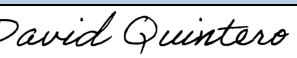
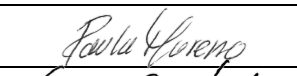
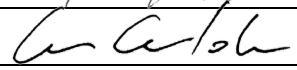
Supersubsidio	ACTA DE REUNION	REALTIME C&S SAS

FECHA	23/07/2025	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**
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:

Cronograma:

1) RT solicita que se revise en la sesión el cronograma enviado por correo el 22 de julio, y se hace la revisión de las actividades que no están al 100%. RT manifiesta que, para la integración y afinamiento es necesario plantear las actividades para completar las mismas, integrar otros equipos y acotar los casos de uso.

	(ETAPA - I) INICIO: INTEGRACIÓN Y AFINAMIENTO		Comienzo	Fin	Recursos	% Avance	% Avance
	IMPLEMENTACIÓN		19/02/2025	28/02/2025		91,4	100,0
3	Ampliación alcance servidores windows	5	19/02/2025	26/02/2025	SSF - RT	70,0	100
4	Integración plataformas linux	7	19/02/2025	28/02/2025	SSF - RT	70,0	100

RT solicita a SSF verificar si se van a incluir otros equipos en el SIEM, de lo contrario llevar la actividad al 100%. Se espera las indicaciones de RT para terminar la tarea.

÷

DESARROLLO

El Ing. David Quintero menciona que en la actividad programada para las 11 am de este mismo día, se terminan integración y casos de uso de la plataforma Linux con lo que hacía falta, que es ambiente productivo y el portal corporativo

El Ing. Cesar Cordoba menciona que después de la reunión la actividad No 4 se podría pasar al 100%. De otro lado, revisando las actividades del cronograma, el tema de transferencia de conocimiento no hay pendientes y se encuentra la 100%, sin embargo, aún no se ha podido lograr hacer las capacitaciones en tendencias de seguridad, y que a la fecha ya se debería haber abordado dos, una que estaba para ejecutarse en abril y la otra en mayo, y a la fecha no hay ninguna aprobada. Se presentaron dos opciones, (Primero una capacitación de la herramienta Vicarius y otra El Mundo Bajo Cyberataque - Desafío de la ciberseguridad en organizaciones, ponente Gottfried Blanco) pero no se ha contestado por correo si alguna ha sido aprobada y seguimos atentos a la respuesta. Si se aprueban, una se realizará en agosto y la otra a principios de octubre.

III	(ETAPA - III) EJECUCIÓN DE ACTIVIDADES - OPERACIÓN		Comienzo	Fin	Recursos	% Avance	% Avance
	TRANSFERENCIA DE CONOCIMIENTO		**20/03/2025**	**28/03/2025**		**100,0**	**100,0**
9	Arquitectura SOC	2 horas	20/03/2025	20/03/2025	RT	100,0	100,0
10	Instalación y Configuración de Agentes Mecanismos de envío de logs desde los dispositivos	2 horas	21/03/2025	21/03/2025	RT	100,0	100
11	Entendimiento de la Plataforma de gestión SOC	2 horas	27/03/2025	27/03/2025	RT	100,0	100
12	Procedimientos de Gestión de Incidentes. Revisión y análisis de los Informes Mensuales	2 horas	28/03/2025	28/03/2025	RT	100,0	100
IV	(ETAPA - IV) EJECUCIÓN DE ACTIVIDADES - OPERACIÓN		Comienzo	Fin	Recursos	% Avance	% Avance
	CAPACITACIONES		**21/04/2025**	**15/12/2025**		**0,0**	**50,0**
13	Jornada 1 de capacitación: Tendencias Recientes o tema por acordar	1 horas	21/04/2025	21/04/2025	RT	0,0	100,0
14	Jornada 2 de capacitación: Tendencias Recientes o tema por acordar	1 horas	21/07/2025	21/07/2025	RT	0,0	100,0
15	Jornada 3 de capacitación: Tendencias Recientes o tema por acordar	1 horas	27/10/2025	27/10/2025	RT	0,0	0,0
16	Jornada 4 de capacitación: Tendencias Recientes o tema por acordar	1 horas	15/12/2025	15/12/2025	RT	0,0	0,0

El Ing. David menciona que RT puede realizar otra propuesta de capacitaciones, por ejemplo, de fabricantes en otros equipos de seguridad o sobre temas de seguridad de la información. Sin embargo, para poderlas aprobar se debe presentar el temario, la presentación y el perfil del ponente, para enviar al equipo de uso y apropiación. El Ing. David manifiesta que se va a revisar la opción de la herramienta Vicarius.

El Ing. Cesar Cordoba menciona que en cuanto a las actividades de escaneos de vulnerabilidades ya se entregaron dos informes de escaneos internos y uno externo, y que ya se lanzó un nuevo escaneo de vulnerabilidades externo del cual ya se hizo entrega parcial, se envío por correo el informe de cuatro dominios y queda pendiente el del portal principal.

