.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.

I. 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.
- **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.

I.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 recoleccion delogs	35%	Promedio de tiempo disponible de los dispositivos de recolección de logs	Herramienta de Gestion 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 Gestion del proveedor	99,70%	100	99,7	0%
					99,6	91	10%
					90	81	20%

CONTRATO DE PRESTACIÓN DE SERVICIOS No. 429 DE 2024 SUSCRITO ENTRE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR Y UT RC SOC SSF 2024

		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%

OBLIGACIONES GENERALES DEL CONTRATISTA:

1. Cumplir con el objeto del contrato y las obligaciones conexas al mismo de acuerdo con lo establecido en el Estudio previo, pliego de condiciones, ficha técnica y la propuesta presentada.
2. Constituir dentro los tres (3) días hábiles siguientes a la firma de contrato la garantía exigida en favor de la Superintendencia del Subsidio Familiar en los términos establecidos en el contrato y mantenerla vigente durante el término de ejecución de este.
3. Presentar los informes y productos en la periodicidad y formalidades exigidas, de conformidad con lo establecido en el contrato.
4. Dar cumplimiento a las obligaciones con los sistemas de seguridad social en salud, pensiones, riesgos laborales y aportes parafiscales, cuando haya lugar a ello y presentar los documentos respectivos que así lo acrediten, conforme a lo establecido en el artículo 50 de la Ley 789 de 2002, en la Ley 828 de 2003, la Ley 1562 de 2012, el Decreto 1072 de 2015 (Único Reglamentario del Sector Trabajo), el Decreto 780 de 2016 (Único Reglamentario del Sector Salud y Protección Social) y demás normas que regulen la materia.
5. Expedir o acreditar los pagos establecidos del sistema de seguridad social en salud, pensiones, riesgos laborales y aportes parafiscales, a través de certificación expedida por el revisor fiscal, si está obligado a tenerlo, o por el representante legal o el contador público, en caso de no tener dicha obligación de conformidad con la normativa vigente

6. Reportar al supervisor, de manera inmediata, cualquier novedad o anomalía que pueda afectar la ejecución del contrato.
7. Guardar total reserva de la información que por razón de sus obligaciones y desarrollo de sus actividades obtenga. Esta es de propiedad de la Superintendencia y solo salvo expreso requerimiento de autoridad competente podrá ser divulgada.
8. Acatar las instrucciones que durante el desarrollo del contrato le imparta la Superintendencia, a través del supervisor del contrato.
9. Desarrollar las actividades, productos y materiales del contrato, bajo los principios, lineamientos y directrices trazadas en el Sistema de Gestión de Calidad y en el Modelo Estándar de Control Interno de la Superintendencia.
10. Responder ante las autoridades competentes por los actos u omisiones que ejecute en desarrollo del contrato, cuando con ellos se cause perjuicio a la administración o a terceros, en los términos del artículo 52 de la Ley 80 de 1993.
11. Responder por la documentación e información que por razón del servicio conserve bajo su cuidado o a la cual tenga acceso sin que pueda reproducirla, divulgarla o publicarla por cualquier medio.
12. Suscribir oportunamente el acta de inicio conjuntamente con el/la supervisor (a) del mismo.
13. Obrar con lealtad y buena fe en el desarrollo del contrato, evitando dilaciones o acceder a peticiones o amenazas de quienes actúen por fuera de la ley con el fin de obligarlos a hacer u omitir algún acto o hecho, debiendo informar inmediatamente al supervisor del contrato y a la Superintendencia.
14. Mantener informada a la Superintendencia sobre las modificaciones de su dirección de domicilio físico y electrónico para comunicación y notificaciones.
15. Atender los requerimientos, instrucciones y recomendaciones que durante el desarrollo del contrato le imparta la Superintendencia a través del supervisor de este, para una correcta ejecución y cumplimiento de sus obligaciones.
16. Disponer de una línea telefónica fija, una línea celular y un correo electrónico para

