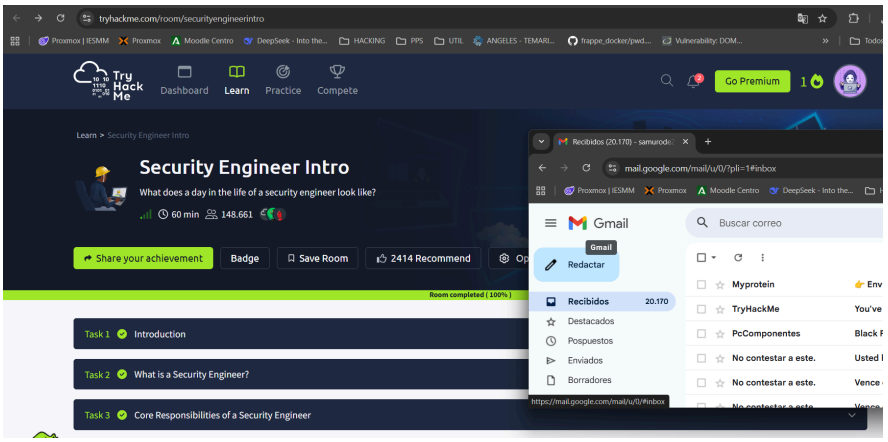
# Tarea 1.6: Fundamentos de Ingeniería de Seguridad y OPSEC


Trabajo realizado por:
Samuel Romero de los Reyes

Curso de especialización:
CETI

# Índice

# 1.Introducción a la Ingeniería de Seguridad (Security Engineer Intro)




## 1.1.Rol y Funciones

El rol principal de un Ingeniero de Seguridad dentro de una organización es proteger los activos digitales y mantener la postura de ciberseguridad de la empresa.
Para ello, el ingeniero:

- Asume la responsabilidad global de la seguridad, asegurando que los riesgos cibernéticos se mantengan al mínimo.
- Diseña e implementa sistemas, redes e infraestructuras seguras, siguiendo principios como secure by design.
- Supervisa y mejora continuamente la seguridad, gestionando cambios, riesgos, vulnerabilidades y cumplimiento normativo.
- Colabora con otros equipos y puede asumir responsabilidades adicionales como gestionar herramientas de seguridad, realizar ejercicios tabletop o participar en planes de recuperación ante desastres.

## 1.2.Conceptos Claves

### 1.2.1.Amenaza

Una amenaza es cualquier evento, acción o actor que puede causar daño a un sistema, datos u organización.

Ejemplo:
Un ciberdelincuente intentando enviar correos de phishing a empleados para robar credenciales.

#### 1.2.2.Vulnerabilidad

Una vulnerabilidad es una debilidad o fallo en un sistema que puede ser explotado por una amenaza.

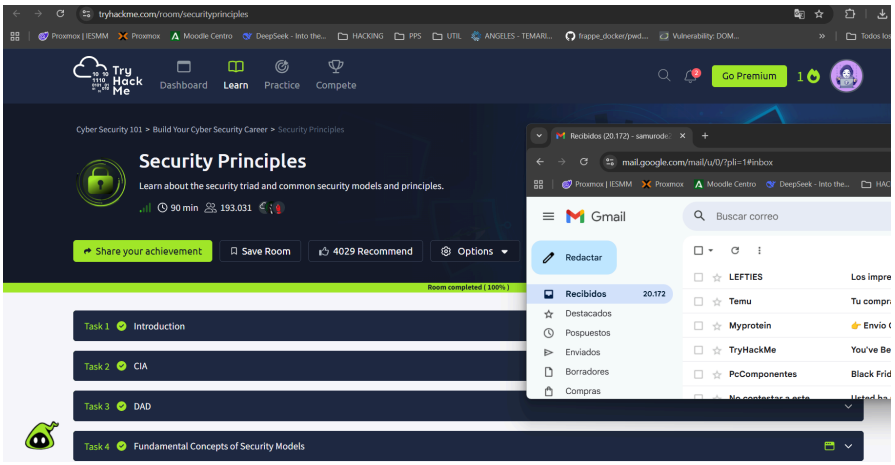
Ejemplo:
Un servidor web que utiliza una versión desactualizada de Apache con una falla conocida que permite la ejecución remota de código.

#### 1.2.3.Riesgo

El riesgo es la probabilidad de que una amenaza explote una vulnerabilidad y el impacto que eso tendría en la organización.

Ejemplo:
Existe un alto riesgo de que un atacante comprometa un servidor desactualizado (vulnerabilidad) mediante un exploit disponible públicamente (amenaza), lo que podría causar pérdida de datos o interrupciones del servicio (impacto).

# 2.Principios de Seguridad (Security Principles)




## 2.2.El Triángulo Fundamental (CIA)

#### 2.2.1.Confidencialidad

La confidencialidad garantiza que solo las personas o entidades previstas pueden acceder a los datos.

Impacto de su violación:

- En compras online: si se filtran datos personales o tarjetas, la empresa sufre pérdidas económicas y de reputación.

