



# Diplomado de Ciberseguridad y Gestión de Seguridad de la Información



## **Módulo 2:**

# Identificación y Mitigación de Riesgos de Seguridad

## **Sesión 1:**

### Tipos de amenazas y riesgos comunes



## OBJETIVO DE LA SESIÓN:

Comprender los tipos de amenazas más comunes en ciberseguridad, su clasificación como riesgos y su impacto en personas y organizaciones.



# ¿Qué es un riesgo en ciberseguridad?

Es la combinación entre la probabilidad de que ocurra una amenaza y el impacto que tendría sobre la organización o persona afectada.

## Fórmula básica:

Riesgo = Probabilidad x Impacto

### Concepto de amenaza

**Amenaza:** Evento potencial que puede explotar una vulnerabilidad y causar daño.

**Ejemplo:** Un hacker intentando acceder sin permiso a un servidor.



### Concepto de vulnerabilidad

**Vulnerabilidad:** Debilidad o falla en un sistema, proceso o persona que puede ser explotada por una amenaza.

**Ejemplo:** Usar la misma contraseña en todas las cuentas.





# Tipos de malware

## Virus

Se adhieren a otros archivos ejecutables y se propagan cuando se abren.

- **Ejemplo:** Un archivo Word infectado que al abrirse propaga el virus.

## Gusanos (worms)

Se replican por redes sin intervención del usuario.

- **Ejemplo:** Envío masivo de copias a todos los contactos del correo.

## Troyanos

Se presentan como programas útiles, pero ocultan software malicioso.

- **Ejemplo:** Un juego gratuito que instala un spyware en segundo plano.

## Spyware

Espía la actividad del usuario para robar información como contraseñas o historiales de navegación.

## Ransomware

Cifra archivos y exige un rescate para liberarlos.

- **Ejemplo:** “WannaCry” afectó a empresas y hospitales en todo el mundo.



# Ransomware (secuestro de información)

tipo de malware que bloquea o cifra los datos de una víctima y exige un rescate para restaurar el acceso.

## Ejemplos comunes

### **Cifrado**

Este tipo cifra los archivos de la víctima, haciéndolos inaccesibles hasta que se paga un rescate

### **Bloqueo de pantalla**

Bloquea el acceso al dispositivo o sistema operativo, mostrando un mensaje que exige un pago

### **Multiextorsión**

No solo cifran los datos, sino que también amenazan con filtrar información confidencial si no se paga

# Ejemplo



Mas información <https://www.noticiasrcn.com/colombia/fiscalia-identifica-a-ransomhouse-como-presuntos-responsables-del-ciberataque-454108>

# Etapas de un ataque de Ransomware



**Etapa 1**

- Reconocimiento

**Etapa 2**

- Compromiso inicial

**Etapa 3**

- Persistencia

**Etapa 4**

- Recopilación de información

**Etapa 5**

- Escalamiento de privilegios

**Etapa 6**

- Desplazamiento lateral

**Etapa 7**

- Ejecución

**Etapa 8**

- Impacto final



# Reconocimiento

Los ciberdelincuentes exploran para identificar vulnerabilidades y recopilar información sobre el objetivo. Buscan sistemas expuestos, fallos específicos o datos valiosos para planificar ataques lucrativos.



Ingeniería  
social

Análisis de  
red

Inteligencia de  
Fuentes Abiertas  
(OSINT)

Ejemplo: Un atacante usa LinkedIn para identificar empleados de una empresa, envía un phishing simulando ser un colega y escanea puertos con Nmap (Network Mapper) para encontrar servidores sin parches.

## Prevención:

- Capacitar empleados contra phishing
- Usar firewalls y herramientas de detección como Nessus
- Limitar exposición en redes sociales.

Etapa 1

Etapa 2

Etapa 3

Etapa 4

Etapa 5

Etapa 6

Etapa 7

Etapa 8

# Exploits de día cero

Robo de credenciales o reclutamiento interno)

- Filtros de correo anti-phishing (e.g., Proofpoint).
- Autenticación multifactor (MFA).
- Parches rápidos para vulnerabilidades conocidas.