comunicación con la Superintendencia por el plazo de ejecución del contrato.
17. Dar cumplimiento a las normas del sistema de gestión integral de la Entidad, tanto en calidad, seguridad y salud en el trabajo, gestión ambiental y seguridad de la información, así como todo lo relacionado con el Modelo Integrado de Planeación y Gestión (MIPG).
18. Evitar los elementos de discriminación sexista del uso del lenguaje escrito, visual y audiovisual, y de la imagen, que perpetúen estereotipos de género y/o generen un ambiente sexual hostil. Para lo cual, deberá abstenerse de hacer, compartir, difundir y promover bromas, chistes y expresiones machistas, así como, hacer uso del Lenguaje incluyente, entendido este como el uso de expresiones lingüísticas que incluyan tanto al género femenino como al masculino, cuando se requiera hacer referencia a ambos y no el uso exclusivo del género masculino.
19. Presentar el informe correspondiente con las observaciones evidenciadas en las visitas y sus respectivos soportes.
20. Asistir a las capacitaciones y/o eventos que sean requeridos por el Supervisor del contrato.
21. Publicar en el expediente contractual digital de la plataforma SECOP II, las cuentas de cobro con sus debidos soportes.
22. Las demás directamente relacionadas con el objeto contractual.

2.5 OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA: Las obligaciones específicas del contrato que resulte serán las siguientes:

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.
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.
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.
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.
5. Utilizar una metodología de gestión de proyectos de amplio uso en el mercado para el control del mismo y aplicar las mejores prácticas de administración como es ITIL V3 o superior, NIST, FIRST.6.
6. Adelantar las actividades de integración de las herramientas tecnológicas definidas, en el caso que aplique.
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, 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:

- 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.

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.
9. Informar a la SSF sobre las amenazas identificadas y que puedan generar la interrupción del servicio contratado.
10. Identificar e implementar las estrategias de recuperación apropiadas para restablecer el servicio contratado dentro de las franjas de tiempo pactadas.
11. Establecer, conjuntamente 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.
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.
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.
14. Desarrollar capacidades predictivas para anticipar posibles amenazas cibernéticas y actuar de manera proactiva en su prevención.
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.
16. El contratista deberá Establecer y promover la adopción de estándares y buenas prácticas en seguridad digital, en línea con el marco normativo existente.
17. El contratista deberá Implementar un enfoque integral de gestión de riesgos e incidentes de seguridad digital, determinando roles y responsabilidades en la entidad.
18. 1El 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.

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.

20. Todos los documentos o información que se produzcan en desarrollo del contrato, serán de uso exclusivo de la Superintendencia del Subsidio Familiar y 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.

CLÁUSULA QUINTA. OBLIGACIONES DE LA SUPERINTENDENCIA:

1. Suministrar la información y documentos necesarios que requiera **EL CONTRATISTA** para el cabal cumplimiento del objeto del contrato.
2. Realizar los pagos correspondientes previa certificación de cumplimiento suscrita por el supervisor del contrato en las condiciones pactadas.
3. Ejercer la supervisión del contrato para verificar el cumplimiento de las obligaciones del contratista.

CLÁUSULA SEXTA. VALOR DEL CONTRATO: El valor del presente contrato es hasta por la suma de **QUINIENTOS SETENTA Y CUATRO MILLONES QUINIENTOS TREINTA MIL PESOS ($574.530.000)** incluido IVA, y todos los costos directos e indirectos, los impuestos, tasas y contribuciones a que haya lugar que conlleve la celebración y ejecución total del contrato.

A continuación, se detallan los valores estimados para la ejecución del proceso:

Ítem	Descripción Necesidad	Valor ofertado incluido IVA
1	Servicio SOC	$278.650.000
2	Servicio de gestión de vulnerabilidades	$154.485.374
3	Servicio de ethical hacking	$141.394.626
TOTAL PROPUESTA ECONÓMICA		$574.530.000

CONTRATO DE PRESTACIÓN DE SERVICIOS No. 429 DE 2024 SUSCRITO ENTRE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR Y UT RC SOC SSF 2024

CLÁUSULA SÉPTIMA. FORMA DE PAGO: La Superintendencia pagará al CONTRATISTA así:

Se efectuará un solo pago sea una vez sea recibido a satisfacción por parte de la Superintendencia la Configuración certifidel SOC e integración de las herramientas y equipos de seguridad informática, la Presentación y aprobación del Plan de Gestión de Seguridad del SOC, y del primer conjunto de informes establecidos en el procedimiento integral para la gestión de incidentes de seguridad y evaluación de vulnerabilidades, incluyendo técnicas de Ethical Hacking, y Plan de Gestión de Seguridad. Así como el estudió de Ethical Haking.

