Supersubsidio	ACTA DE REUNION	RealTime C&S SAS

FECHA	01/10/2025	HORA INICIO	9.00 am	DURACIÓN (HORAS)	1	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**
Juan Jose Olivella	OTIC SSF	Profesional	
David Quintero	OTIC SSF	Profesional	
Paula Andrea Moreno	OTIC SSF	Profesional	
Cesar Dario Cordoba	RealTime	Gerente de Proyecto	
Leandro Calderón	RealTime	Líder SOC	NO FIRMA
Giovanny Caicedo	RealTime	Consultor	NO FIRMA

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

DESARROLLO

AVANCE DEL PERIODO:

- Avance en escaneos de vulnerabilidades: De acuerdo con la aprobación de la semana pasada, se inició el escaneo de vulnerabilidades externas a los 5 portales de la SSF, avance 30%.

- Continua pendiente la entrega de la lista de asistencia y la encuesta de satisfacción de la capacitación en tendencias de seguridad No. 1, datos necesarios para realizar la rifa de premiación. SSF informó que la solicitud fue escalada al equipo de Uso y Apropiación, pero a la fecha no hay novedades.

- RT informa que la segunda Capacitación en tendencias de seguridad se enfocará en atender los hallazgos de la prueba de Ingeniería Social, según lo acordado. La propuesta, incluye la información solicitada por el equipo de Uso y Apropiación, se enviará a más tardar mañana.

DESARROLLO

- Actas de seguimiento: SSF informó que las actas firmadas quedaron en la carpeta de “Aprobadas”. Se continua la revisión y firma por ambos equipos.

- RT presenta el siguiente Plan de EH interno, el cual se enviará por correo para lectura y solicitud de ajustes:

PLAN DE TRABAJO EH INTERNO

1. Objetivos y Alcance
Objetivos: Identificar y reportar las vulnerabilidades que se pueden explotar y que causarían por ejemplo filtración de datos, entre otros

2. Alcance:
Dado que la prueba es de caja negra y simulando un visitando, dependiendo del punto físico que se asigne SSF para realizar el escaneo, se lograrán alcanzar servidores y equipos de red, que no estén protegidos o con deficiencias, por esquema de seguridad perimetral de la entidad. Para los que se logren alcanzar se hará las siguientes pruebas:
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
h. Informe del Ethical hacking
i. Plan de remediación y apoyo a la remediación.

3. Metodología
La prueba se realizará sin conocimiento previo de la arquitectura de la red, credenciales de acceso, IPs internas, o cualquier otra información confidencial, caja negra. Se especifica que el equipo de hackers éticos actuara como un visitante o empleado descontento, comenzando con acceso mínimo a la red. Requerimiento asignación de un punto de red al equipo de RT.

4. Fases de la Evaluación

Reconocimiento (Interno): El equipo intenta descubrir información sobre la red, como direcciones IP, subredes, servicios activos y dispositivos conectados, utilizando herramientas de escaneo y técnicas pasivas. Esta etapa se realizará el 07 de octubre hasta el 10 de octubre.

Análisis de Vulnerabilidades: Se buscan fallos en los sistemas y configuraciones que se hayan descubierto en la fase de reconocimiento. Esto se realizará del 13 al 16 de octubre. Estos resultados se presentan a SSF para acordar cuales están autorizados el intento de explotación.

Explotación: Una vez identificadas las vulnerabilidades, se intenta explotarlas para obtener acceso, elevar privilegios o moverse a otros sistemas de interés. Del 21 al 23 de octubre

÷

Supersubsidio	ACTA DE REUNION	REALTIME C&S SAS

DESARROLLO
Post-Explotación: Se determina el impacto de la explotación y se evalúa qué tan lejos se puede llegar dentro de la red (persistencia, movimiento lateral, etc.). Se presenta que se pudo explotar finalmente de acuerdo con lo autorizado. 24 de octubre Generación de Reporte: Se documentan los hallazgos y se preparan las recomendaciones. 31 de octubre. Entrega y presentación del Informe.

COMPROMISOS PACTADOS		
Descripción	Responsable	Fecha de Entrega
Entrega de lista de asistencia y retroalimentación de la primera capacitación	David Quintero	08/10/2025
Entrega de temario para segunda capacitación	Leandro Calderón	06/10/2025
Envío plan de EH interno	Leandro Calderón	02/10/2025

÷