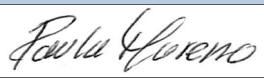
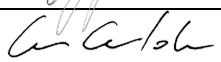
Supersubsidio	ACTA DE REUNION	RealTime C&S SAS

FECHA	02/04/2025	HORA INICIO	9.00 am	DURACIÓN (HORAS)	2	ACTA No.	XX
ASUNTO	Realizar reunión seguimiento del Proyecto						
CONTRATO /PROYECTO	Numero de Contrato SSF SASI 429 DE 2024 – UT RC SOC						
ÁREA RESPONSABLE	OTIC	Clasificación de la información del documento (No marque opción para información pública)	☐Uso Interno. X Clasificada. ☐Reservada.				

ASISTENTES Y FIRMANTES			
Nombre	**Área / Entidad**	**Cargo/Tipo de vinculación**	**Firma**
Paula Andrea Moreno	OTIC SSF	Profesional	
David Quintero	OTIC SSF	Profesional	
Juan Jose Olivella	OTIC SSF	Profesional	
Cesar Dario Cordoba	RealTime	Gerente de Proyecto	
Leandro Calderón	RealTime	Líder SOC	NO FIRMA
Eduard Méndez	RealTime	Consultor Senior de Despliegue	NO FIRMA
David Silva	RealTime	Profesional de Apoyo Implementación	NO FIRMA

TEMAS	
1	Avances del periodo
2	Tareas a realizar próximo periodo
3	Compromisos

DESARROLLO

AVANCE DEL PERIODO:

1. Se presenta de acuerdo con la solicitud verificación de cumplimiento de los numerales 1.4 y 1.5 de del anexo técnico

÷

Supersubsidio	ACTA DE REUNION	REALTIME C&S SAS

DESARROLLO

Numeral	Obligación	Proceso de Seguridad	Herramientas a utilizar para cumplimiento	Explicación de cumplimiento.
1.4.	Especificaciones Técnicas Generales del Servicio de Gestión de Vulnerabilidades.			
a	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 de Incidentes	FortiSIEM	El SIEM vigila constantemente la ingesta e información a través de los protocolos Syslog, SNMP y Ping, para la detección de un evento anómalo.
b	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 de Vulnerabilidades	Vicarius para análisis interno y Burpsuite para análisis externo.	Para Vicarius se requiere instalar un agente sobre los equipos en los cuales se realizará las evaluaciones de vulnerabilidades. Para BurpSuite para portales Web (ips y dominios).
c	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 Incidentes	FortiSIEM y GLPI	FortiSIEM genera el informe y se envía a los interesados vía correo. GLPI para gestionar las solicitudes de casos.
d	Gestión de alertas: Deberá gestionar los diferentes eventos, alertas o incidentes de seguridad informática y ciberseguridad.	Gestión SOC	FortiSIEM	El SIEM vigila constantemente la ingesta e información a través de los protocolos Syslog, SNMP y Ping, para la detección de un evento anómalo.
e	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.	Gestión de Vulnerabilidades	FortiSIEM; Vicarius para análisis interno y Burpsuite para análisis externo.	Se entregaron dos usuarios de FortiSIEM, y se entregarán 2 Usuarios de Vicarius y 2 usuarios de BurpSuite para equipos y dominios de SSF.
f	Tipo de amenazas a analizar: se enlistan a continuación sin embargo se aclara que no se deben limitar a las mencionadas:			

÷

DESARROLLO

	o Malware y Ransomware. o Phishing. o Ataques DDoS. o Violencia de datos. o Vulnerabilidades y parches: Seguimiento de sistemas que no están actualizados y que pueden ser objetivos fáciles para atacantes o 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.	Gestión de Vulnerabilidades	FortiSIEM mitre att&ck Vicarius BurpSuite	Para Malware, Rasonware, Phising, Ataque DDoS, se detecta y analiza desde el FortiSIEM. Vulnerabilidades y Parches con Vicarius y BurpSuite Para tendencias en amenazas emergente se detecta y analiza con mitre att&ck, modulo propio del FortiSIEM.
g	Las herramientas dispuestas para realizar el análisis podrán ser establecidas por el contratista según considere.	NA	NA	NA
h	El análisis deberá permitir realizar comparativos mensuales que permitan identificar patrones en el tiempo.	Gestión Vulnerabilidades	Vicarius BurpSuite	Identificación de vulnerabilidades mensuales y su respectiva comparación con el periodo anterior.

1.5.	Especificaciones Técnicas Generales del Servicio de Ethical Hack			
a	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.	Herramientas para la realización de EH. Prueba phishing	BurpSuite KaliLInux Nmap Metaexploit WireShark	Se realizará un primer ejercicio en abril 2025 y el retest en noviembre 2025.
b	Las pruebas de Ethical Hacking se deberá realiza mediante las siguientes características técnicas:			
b.1	Prueba de penetración externa: Evaluación de seguridad desde fuera del entorno de la empresa sin tener conocimiento previo de los sistemas.			

÷

DESARROLLO

	* Movimientos Laterales * Escalamiento de privilegios * SQL Injection * Cross Site Scripting * Ataques de directorio transversal * Ataques por referencia directa a objetos * Ingeniería social*- Informe del Ethical hacking * Plan de remediación y apoyo a la remediación.	Herramientas para la realización de EH. Prueba phishing	BurpSuite KaliLInux Nmap Metaexploit WireShark	Se realizará pruebas de una conexión de internet
b.2	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.			
	* Movimientos Laterales * Escalamiento de privilegios * SQL Injection * Cross Site Scripting * Ataques de directorio transversal * Ataques por referencia directa a objetos * Ingeniería social*- Informe del Ethical hacking * Plan de remediación y apoyo a la remediación.	Herramientas para la realización de EH. Prueba Tailgating.	BurpSuite KaliLInux Nmap Metaexploit WireShark	Se realizará pruebas desde un punto interno.

2. En la tarde se enviará la agenda para las transferencias de conocimiento de este jueves y viernes.

3. RT queda atenta a la definición y entrega de información para parametrización del monitoreo en las plataformas de la SSF. Cuando se requiera se realizará reunión con los administradores de los diferentes sistemas de información.

TAREAS DEL PRÓXIMO PERIODO

EN IMPLEMENTACION

- ✓ Transferencia de capacitaciones el 03 y 04 de abril.
- ✓ Sesiones de trabajo para validación de casos de uso
- ✓ Programación para escaneo de vulnerabilidades externas.

÷

Supersubsidio	ACTA DE REUNION	REALTIME C&S SAS

DESARROLLO
✓ Preparación de pruebas Ingeniería social y EH ✓ Explicación y funcionamiento agentes vicarius EN OPERACIÓN ✓ Entrega de informe trimestral acumulado (primer trimestre)

COMPROMISOS PACTADOS		
Descripción	Responsable	Fecha de Entrega
Agenda para la transferencia de conocimiento de este jueves y viernes (3 y 4 de abril)	RT	02/04/2025
Entrega de información para monitoreo SOC	SSF	09/04/2025

÷