NOTA: Para efectos del trámite de pago se recepcionarán las facturas y demás documentos antes del 20 de diciembre de 2024. Conforme a este requisito, el Supervisor debe coordinar con el proveedor el cumplimiento de las formalidades para el pago.

Todo pago está sujeto a la disponibilidad del programa anual mensualizado de caja-PAC que tenga aprobada la Superintendencia del Subsidio Familiar y a los procesos de revisión y trámite en el Grupo de Gestión Financiera.

(*) PARÁGRAFO: De conformidad con el artículo 1.1, directiva presidencial 09 de 2020, el contratista de la entidad que esté obligado a facturar electrónicamente deberá presentar factura electrónica (PDF representación gráfica y XML de la factura), previamente validada por la DIAN como requisito para el pago de los servicios contratados y de acuerdo con las especificaciones que determine el Grupo de Gestión Financiera. De lo contrario y atendiendo a la condición tributaria del contratista podrá aportar cuenta de cobro o documento equivalente.
En caso de ser obligado a facturar electrónicamente deberá inscribir esta responsabilidad en el Registro Único Tributario -RUT, y generar la factura electrónica bajo las condiciones y especificaciones dadas por el Grupo de Financiero para el pago.

Nota 1: Si la factura o documento de cobro no ha sido correctamente elaborada y no es posible su corrección por parte del proveedor o no se acompañan los documentos requeridos, el término para el pago solo se contará a partir de la fecha en que se presenten debidamente corregidas o desde aquella en que se haya aportado el último de los documentos. Las demoras que se presenten por estos conceptos será responsabilidad del contratista o proveedor y no tendrá derecho a ello a pago de intereses o compensación de ninguna naturaleza.

Nota 2: Si, llegará a quedar recursos disponibles de alguna actividad establecida en las especificaciones técnicas, por alguna causal externa y ajena a la voluntad de las partes, estos recursos podrán ser utilizados para la ejecución de otra actividad que los necesite y que previamente se encuentre contemplada en las especificaciones técnicas, con el fin de coadyuvar a la optimización de recursos por parte de la Entidad y al cumplimiento del objeto contractual.

Requisitos para el pago:

a) **El contratista deberá entregar al supervisor del contrato los siguientes soportes:**
   1. Informe de la Supervisión del contrato, avalando el pago solicitado e informe sobre el estado de ejecución de contrato, según formatos preestablecidos.
   2. Factura o documento equivalente, según corresponda. La factura deberá cumplir los requisitos establecidos en el Estatuto Tributario, y demás normas que lo modifiquen, adicionen o aclaren;
   3. Informe mensual de actividades correspondiente al período que está cobrando, para ser avalado por el supervisor del contrato con los respectivos soportes.
   4. Allegar la certificación del pago de los aportes al Sistema de Seguridad Social Integral en salud, pensión y riesgos laborales, del mes inmediatamente anterior o actual al que se va a pagar, realizados por parte del CONTRATISTA, de conformidad con el artículo 50 de la Ley 789 de 2002. Persona jurídica: certificación expedida por el revisor fiscal, si está obligado a tenerlo, o por el representante legal **o el contador público,** en caso de no estar obligado a tener revisor fiscal.
   5. Formatos y soportes definidos en el procedimiento "CAUSACIÓN DE OBLIGACIONES PARA PAGOS A TERCEROS E **INSTRUCTIVO DE PAGOS** reglamentado por el Grupo de Gestión Financiera de la Superintendencia.

b) **El supervisor del contrato deberá:**

   1. Expedir la certificación de cumplimiento, previa revisión de los documentos indicados en el literal a) anterior y entregar al contratista.
   2. Remitir al Grupo de Gestión Contractual, para que obren en la carpeta del contrato, fotocopia de la certificación de cumplimiento, con los soportes de la prestación del servicio junto con la fotocopia del formato de ingreso de los bienes al almacén (cuando se trate de bienes), y los

documentos suministrados por el contratista, relacionados en el literal a), según aplique para cada pago.

