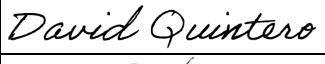
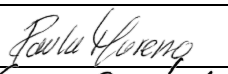
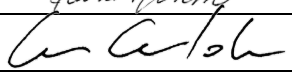
| Supersubsidio | ACTA DE REUNION | RealTime C&S SAS |
|---|---|---|

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **FECHA** | 16/07/2025 | **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.<br>X Clasificada.<br>☐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 |
| 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 Tendencias de Seguridad:

   - Pendiente por SSF la aprobación de temario y fecha de capacitación propuesto por correo el 20/05/2025: El Mundo Bajo CiberAtaque. Desafíos de la Ciberseguridad en las Organizaciones. **SSF informa que tiene pendiente contestar por correo**.

   - A solicitud de SSF no se realizó la sesión el 15/05/2025 de la presentación del caso de uso Vicarius. **SSF informa que tiene pendiente contestar por correo**.

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

   - Se encuentran desplegados 21 agentes definidos por SSF. RT está disponible si se necesita apoyo para el desplieguen de nuevos agentes.

÷

**DESARROLLO**

- RT informa que envío informe de vulnerabilidades para todos los agentes desplegados, mediante correo (10/06/2025).
  **SSF informa que contestará por correo si tiene observaciones.**

- RT informa que envío informe de vulnerabilidades para 5 activos de información el viernes 11 de Julio 2025, solicitados mediante correo de la Ing. Paula (11/07/2025). SSF informa que se debe ajustar el informe dado que no entrega la información solicitada. El compromiso por RT es enviar el informe ajustada durante este mismo día. Queda pendiente revisar si el ajuste corresponde a la información solicitada.

- Respecto a la plantilla de informe de vulnerabilidades, se enviará el día de hoy una nueva (diferente a la plantilla trabajada anteriormente) con el informe comprometido para los 5 activos de información solicitados por la Ing. Paula. **SSF dará retroalimentación del informe y la plantilla, mediante correo**.

3. Pruebas de Vulnerabilidad Externa

- Se entregó por correo el primer informe de pruebas de vulnerabilidades externas para los 5 dominios externos (30/05/2025).
  **SSF revisará y contestará por correo si tiene observaciones.**

- RT informa que envío informe de vulnerabilidades oportunamente, correspondiente al escaneo del portal GLPI mediante correo (10/07/2025).
  **SSF informa que contestará por correo si tiene observaciones.**

- RT informa que envío segundo informe de vulnerabilidades de 4 dominios mediante correo (15/07/2025) y que está en ejecución el escaneo del portal principal.
  **SSF informa que contestará por correo si tiene observaciones de los informes.**

4. Ingeniería social y Ethical Hacking

- SSF envío Landing para la captura de credenciales. RT ejecuto la prueba y envío el informe el 14 de julio. **Queda pendiente la revisión y envío de observaciones por parte de SSF**. Se acuerda que el 17 de julio a las 11 am, se hará presentación del informe.

- En cuanto a las fechas de la prueba de ingeniería social interna que está pendiente de aprobación, SSF propone que se haga el 30 o 31 de julio. RT revisará la viabilidad para realizar la prueba en las fechas solicitadas.

5. Configuración SOC:

Se realizó reunión para lograr el reenvío logs FortiWAF referentes a ataques de OWASP10. El detalle de los resultados de la reunión los enviará por correo el día de hoy el Ing. Eduard Mendez. Pendiente realizar el mismo ejercicio para el firewall. RT Informa que esta atento a la invitación para realizar pruebas.

÷

**DESARROLLO**

En cuanto a BD, el Ing. Eduard informó que esta pendiente por atender el correo enviado el 25 de abril de 2025, con el asunto: Requerimientos log de eventos Base de Datos, para envío de logs al SIEM.

Se realizó reunión para configuración portal WEB pruebas, para envío de eventos a la consola SIEM, El Ing. Eduard enviará correo con el detalle de actividades realizadas y compromiso para el portal WEB de producción.

RT sigue pendiente la customización de los casos de uso para JURIDICA, SIMON y FW.
SSF informará por correo cuando se puede realizar una sesión conjunta.

6. Subsanar y enviar los siguientes informes:

- Pendientes revisión y firma de actas.
  **El Ing. Juan José informa que están pendientes algunas actas de revisión para su firma.**

TAREAS DEL PRÓXIMO PERIODO

EN IMPLEMENTACION

- ✓ En ejecución de pruebas de Ingeniería social (externas).
- ✓ Terminar configuración SOC, implementación de los casos de uso para JURIDICA, SIMON, y FW.
- ✓ Capacitaciones en tendencias de seguridad.

EN OPERACIÓN

- ✓ Elaboración próximo informe mensual
- ✓ Revisión de actas
- ✓ Revisión Informe mensual.

**COMPROMISOS PACTADOS**

| Descripción | Responsable | Fecha de Entrega |
|---|---|---|
| Enviar por correo respuesta y/o fecha de la capacitación “El Mundo Bajo CiberAtaque. Desafíos de la Ciberseguridad en las Organizaciones” | Juan José Olivella | 09/07/2025 |
| Enviar por correo observaciones del primer informe de pruebas de vulnerabilidad externa. | Juan José Olivella | 09/07/2025 |

÷

| | | |
|---|---|---|
| Enviar por correo observaciones del segundo informe de pruebas de vulnerabilidad externa (4 dominios). | David Quintero | 23/07/2025 |
| Entregar nueva plantilla para informe de pruebas de vulnerabilidades interna | Eduard Mendez | 18/07/2025 |
| Entregar nuevamente el informe para 5 servidores solicitado el 11 de julio por la Ing. Paula. | Leandro Calderón | 16/07/2025 |
| Enviar por correo observaciones del informe de pruebas de vulnerabilidad interna (todos los agentes). | Juan José Olivella | 23/07/2025 |
| Configuración SOC (JURIDICA, SIMON, y FW) | Juan José Olivella | 23/07/2025 |

÷