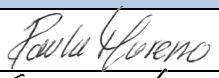
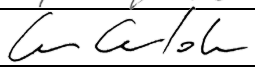
Supersubsidio	ACTA DE REUNION	RealTime C&S SAS

FECHA	21/05/2025	**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	
Cesar Dario Cordoba	RealTime	Gerente de Proyecto	
Leandro Calderón	RealTime	Líder SOC	NO FIRMA
Eduard Méndez	RealTime	Consultor Senior de Despliegue	NO FIRMA

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

DESARROLLO

AVANCE DEL PERIODO:

1. Charlas de Transferencia de Conocimiento y Charlas de Tendencias de Seguridad:

- El caso de uso Vicarius. A solicitud de SSF no se realizó la sesión el 15 de mayo. Pendiente acordar nueva fecha, RT propone que la sesión sea el 28 o 29 de mayo. Sin embargo, RT menciona que es conveniente solucionar previamente la desconexión de activos que se observa en la consola, para lo cual se requiere recoger los logs y validar si es un problema con el endpoint o de conectividad, entre otros, para esto se puede agendar un espacio de trabajo.

  Vicarius en la carta de respuesta a solicitud de RT informa el origen del problema de licenciamiento, mencionando que “En un proceso interno de la compañía, se inactivaron algunos tenant por su no acceso al mismo, por un error humano se realizó la desactivación del acceso de la consola de Supersubsidio la cual estaba en producción, al momento de hacer el reporte trabajamos al interno de forma inmediata y se reactivó el acceso a la plataforma y el servicio”.

- RT realizó una nueva propuesta de capacitación así:

÷

DESARROLLO

Título: El Mundo Bajo CiberAtaque. Desafíos de la Ciberseguridad en las Organizaciones.

Agenda.
1. El quinto dominio.
2. Cuatro casos de ataques.
3. Tendencias de ciberdelincuencia.
4. Acciones para mitigar los ataques.
5. Conclusiones.

Ponente. Gottfried Blanco

Fecha propuesta el próximo miércoles 28 de mayo.

Pendiente de aprobación por SSF y definición de hora.

2. Revisión de despliegue Vicarius para análisis de vulnerabilidades internas.

RT solicita agendar espacio de trabajo para solucionar la desconexión de activos que se observa en la consola, para lo cual se requiere recoger los logs y validar si es un problema con el endpoint o de conectividad, entre otros, quedamos atentos a la agenda disponible de SSF.

3. Ingeniería social y Ethical Hacking

En cuanto a Ingeniería Social, el día lunes 19 de mayo, se realizó reunión para acordar detalles, el Ing. Juan José Olivella indicó que se puede realizar la prueba usando el evento de convocatoria de contratación de la Comisión Nacional del Servicio Civil. RT enviará la plantilla con un mensaje alusivo al tema acordado y desde el dominio comprado para la prueba.

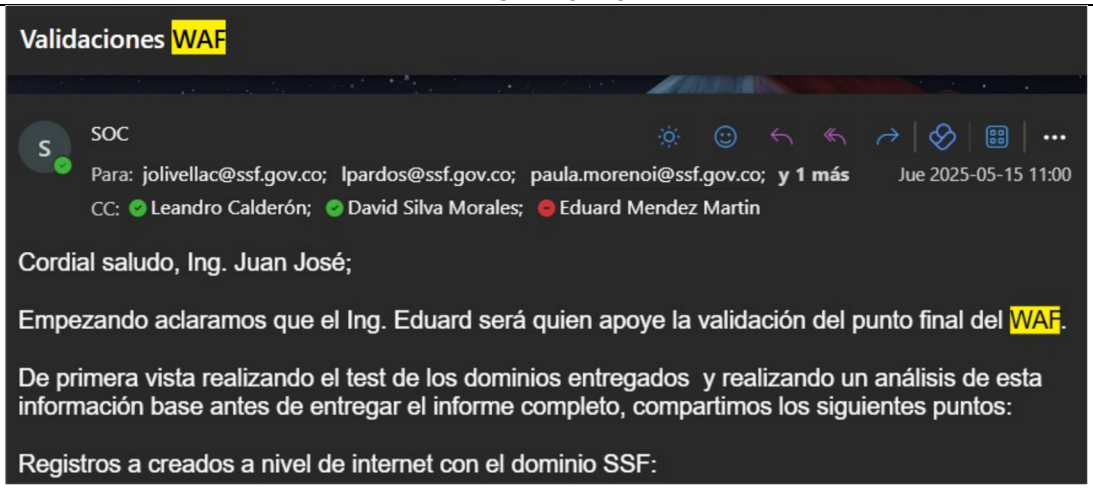
La Prueba EH: empieza el 23 de mayo.

