PRESTAR SERVICIOS DE MONITOREO Y ATENCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ID: OTIC-756)

Supersubsidio

Diciembre 12 de 2024

Supersubsidio

PLAN DE TRABAJO

REALTIME CONSULTING & SERVICES
Líderes en Soluciones de Seguridad
(SOC/NOC, Analítica de Datos, SGSI, Ethical Hacking, MSPI y Ciberseguridad)

conviest.

1. Alcance del proyecto
2. Equipo de Trabajo
3. Cronograma general del proyecto
4. Avances del Proyecto
5. Compromisos

Supersubsidio

REALTIME CONSULTING & SERVICES
Líderes en Soluciones de Seguridad
(SOC/NOC, Analítica de Datos, SGSI, Ethical Hacking, MSPI y Ciberseguridad)

conviest.

1. EQUIPO DE TRABAJO

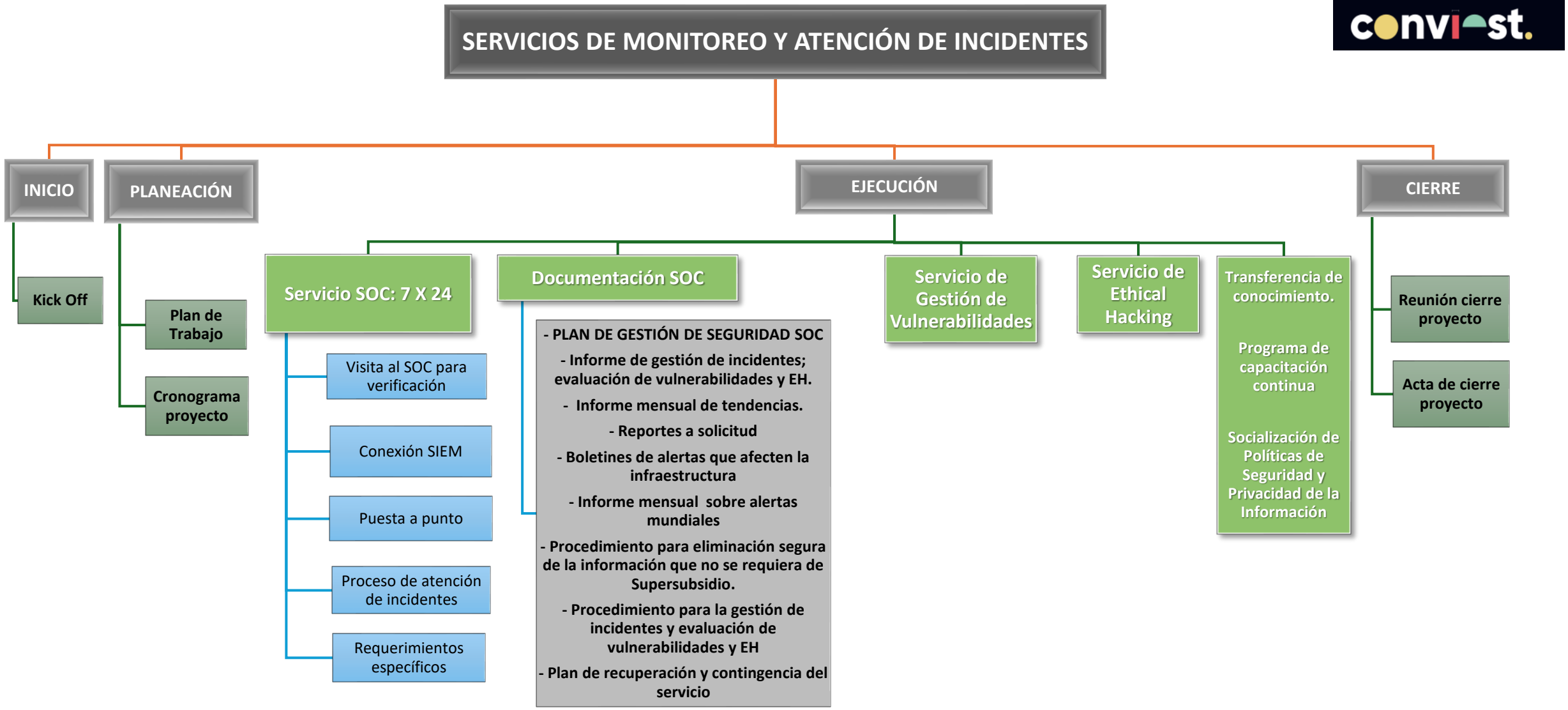
SUPERSUBSIDIO

- EQUIPO DE TRABAJO SUPERSUBSIDIO

REALTIME

- CAMILO RODRIGUEZ, GERENTE DE SERVICIOS
- CESAR CORDOBA, GERENTE DE PROYECTOS
- EDUARD MENDEZ, CONSULTOR SENIOR DE DESPLIEGUE
- JENSY MARTINEZ, LIDER SOC
- RAFAEL MORALES, CONSULTOR TECNICO SOC
- RONALD VARGAS, ANALISTA NIVEL 2 SOC
- LEANDRO CALDERON, APOYO LIDER SOC
- DAVID SILVA, APOYO IMPLEMENTACION