- En un hospital: si un atacante roba historias clínicas y las publica, el proveedor de salud incurre en pérdidas, responsabilidades legales y daño a pacientes.

#### 2.2.2.Integridad

La integridad asegura que los datos no puedan ser alterados sin autorización, y que si se alteran, la alteración pueda detectarse.

Impacto de su violación:

- En compras: pedidos enviados al lugar incorrecto.
- En hospitales: riesgo de tratamientos peligrosos o diagnósticos totalmente incorrectos.

#### 2.2.3.Disponibilidad

La disponibilidad garantiza que un sistema o servicio esté accesible cuando se necesite.

Impacto de su violación:

- En un comercio online: los clientes abandonan la tienda si la web falla repetidamente.
- En un hospital sin papel: si la base de datos queda inaccesible, el centro no puede funcionar adecuadamente y el tratamiento de los pacientes queda estancado.

### 2.3.Análisis de Principios

#### 2.3.1.Defensa en Profundidad (Defence in Depth)

Este principio consiste en crear un sistema con múltiples niveles de seguridad, de modo que no exista un único punto de fallo.

Cómo mejora la postura de seguridad:

- Dificulta el avance del atacante, incluso si rompe una capa.
- Limita el alcance del ataque, porque debe superar varias barreras consecutivas.
- Aumenta el tiempo de detección, ya que más niveles significan más puntos donde registrar actividad sospechosa.
- Reduce la probabilidad de que un fallo puntual derive en una brecha completa.

### 2.3.2.Principio de Mínimo Privilegio (Least Privilege)

El estándar ISO/IEC 19249 lo incluye como uno de sus cinco principios de diseño. Significa que a cada usuario o proceso solo se le deben otorgar los permisos estrictamente necesarios para realizar su tarea, y nada más.

Cómo mejora la postura de seguridad

- Reduce el impacto de un fallo humano o un error: si el usuario no tiene permisos de escribir, no podrá modificar datos por accidente.
- Minimiza el daño si una cuenta es comprometida: un atacante no podrá hacer más que lo que la cuenta ya podía hacer.
- Limita el movimiento lateral dentro del sistema.
- Evita que usuarios o aplicaciones accedan a información que no deberían ver.

### 2.3.3.Principio de “Confiar pero Verificar” (Trust but Verify)

El principio enseña que aunque se confíe en un usuario o sistema, siempre se debe verificar su comportamiento.

Esto requiere:

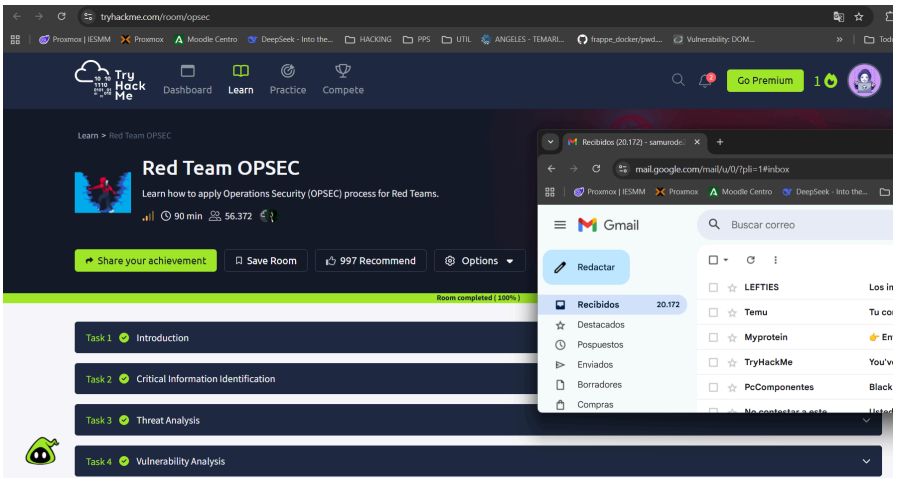
- Registro y auditoría (logs).
- Sistemas automatizados como proxies, IDS/IPS, etc.
- Revisión periódica de actividad.

Se reconoce que revisar absolutamente todo es imposible, por lo que la verificación debe apoyarse en mecanismos automáticos.

Cómo mejora la postura de seguridad

- Permite detectar actividades anómalas incluso de entidades “de confianza”.
- Disminuye el riesgo de abuso interno o comportamientos inesperados.
- Evita que la confianza se convierta en una vulnerabilidad.
- Facilita la investigación de incidentes gracias al registro de acciones.

# 3.Seguridad Operacional OPSEC (Red Team OPSEC)




## 3.1.Definición y Propósito

OPSEC es un proceso sistemático diseñado para negar a un adversario el acceso a información crítica sobre nuestras intenciones, capacidades, actividades y limitaciones. Su objetivo es impedir que el adversario pueda reunir indicios que revelen la planificación o ejecución de actividades sensibles. Este proceso incluye cinco pasos:

1. Identificar información crítica
2. Analizar amenazas
3. Analizar vulnerabilidades
4. Evaluar riesgos
5. Aplicar contramedidas

OPSEC es esencial porque:

1. Protege información que, si se obtiene, puede perjudicar la operación.

La información crítica no tiene por qué ser secreta, cualquier dato que ayude al adversario a anticiparse o interferir en nuestras acciones puede comprometer la misión.