3. Elaborar y tramitar el acta de liquidación del contrato, y adjuntar el certificado de pagos y saldos expedida por el Coordinador del Grupo de Gestión Financiera.

c) Para solicitar el pago, el contratista deberá radicar en el Grupo de Gestión Financiera:

1. Factura electrónica (**representación gráfica y XML) t**ramitada ante la DIAN, si aplica, según instructivo de pagos del grupo de gestión financiera.

2. Fotocopia de la correspondiente Certificado de Cumplimiento para Trámite de Pagos expedida por el supervisor del contrato, junto con el formato de ingreso de los bienes al almacén, cuando se trate de bienes.

Nota 1: La factura deberá cumplir los requisitos establecidos en el Estatuto Tributario y demás normas que lo modifiquen, adicionen o aclaren.

El término para el pago sólo podrá contarse desde el momento en que los documentos que soportan dicho pago estén completos y correctamente elaborados. Las demoras que se presenten en los pagos, por causas imputables al contratista, serán responsabilidad del contratista.

d) Programación del pago en el Plan Anual Mensualizado de Caja PAC

1. El Grupo de Gestión Financiera solicitara el PAC de acuerdo con lo programado por cada dependencia, de acuerdo con el calendario fijado para cada vigencia, por el Ministerio de Hacienda y Crédito Público.
2. **Pago:** El pago se realizará una vez aprobado el PAC por parte del Ministerio de Hacienda y Crédito Público.

Nota 2: El contratista debe subir a la plataforma correspondiente los documentos para su respectivo cobro de conformidad con el artículo 4º la Ley 2010 de 2019 que adiciona el parágrafo 3 y 5 al artículo 437 del Estatuto Tributario, en el que establece: “PARÁGRAFO 3. (…) Para la celebración de contratos de venta de bienes y/o de prestación de servicios gravados por cuantía individual y superior a 3.500 UVT, estas personas deberán inscribirse previamente como responsables del impuesto sobre las ventas (IVA), formalidad que deberá exigirse por el contratista

para la procedencia de costos y deducciones. Lo anterior también será aplicable cuando un mismo contratista celebre varios contratos que superen la suma de 3.500 UVT. (…)". PARÁGRAFO 5. Los límites de que trata el parágrafo 3 de este artículo serán 4.000 UVT para aquellos prestadores de servicios personas naturales que derivan sus ingresos de contratos con el Estado.

Por lo anterior, los contratistas que para el presente año superen el monto establecido o quienes ya estuvieran como responsables del impuesto sobre las ventas (IVA), deberán presentar factura de venta, con los requisitos del artículo 617 del Estatuto Tributario, incluyendo el impuesto al valor agregado (IVA) para cada pago.

CLÁUSULA OCTAVA. IMPUTACIÓN PRESUPUESTAL: El valor del presente contrato se ampara con cargo al certificado de disponibilidad presupuestal No. 31324 del 09 de abril de 2024, expedido por el Grupo de Gestión Financiera.

Número y fecha	Valor
45524 del 30 de julio de 2024	$ 580.000.000

CLÁUSULA NOVENA. PLAZO DEL CONTRATO: El plazo de ejecución del contrato será de 13 meses contados a partir de la suscripción del Acta de Inicio y cumplimiento de los demás requisitos de ejecución. Dicho plazo deberá entenderse de la siguiente manera; Deberán efectuarse todas las tareas de configuración e implementación del sistema Soc , en todos los equipos de la entidad, dicha actividad no podrá superar el 31 de Diciembre de 2024,entiéndase para este efecto todos los equipos tanto on premise, como en la nube enunciados en el anexo técnico, una vez la implementación y configuración sea recibida a satisfacción por parte del supervisor del contrato, se empezaran a contar los (12) meses para la prestación del servicio de monitoreo el cual debe cumplir con todas las especificaciones descritas en el anexo técnico..