2. Alcance del proyecto - WBS

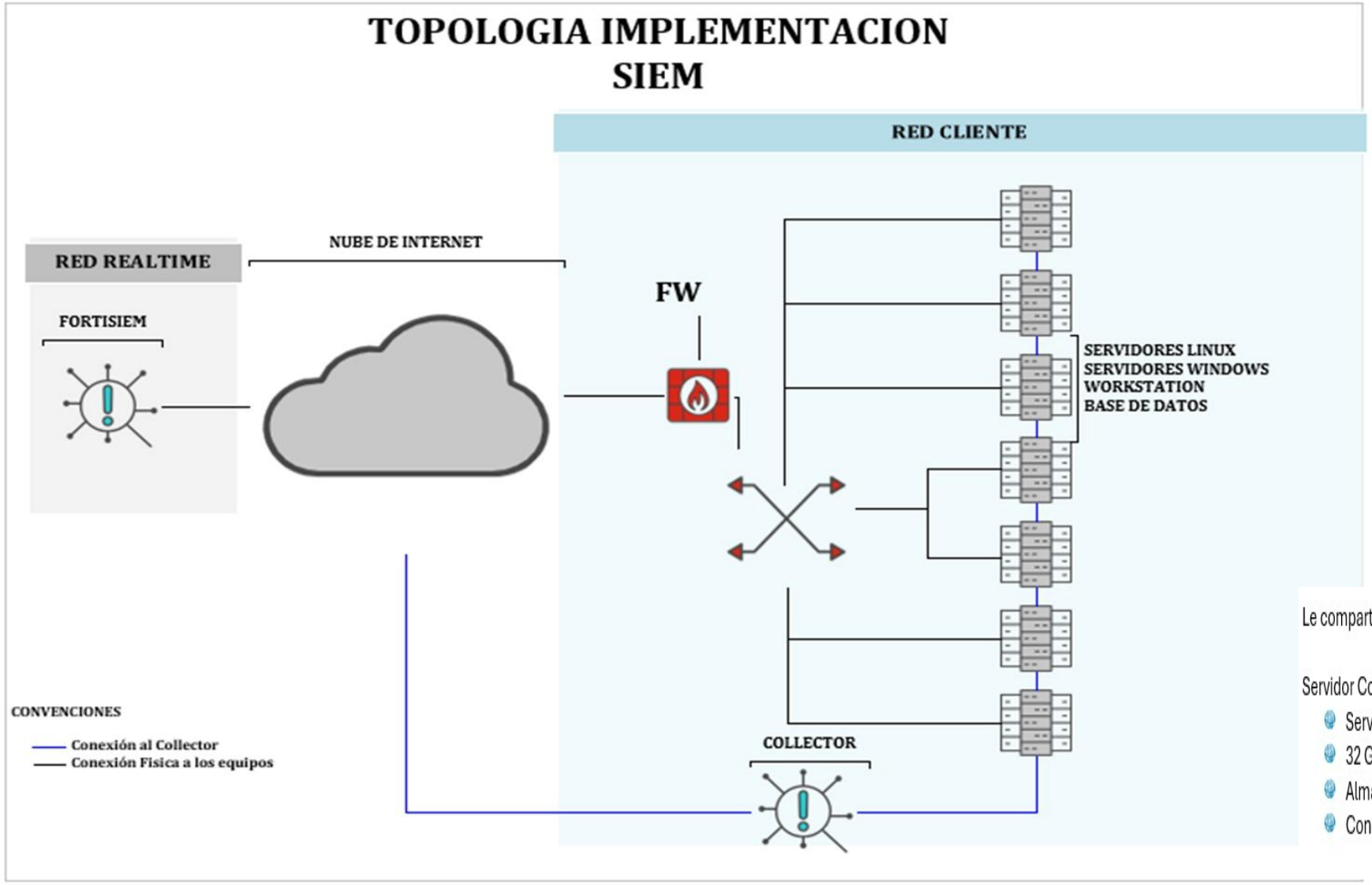


Supersubsidio

2. Alcance del proyecto - WBS

REALTIME CONSULTING & SERVICES
Líderes en Soluciones de Seguridad
(SOC/NOC, Analítica de Datos, SGSI, Ethical Hacking, MSPI y Ciberseguridad)

conviest.



Le comparto los requerimientos de computo que se requieren para máquina virtual:

Servidor Colector SIEM:

- Servidor con 8 core,
- 32 GB de memoria RAM.
- Almacenamiento: 25 GB partición OS y 100 GB partición OPT.
- Conectividad física de red dentro de la infraestructura de TI.

Supersubsidio

REALTIME CONSULTING & SERVICES
Líderes en Soluciones de Seguridad
(SOC/NOC, Analítica de Datos, SGSI, Ethical Hacking, MSPI y Ciberseguridad)

conviest.

3. Cronograma general del proyecto

Plazo de Ejecución 13 meses

Ítem	Actividad	Fecha objetivo
1	Reunión de Inicio	09/12/2024
2	Visita a las instalaciones del SOC - RT	09/12/2024
3	Entrega de Plan de Trabajo y Cronograma	10/12/2024
4	Levantamiento de información de los equipos a conectar	11/12/2024
5	Levantamiento de información desde el SIEM actual	11/12/2024
6	Plan de conexión de equipos de la SSF	11/12/2024
7	Instalación y configuración y puesta a punto	12/12/2024
8	Entrega de procedimientos de gestión	19/12/2024