2. Evita que el adversario pueda relacionar actividades entre sí.

Si varios elementos (IP, dominios, herramientas, hostnames, etc.) apuntan al mismo origen, el adversario puede detectar, bloquear o neutralizar la operación. Una única pista mal gestionada puede permitirle unir todas las piezas.

3. Limita la capacidad del adversario para entender nuestras intenciones y capacidades.

Si la blue team u otros actores maliciosos pueden identificar qué herramientas empleamos, qué infraestructura usamos o qué estamos intentando hacer, estarán en mejor posición para detenernos.

4. Reduce el impacto de vulnerabilidades de OPSEC.

Una vulnerabilidad aparece cuando el adversario puede obtener información crítica y usarla para afectar nuestros planes. Sin OPSEC, estas vulnerabilidades se multiplican.

5. Permite evaluar riesgos de forma realista.

OPSEC obliga a analizar la probabilidad de que una vulnerabilidad sea explotada y el coste de que eso ocurra. Esto ayuda a priorizar qué proteger y cómo protegerlo.

6. Establece contramedidas que impiden, engañan o dificultan la obtención de información.

Las contramedidas buscan evitar la detección, generar interpretaciones alternativas o impedir que el adversario recoja datos.

## 3.2. El Proceso OPSEC

### 3.2.1. Identificación de información crítica

Consiste en determinar qué información, si fuera obtenida por el adversario, podría perjudicar la operación. Incluye datos sobre intenciones, capacidades, actividades, limitaciones, infraestructura, dominios, IPs, herramientas o cualquier elemento que permitiría al adversario anticiparse o bloquear la misión.

### 3.2.2. Análisis de amenazas

Implica identificar quiénes son los adversarios, cuáles son sus intenciones y cuáles son sus capacidades. En un contexto de red team, el blue team es un adversario porque busca impedir nuestras acciones, pero también lo son actores maliciosos externos con capacidades e intenciones variables.

### 3.2.3. Análisis de vulnerabilidades

Se busca detectar situaciones en las que un adversario pueda obtener información crítica y usarla en nuestra contra.

### 3.2.4. Evaluación de riesgos

Consiste en valorar la probabilidad de que una vulnerabilidad sea explotada y el impacto que tendría si ocurre. Esto requiere conocer las capacidades del adversario.

#### 3.2.5.Aplicación de contramedidas

Son las acciones destinadas a impedir que el adversario obtenga información crítica, ofrecer interpretaciones alternativas o dificultar sus capacidades de recopilación.

### 3.3.Aplicación Práctica

Un empleado trabaja desde casa y, sin darse cuenta, publica en LinkedIn una foto de su escritorio para mostrar su “setup de teletrabajo”.
En la imagen se ve:

- La pantalla con una lista de proyectos internos
- Nombres de clientes
- Un documento abierto que muestra parcialmente un diagrama de red

Un ciberdelincuente o incluso un competidor que monitoriza redes sociales podría:

- Identificar clientes actuales
- Inferir tecnologías usadas por la empresa
- Detectar sistemas internos
- Preparar ataques dirigidos (phishing, explotación de sistemas concretos, ingeniería social, etc.)

Contramedida específica:

Aplicar una política clara de OPSEC que prohíba compartir imágenes u otro contenido que pueda revelar información crítica sin revisión previa.

Como:

● Requerir que todo el personal use fondos de pantalla neutros y bloquee la pantalla antes de hacer fotos.

● Formación en OPSEC para identificar qué información podría ser crítica y no debe exponerse.

## 4.Conclusión Personal

Comprender los fundamentos de la Ingeniería de Seguridad antes de adentrarse en aspectos técnicos avanzados es esencial para desarrollar una visión completa y profesional de la ciberseguridad. La introducción al rol del ingeniero de seguridad, sus funciones, responsabilidades y la necesidad de mantener una postura de seguridad coherente permite entender que la defensa no se basa solo en

herramientas, sino en criterios, análisis y diseño estratégico. Conocer desde el inicio qué son las amenazas, las vulnerabilidades y los riesgos proporciona el contexto necesario para interpretar cualquier tecnología o ataque con una mentalidad orientada a la protección.

Del mismo modo, los principios fundamentales como el modelo CIA, la defensa en profundidad, el principio de mínimo privilegio o confiar pero verificar refuerzan esa base, mostrando que toda solución técnica debe alinearse con estos pilares si se quiere construir seguridad real y sostenible.

En cuanto a las salas, la que me resultó más útil fue la de OPSEC, porque muestra cómo incluso cuando se dominan los fundamentos técnicos, una mala gestión de la información puede comprometer toda una operación. La conexión entre teoría y práctica en OPSEC hace evidente la importancia de la disciplina, la planificación y la atención al detalle en cualquier actividad de seguridad ofensiva o defensiva.