CLÁUSULA DÉCIMA. SUPERVISIÓN:

La supervisión y control de la ejecución del contrato estará a cargo de Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones o a quien designe el ordenador del gasto. En virtud de lo señalado por el artículo 83 de la Ley 1474 de 2011 y el Artículo 2.2.1.2.1.2.19 del Decreto 1082 de 2015, se podrá contar con el apoyo a la Supervisión por parte de un profesional o un equipo de profesionales, sin que dicho apoyo implique el

traslado de la responsabilidad del ejercicio de la supervisión, de acuerdo con lo que se describe a continuación:

Cargo	Jefe de Oficina
Dependencia	Oficina de Tecnologías de la Información y las Comunicaciones

Son funciones del supervisor:

1. Velar por la debida ejecución del contrato y si es el caso, exigir al CONTRATISTA la información que considere necesaria.
2. Verificar el adecuado cumplimiento de los plazos.
3. Informar oportunamente y por escrito a la Secretaria General cualquier novedad y/o inconveniente que se presente en la ejecución del contrato.
4. Elaborar y suscribir el acta de liquidación del contrato.
5. Verificar y dejar constancia del cumplimiento del CONTRATISTA con las obligaciones de seguridad social integral y parafiscal, para cada pago que se realice, de conformidad con lo establecido en el artículo 50 de la Ley 789 de 2002, el artículo 23 de la Ley 1150 de 2007 y el Decreto 0862 de 2012.
6. Remitir al Grupo Gestión Contractual todos los documentos que soportan el desarrollo del contrato, como son entre otros: Acta de inicio, informes de ejecución del contrato, certificaciones de cumplimiento, certificaciones de paz y salvo por seguridades sociales integrales y parafiscales, comunicaciones escritas que se dirijan entre el contratista y el supervisor y acta de liquidación del contrato.
7. Las demás que le competan, de acuerdo a la naturaleza del contrato, de conformidad a lo señalado por los artículos 82 a 86 de la Ley 1474 de 2011, y la resolución 0818 de 2021 de la Superintendencia del Subsidio Familiar en el Título III de supervisión e interventoría de los contratos.
8. Todas las solicitudes y órdenes del supervisor en la ejecución del presente contrato deberán constar por escrito y deberán encontrarse debidamente documentado por el supervisor en la carpeta de ejecución contractual.
9. Verificar la terminación del contrato, dentro de ello la revisión del expediente contractual respectivo, sus documentos completos que reflejen de manera inequívoca el desarrollo de este y con base en dicha verificación conminar al contratista para que haga entrega de lo que faltare, si ese fuera el caso.
10. Verificar que se mantengan las condiciones con las que se acredite puntaje adicional o factores de desempate en la evaluación de las ofertas por el termino de ejecución del contrato. (si aplica)
11. Verificar la condición de calidad del servicio o producto entregado.
12. Adjuntar la carpeta contractual, documentos y los soportes del servicio prestado o producto recibido en debida forma

CONTRATO DE PRESTACIÓN DE SERVICIOS No. 429 DE 2024 SUSCRITO ENTRE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR Y UT RC SOC SSF 2024

CLÁUSULA DÉCIMA PRIMERA. GARANTÌA DEL CONTRATO: EL CONTRATISTA debe constituir a favor de la SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR NIT 860.503.600-9 Dirección Carrera 69 No. 25B – 44 pisos 3,4 y 7, las garantías De acuerdo con lo establecido en el artículo 7º de la Ley 1150 de 2007, la Seccion Tercera, Subsección 1 GARANTÍAS del Decreto 1082 de 2015, el contratista deberá amparar los riesgos derivados de la presente contratación, de conformidad con la siguiente tabla:

AMPAROS	PORCENTAJE MÍNIMO Sobre el valor del contrato	VIGENCIA
Cumplimiento	10%	Vigencia del contrato y 6 meses más o hasta liquidación efectiva del contrato.
Calidad del servicio	10%	Plazo del contrato y un (1) año más más.
Salarios y prestaciones sociales	5%	Plazo de ejecución y 3 años más

Nota 1: Cuando se trate de patrimonios autónomos y garantías bancarias estas deberán ser otorgadas de conformidad con la norma vigente.