4. Pruebas de Vulnerabilidad Externa

Termino la prueba de Vulnerabilidad Externa, pendiente informe final, sin embargo, se informó un avance el día jueves 15 de mayo en donde se indico por correo, la identificación de varios subdominios que corresponden a supersubsidio, y en donde se identificaron algunas vulnerabilidades. Ver a continuación imagen del correo enviado, detalles en el correo.

÷

DESARROLLO



5. Configuración SOC:

Se sigue verificando y ajustando la customización de los casos de uso para LUPITA, JURIDICA y SIMON.

RT sigue pendiente de confirmación de cuando realizarán las actividades de BD y Firewall indicadas por el Ing. Eduard Mendez. Por parte SSF manifiesta que está pendiente reunión de revisión interna la cual se debe realizar cuando se reintegre el equipo SSF que esta sin contrato desde el 09 de mayo.

6. Subsanar y enviar los siguientes informes:

- Informe trimestral (correcciones): Sigue pendiente entrega de observaciones por SSF. La Ing. Paula Andrea Moreno indica que se puede cerrar este pendiente dejando aceptado el Informe.
- Se entregó por correo el 13 de mayo el informe mensual de actividades, pendiente revisión por SSF
- Están pendientes de firma las actas, se planteará reunión para firmas el próximo lunes 26 de mayo.

Se acuerda con la Ing. Paula Moreno el próximo lunes 26 de mayo agendar un espacio para revisar informes y actas pendientes de aprobación y/o firma. Pendiente confirmación SSF.

7. Informe mensual SOC:

No se han recibido observaciones por parte de SSF al informe entregado de abril.

8. Solicitudes GLPI

Se revisó las respuestas a los dos casos puestos por SSF en la herramienta.

÷

Supersubsidio	ACTA DE REUNION	REALTIME C&S SAS

DESARROLLO

- En cuanto a uno de los casos “no reporte del SOC del apagado de la plataforma GLPI por parte de SSF”, RT informó que el tema se trató en la reunión pasada y que la respuesta estaba oportunamente en la herramienta GLPI.
  En la respuesta se mencionaba que las reglas solamente están configuradas para indisponibilidades por eventos de seguridad y que el apagado de la plataforma GLPI de SSF aparece como realizado manualmente, es decir como un evento de red y no de seguridad, por lo cual el sistema no alerto, sin embargo, se revisarán conjuntamente una serie de reglas para adecuar la configuración a las necesidades de SSF.

- El otro caso, fue la solicitud de la arquitectura SOC. RT la atendió oportunamente en la herramienta GLPI y se está en espera de observaciones por SSF.

TAREAS DEL PRÓXIMO PERIODO

EN IMPLEMENTACION

- ✓ En ejecución de pruebas de Ingeniería social.
- ✓ Terminar configuración SOC, implementación de los casos de uso para LUPITA, JURIDICA y SIMON
- ✓ Informe de pruebas de vulnerabilidad externa para los dominios:
  - https://www.ssf.gov.co/;
  - https://www.supersubsidio.gov.co;
  - https://www.ssf.col;
- ✓ Revisión implementación actual Vicarius
  - Fabricante Vicarius presentará caso de uso en fecha posterior, sin acordar aún.
  - Identificar causa raíz de desconexión de equipos de la consola Vicarius
  - Evaluar la posibilidad de implementar un Proxy para Vicarius

EN OPERACIÓN

- ✓ SSF entrega de observaciones informe mensual abril
- ✓ Revisión de actas

COMPROMISOS PACTADOS

Descripción	Responsable	Fecha de Entrega
Presentación caso de uso Vicarius	SSF	Aplazado, SSF indicará fecha
Solucionar el problema de desconexión de servidores de la consola Vicarius	SSF	Pendiente autorización de SSF para recoger logs

÷

Configuración SOC (LUPITA, JURIDICA y SIMON)	SSF - RT	Aplazado, SSF indicará fecha
Inicio de pruebas de EH	RT	23/05/2025
Evaluar la posibilidad de instalar proxy Vicarius	SSF	21/05/2025

÷