9	Inicio del servicio de monitoreo	19/12/2024
10	Plan de pruebas de vulnerabilidad y EH	19/12/2024
11	Plan de capacitaciones y transferencia de conocimiento	19/12/2024
	Transferencia de conocimiento	21/01/2025 - 24/01/2025
12	Informe mensual de gestión	20/12/2024
13	Informe mensual resultado del monitoreo	20/12/2024
14	Informe periódicos de gestión de seguridad, evaluación de vulnerabilidades y EH.	23/12/2024
15	Reunión y acta de cierre	09/01/2026

Supersubsidio

REALTIME CONSULTING & SERVICES
Líderes en Soluciones de Seguridad
(SOC/NOC, Analítica de Datos, SGSI, Ethical Hacking, MSPI y Ciberseguridad)

conviest.

4. TRANSFERENCIA DE CONOCIMIENTO		
Duración	20/01/2024	**Fecha objetivo**
2 horas	20/01/2024	20/01/2024
2 horas	20/01/2024	21/01/2024
2 horas	20/01/2024	22/01/2024
2 horas	20/01/2024	23/01/2024

4. CAPACITACIONES PROPUESTAS		
1	La IA en la seguridad de la Información	20/01/2024
2	Ley 1581 Protección de Datos Personales.	21/01/2024
3	Minería de Datos	22/01/2024
4	Modelo de Seguridad y Privacidad de la Información MPSI	23/01/2024

Supersubsidio

REALTIME CONSULTING & SERVICES
Líderes en Soluciones de Seguridad
(SOC/NOC, Analítica de Datos, SGSI, Ethical Hacking, MSPI y Ciberseguridad)

conviest.