Nota 2: Se debe mantener actualizadas las vigencias y montos de los amparos de las garantías constituidas con ocasión de la suscripción del Contrato, en el evento de presentarse modificaciones en valor y/o plazo y hasta la liquidación del mismo.

CLÁUSULA DÉCIMA SEGUNDA. CONFIDENCIALIDAD: Todos los documentos e información que se produzcan en desarrollo del contrato, serán de uso exclusivo de la Superintendencia del Subsidio Familiar y **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. . Esta confidencialidad será continua y no vence ni por terminación ni por caducidad del contrato.

CLÁUSULA DÉCIMA TERCERA. INDEMNIDAD: EL CONTRATISTA indemnizará, defenderá y mantendrá indemne a **LA SUPERINTENDENCIA,** a sus empleados y propiedades por cualquier reclamo, acción u omisión derivada del desarrollo y ejecución del presente contrato por **EL CONTRATISTA**, sus directores, personal, agentes, empleados y representantes. **EL CONTRATISTA** será el único

responsable por los daños y perjuicios causados a terceros por acciones u omisiones del CONTRATISTA, sus directores, agentes, personal, empleados y representantes en desarrollo y ejecución del presente contrato.

CLÁUSULA DÉCIMA CUARTA. INTERPRETACIÓN, MODIFICACIÓN Y TERMINACIÓN UNILATERAL Y SOMETIMIENTO A LA LEY NACIONAL DEL CONTRATO: De conformidad con lo dispuesto por los artículos 14 al 18 de la Ley 80 de 1993, en concordación con la Ley 1150 de 2007, sin que exista por ello indemnización por parte de la SUPERINTENDENCIA las cláusulas excepcionales de interpretación, modificación y terminación unilateral, sometimiento a la ley nacional del contrato por parte de la Entidad, se entienden incorporadas en el presente contrato.

CLÁUSULA DÉCIMA QUINTA. DE LA CESIÓN DEL CONTRATO: Salvo autorización expresa de **LA SUPERINTENDENCIA**, **EL CONTRATISTA** no podrá ceder o subcontratar el cumplimiento de sus obligaciones ni total ni parcialmente del presente contrato.

CLÁUSULA DÉCIMA SEXTA. INHABILIDADES E INCOMPATIBILIDADES SOBREVINIENTES: **El CONTRATISTA** manifiesta bajo la gravedad del juramento que no se encuentra incurso en causales de inhabilidad y/o incompatibilidad legal para suscribir el presente contrato. Si llegare a sobrevenir inhabilidad o incompatibilidad, **EL CONTRATISTA** renunciará a su ejecución.

PARÁGRAFO: Presentada la causal de inhabilidad o incompatibilidad sobreviniente, **EL CONTRATISTA** deberá informar por escrito a **LA SUPERINTENDENCIA**, dentro de los tres (3) días hábiles siguientes a su acaecimiento; podrá proponer un candidato para la cesión del mismo, el cesionario deberá reunir las condiciones y calidades por las cuales fue adjudicado el contrato y este manifestará por escrito que se encuentra dispuesto a continuar con la ejecución del contrato en las mismas condiciones pactadas. **LA SUPERINTENDENCIA,** se reserva la facultad de aceptar al candidato propuesto por **EL CONTRATISTA,** o en su defecto, autorizará la cesión a favor de un tercero que reúna las condiciones requeridas para continuar con la ejecución contractual.