El Ing. David Quintero solicita que en el cronograma se incluya la fecha real de ejecución y se dejen los informes en el repositorio organizadas por carpetas de acuerdo al cronograma.

Supersubsidio	ACTA DE REUNION	REALTIME C&S SAS

DESARROLLO

V	(ETAPA - V) EJECUCIÓN DE ACTIVIDADES - OPERACIÓN		Comienzo	Fin	Recursos	% Avance	% Avance
	GESTION DE VULNERABILIDADES		3/03/2025	15/12/2025		52,5	62,5
17	Definición de Objetivos pruebas de vulnerabilidad	1	3/03/2025	3/03/2025	SSF	100,0	100,0
18	Escaneos y Analisis de Vulnerabilidades Marzo	5	17/03/2025	22/03/2025	RT	100,0	100,0
19	Entrega de Informe	1	28/03/2025	28/03/2025	RT	100,0	100,0
20	Escaneos y Analisis de Vulnerabilidades Junio	5	16/06/2025	21/06/2025	RT	60,0	100,0
21	Entrega de Informe	1	30/06/2025	30/06/2025	RT	60,0	100,0

El Ing. Cesar Cordoba indica que, en cuanto a la prueba de Ingeniería Social Externa (prueba phishing) ya fue ejecutada, se entregó el informe, se realizó presentación de resultados y fue aprobado por la SSF. La prueba fue ejecutada y presentada por el Ing. Jairo Garcia. Esta pendiente la ejecución de la prueba de Ingeniería Social Interna, el cual se está revisando internamente para hacer la propuesta. El Ing. Leandro Calderón menciona que realizó dos propuestas de distracción de la prueba, una con una actividad de SST y la otra una capacitación de Seguridad Informática en el auditorio. En la reunión se discuten los pro y contras de cada propuesta, finalmente se concluye que RT revisará los costos de alquiler del auditorio y los otros temas revisados, y sino es viable se hará la propuesta inicialmente planteada con una actividad de SSF. Leandro insiste que se debe aprobar de una vez para poder agendar con el externo que realiza la actividad de SST

El Ing. Leandro Calderón menciona que en cuanto a las redes wifi se buscaba detectar redes abiertas o cifrados débiles para minimizar el riesgo cuando se comparte la wifi con celulares; esta inspección esta alineada a encontrar vulnerabilidades que dejan los funcionarios.

La Ing. Paula Andrea Moreno menciona que ve más viable la primera propuesta, porque con la segunda, el personal de RT en el recorrido por los pisos debería ir acompañado de personal de la entidad, entonces se complica el ejercicio; mientras que con la primera opción va recorriendo los pisos con el personal de SST y quedan libres para recorrer todas las instalaciones por que previamente se autorizó el acceso.

RT enviará propuesta de dos nuevas fechas de agosto para ejecutar la primera propuesta es decir con la fachada de actividades SSF.

El Ing. Cesar Cordoba informa que, de acuerdo a la programación el día de hoy se lanza la prueba de Ethical Hacking Externo, en donde se realizarán las pruebas de movimientos laterales, escalamiento de privilegios, SQL injection, cross site scripting, ataques de directorio transversal y ataques de referencia directa a objetos. De acuerdo a lo conversado con el Ing. Juan Jose y al requerimiento contractual es una prueba de caja negra, pero es de forma controlada, es decir esta notificada la SSF y el SOC. Se espera que el informe esta para la próxima semana.

El Ing. Cesar Cordoba menciona que para la prueba de Ethical Hacking interna se requiere un punto de acceso interno, para realizar la prueba como si fuera un visitante, en ese punto se sentará una persona para lanzar la prueba o instalar una máquina en la red de SSF para realizar el ataque desde allí.

El Ing. Leandro Calderón menciona que otra opción es instalar un a máquina con Burp Suite en la red de SSF para que remotamente se pueda acceder y desde allí lanzar la prueba sin necesidad de llevar un equipo. El Ing. David Quintero responde que al respecto RT pase la propuesta que da cumplimiento al contrato y que SSF revisa y toma la decisión.

Supersubsidio	ACTA DE REUNION	REALTIME C&S SAS

DESARROLLO
En cuanto a la revisión del cronograma, el Ing. Cesar Cordoba menciona que RT se encuentra al día con el envío de los informes mensuales SOC y que todos han sido aceptados por SSF.

COMPROMISOS PACTADOS		
Descripción	Responsable	Fecha de Entrega
Informar el inicio de la prueba de EH Externo	Leandro Calderón	23/07/2025
Finalizar el segundo escaneo de vulnerabilidades interno	Leandro Calderón	30/07/2025
Entrega del informe de escaneo de vulnerabilidad externo del portal principal	Leandro Calderón	30/07/2025
Cerrar la configuración de la plataforma Linux en la sesión de las 11 am	David Quintero/Eduard Mendez	23/07/2025

÷