5. Entrega de Copias de Seguridad y Casos de Uso

Ítem	Actividad	Fecha objetivo
1	Acordar la información que se debe entregar	09/12/2025
2	Identificar responsables	09/12/2025
3	Establecer mecanismos físicos y lógicos para la entrega de la Información	10/12/2025
4	Generar copias de seguridad	30/12/2025
5	Elaborar documentación	30/12/2025
6	Proceder con la ejecución de la entrega	01/01/2026
7	Elaborar acta de entrega	02/01/2026

Supersubsidio

REALTIME CONSULTING & SERVICES
Líderes en Soluciones de Seguridad
(SOC/NOC, Analítica de Datos, SGSI, Ethical Hacking, MSPI y Ciberseguridad)

conviest.

6. Entrega de Copias de Seguridad y Casos de Uso

Ítem	Actividad	Fecha objetivo
1	Acordar la información que se debe entregar	09/12/2025
2	Identificar responsables	09/12/2025
3	Establecer mecanismos físicos y lógicos para la entrega de la Información	10/12/2025
4	Generar copias de seguridad	30/12/2025
5	Elaborar documentación	30/12/2025
6	Proceder con la ejecución de la entrega	01/01/2026
7	Elaborar acta de entrega	02/01/2026

Supersubsidio

REALTIME CONSULTING & SERVICES
Líderes en Soluciones de Seguridad
(SOC/NOC, Analítica de Datos, SGSI, Ethical Hacking, MSPI y Ciberseguridad)

7. Estándares Aplicados

Ítem	DIRECTRICES y LINEAMIENTOS	APLICACIÓN
1	ISO 20000-1	Se aplicará este estándar internacional para definir los requisitos, establecer, implementar, operar, monitorear, revisar, mantener y mejorar los servicios SOC entregados a la SSF.
2	ISO 27001	Se aplicará este estándar internacional en la sección que corresponde al monitoreo de eventos SOC para establecer, implementar, mantener y mejorar para fortalecer los controles correspondientes del Sistema de Gestión de la Seguridad de la Información de la SSF.
3	SOMM – SECURITY OPERATIONS MODEL	Se tendrá en cuenta el Modelo de Madurez de Operaciones de Seguridad (SOMM) para evaluar y mejorar sus capacidades de ciberseguridad del SOC. Proporciona un enfoque estructurado para evaluar la efectividad de las operaciones de seguridad, identificar áreas de mejora y desarrollar una hoja de ruta para mejorar la postura de seguridad.

Supersubsidio

REALTIME CONSULTING & SERVICES
Lideres en Soluciones de Seguridad
(SOC/NOC, Analítica de Datos, SGSI, Ethical Hacking, MSPI y Ciberseguridad)

6. Formato de avance y compromisos del proyecto

conviest.

Ítem	Actividad	Estado	Compromiso	Fecha Real
1	Reunión de Inicio			09/1272024
2	Visita a las instalaciones del SOC - RT			
3	Entrega de Plan de Trabajo y Cronograma			
4	Plan de conexión de equipos de la SSF			
5	Configuración y puesta a punto			
6	Puesta a punto del canal de comunicaciones SSF y RT			
7	Entrega de procedimientos de gestión			
8	Inicio del servicio de monitoreo			
9	Plan de pruebas de vulnerabilidad y EH			
10	Plan de capacitaciones y transferencia de conocimiento			
11	Informe mensual de gestión			
12	Informe mensual resultado del monitoreo			
13	Informe periódicos de gestión de seguridad, evaluación de vulnerabilidades y EH.			
14	Reunión y acta de cierre			

Supersubsidio

7. Próximos pasos

REALTIME CONSULTING & SERVICES
Líderes en Soluciones de Seguridad
(SOC/NOC, Analítica de Datos, SGSI, Ethical Hacking, MSPI y Ciberseguridad)

conviest.

Planeación

- Levantamiento de Información
- Instalación del Collector y agentes
- Conexión con el SOC RT
- Entrega Plan de Trabajo y cronograma
- Entrega de plan de conexión del SOC
- Entrega del plan de capacitación y transferencia de conocimiento
- Entrega del plan de vulnerabilidades y EH.
- Entrega de procedimientos de atención de incidentes

Ejecución

- Configuración y puesta a punto
- Inicio del Servicio