CLÁUSULA DÉCIMA SEPTIMA. MULTAS: LA SUPERINTENDENCIA tendrá la facultad de imponer multas, en caso de incumplimiento parcial o total de cualquiera de las obligaciones a cargo del **CONTRATISTA**, de conformidad con el Artículo 17 de la Ley 1150 de 2007 y el Artículo 86 de la Ley 1474 de 2011(Estatuto Anticorrupción). **EL CONTRATISTA** autoriza a **LA SUPERINTENDENCIA** para imponerle multas y, a realizar los descuentos correspondientes de los saldos a favor del **CONTRATISTA**, mediante Acto Administrativo en la cuantía que a continuación se describe, así:

1. Por incumplimiento en los términos de legalización del contrato: si el contratista, no allega en los términos establecidos en el contrato los documentos necesarios para la legalización de este, se causará una multa de cinco (5) salarios mínimos legales mensuales diarios vigentes, por cada día calendario transcurrido a partir de la fecha prevista para el cumplimiento de esta obligación y hasta su completa satisfacción, o se aplicará la cláusula penal en la misma proporción.

2. Por no cumplir con cualquiera de las obligaciones contenidas en el contrato o en los documentos que lo integran, o cumplirlas deficientemente o por fuera del tiempo estipulado, se causará una multa equivalente al uno por mil (1 x 1000) del valor del contrato, por cada día calendario que transcurra desde la fecha prevista para el cumplimiento de dichas obligaciones y hasta cuando estas efectivamente se cumplan, o se aplicará la cláusula penal en la misma proporción.

En todo caso por mora o incumplimiento de las obligaciones por parte del CONTRATISTA y previo requerimiento del supervisor, la Superintendencia podrá imponer y hacer exigibles las multas diarias y sucesivas equivalentes al uno por ciento (1%) del valor de este CONTRATO, las cuales entre sí no podrán exceder del diez por ciento (10%) del valor de este.

El pago o deducción de las multas y/o cláusula penal no exonerará al contratista, del cumplimiento de sus obligaciones emanadas del contrato de contratista. La imposición de la multa o de la cláusula penal atenderá criterios de oportunidad, razonabilidad, proporcionalidad y gravedad de la obligación incumplida.

PARÁGRAFO PRIMERO: La imposición de la multa atenderá criterios de oportunidad, razonabilidad, proporcionalidad y gravedad de la obligación incumplida.

PARÁGRAFO SEGUNDO: El valor máximo de las multas señaladas anteriormente, no podrá superar el diez por ciento (10%) del valor del contrato. El pago o deducción de las multas no exonerará al **CONTRATISTA**, del cumplimiento de sus obligaciones emanadas del presente contrato.

CLAUSULA DÉCIMA OCTAVA. CLÁUSULA PENAL PECUNIARIA: En caso de incumplimiento parcial o total del contrato o el mero retardo en el cumplimiento de las obligaciones contractuales. **EL CONTRATISTA** pagará a **LA SUPERINTENDENCIA**, a título de pena pecuniaria, una suma equivalente hasta el diez por ciento (10 %) del valor total del contrato. La tasación de la cláusula penal atenderá criterios de razonabilidad, proporcionalidad y gravedad del incumplimiento.

La imposición de esta pena pecuniaria se considerará como una estimación anticipada de perjuicios que el **CONTRATISTA** cause a la **SUPERINTENDENCIA**. El valor pagado como cláusula penal no es óbice para demandar, ante el juez del contrato, la indemnización integral de perjuicios causados si estos superan el valor de esta. **EL CONTRATISTA,** autoriza expresamente a la Entidad para hacer el descuento correspondiente de los saldos adeudados por la Entidad.

PARÁGRAFO PRIMERO: El pago o deducción de la cláusula penal no exonerará al **CONTRATISTA** del cumplimiento de sus obligaciones emanadas del presente contrato.

PARÁGRAFO SEGUNDO: En caso de proceder la imposición de la cláusula penal, se aplicará el procedimiento establecido en los artículos 17 de la Ley 1150 de 2007 y 86 de la Ley 1474 de 2011

CLÁUSULA DÉCIMA NOVENA. CADUCIDAD: Mediante acto administrativo debidamente motivado, decretar la caducidad del presente contrato, cuando se presente las causales señaladas en el artículo 90 de la Ley 418 de 1997. La declaratoria de caducidad no impedirá que la **SUPERINTENDENCIA** contrate con persona la continuación de la ejecución del objeto del contrato. La declaratoria de caducidad será constitutiva del siniestro de incumplimiento y no habrá lugar a indemnización alguna para el contratista, quien se hará acreedor de las sanciones e inhabilidades previstas en la Ley.

CLÁUSULA VIGÉSIMA. MECANISMOS DE SOLUCIÓN DE CONFLICTOS: En el evento de que surjan diferencias con ocasión de la ejecución del contrato o de su liquidación, las partes buscarán mecanismos de arreglo directo, tales como la negociación directa, la amigable composición o la conciliación. En tal caso las partes dispondrán de un término de un mes a partir de la fecha en que cualquiera de ellas haga una solicitud en tal sentido. Dicho término podrá ser prorrogado por mutuo acuerdo.

CLÁUSULA VIGÉSIMA PRIMERA. LIQUIDACIÓN: De conformidad con lo dispuesto por los artículos 60 de la Ley 80 de 1993, modificado por el artículo 11 de la Ley 1150 de 2007 y modificado por el artículo 217 del Decreto 019 de 2012, presente contrato se liquidará dentro de los cuatro (4) meses siguientes a la expiración del término previsto para la ejecución del contrato o a la expedición del acto administrativo que ordene la terminación, o a la fecha del acuerdo que la disponga. Si EL CONTRATISTA no se presenta a la liquidación previa notificación o convocatoria que le haga la entidad, o las partes no lleguen a un acuerdo sobre su contenido, la SUPERINTENDENCIA liquidará en forma unilateral dentro de los dos (2) meses siguientes, de conformidad con lo dispuesto en el artículo 141 de la Ley 1437 de 2011. Vencido el plazo anterior sin lograr la liquidación, la misma podrá

ser realizada en cualquier tiempo dentro de los dos años siguientes al vencimiento de los términos antes señalados, de mutuo acuerdo o unilateralmente.

CLÁUSULA VIGÉSIMA SEGUNDA. RESPONSABILIDAD-. EL CONTRATISTA responde civil y penalmente tanto por el incumplimiento de las obligaciones derivadas del contrato como por los hechos u omisiones que se le fueren imputadas y que causen daño o perjuicio a la SUPERINTENDENCIA todo de conformidad con lo dispuesto por los artículos 52, 53 y 56 de la Ley 80 de 1993, y demás normas aplicables.

CLÁUSULA VIGÉSIMA TERCERA. DOCUMENTOS: Hacen parte integrante del presente contrato los siguientes documentos: a) Los estudios previos y demás documentos del proceso de selección, el pliego de condiciones, las observaciones y respuestas a las mismas, adendas y la propuesta presentada por **EL CONTRATISTA y sus anexos**. b) Los documentos, actas, acuerdos, comunicaciones y demás actos que se produzcan en desarrollo del objeto del contrato.

CLÁUSULA VIGÉSIMA CUARTA: PERFECCIONAMIENTO Y EJECUCIÓN. El presente contrato se entiende perfeccionado con la firma de las partes y para su ejecución requiere la aprobación de la garantía única del contrato.

CLAUSULA VIGÉSIMA QUINTA. LUGAR DE EJECUCIÓN: El lugar de domicilio del contrato será la ciudad de Bogotá D.C., el lugar de ejecución del contrato será en la sede de la Superintendencia del Subsidio Familiar ubicada en la carrera 69 No. 25 B-44 en la ciudad de Bogotá D.C.

Para constancia se firma en Bogotá D.C.

(firmado Electrónico a través del SECOP II)
KATERIN GÓMEZ OLAYA
SECRETARIA GENERAL
SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR

(firmado Electrónico a través del SECOP II)
ANA MILENA MORALES LÓPEZ BELTRAN
CC. 52.705.962
UT RC SOC SSF 2024

Proyectó: Andrés Barrios Suárez – Abogado -Grupo de Gestión Contractual.

Aprobó: Sandra Patricia Gaitán Fajardo – Abogada – Grupo de Gestión Contractual.