## Etapa 8

# Persistencia: Asegurando el Control



Los atacantes garantizan acceso continuo creando puertas traseras o modificando sistemas. En 2022, el 82% de los ataques de ransomware usaron tácticas de persistencia (Coveware).

Puertas traseras  
con malware sin  
archivos

Modificación de  
AutoStart, tareas  
programadas o  
registro.

Secuestro de  
procesos  
legítimos (e.g.,  
svchost.exe).

## Prevención:

- Monitorear procesos con herramientas como Sysinternals.
- Escanear con antivirus
- Deshabilitar AutoRun y revisar registros.

Ejemplo: Un atacante instala un rootkit que crea una tarea programada para ejecutarse cada hora, manteniendo acceso incluso tras reinicios.

Etapa 1

Etapa 2

Etapa 3

Etapa 4

Etapa 5

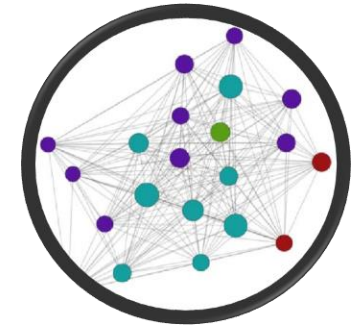
Etapa 6

Etapa 7

Etapa 8

# Recopilación de Información

Los atacantes recolectan datos críticos sobre la red para maximizar el impacto del ataque, identificando activos valiosos como propiedad intelectual o datos de clientes.



Escaneo de red  
para mapear  
sistemas.

Keyloggers para  
capturar  
credenciales.

Descubrimiento  
de datos para  
localizar  
archivos  
sensibles.

## Prevención:

- Usar cifrado de datos
- Implementar detección de intrusos (IDS).
- Restringir acceso a datos sensibles.

Ejemplo: Un atacante usa un keylogger para capturar contraseñas y escanea la red para localizar bases de datos financieras.

Etapa 1

Etapa 2

Etapa 3

Etapa 4

Etapa 5

Etapa 6

Etapa 7

Etapa 8

# Escalamiento de Privilegios

Los atacantes buscan derechos administrativos para controlar la red, explotando configuraciones débiles. El 40% de las identidades vulnerables son cuentas de administrador (Illusive).



Exploits de  
configuraciones  
débiles

Robo de  
credenciales

Ataques a  
Active Directory  
o Azure.

## Prevención:

- Aplicar Mínimos privilegios.
- Parchear sistemas regularmente.
- Monitorear privilegios de usuarios

Ejemplo: Un atacante extrae credenciales de administrador desde Active Directory, obteniendo control total de la red.

Etapa 1

Etapa 2

Etapa 3

Etapa 4

Etapa 5

Etapa 6

Etapa 7

Etapa 8

# Desplazamiento Lateral

Los atacantes se mueven por la red para comprometer más sistemas, buscando activos críticos. El 25% de los incidentes involucran desplazamiento lateral (VMware, 2022).



Uso de RDP,  
SMB o  
PowerShell

Exploits de  
software sin  
parches

Robo de  
credenciales  
para nuevos  
hosts.

## Prevención:

- Segmentar redes para limitar acceso.
- Deshabilitar RDP innecesario.
- Monitorear tráfico con firewalls.

Ejemplo: Un atacante usa credenciales robadas para acceder a servidores, cifrando datos en múltiples sistemas

Etapa 1

Etapa 2

Etapa 3

Etapa 4

Etapa 5

Etapa 6

Etapa 7

Etapa 8

# Ejecución

Los atacantes personalizan y distribuyen el ransomware, asegurando canales de comando y control (C2). Es la última etapa antes del impacto, con oportunidad final para detener el ataque.



Personalización  
de ransomware.

Pruebas de  
distribución

Canales C2  
para  
comunicación

Ejemplo: Un operador de ransomware prueba un archivo en un servidor comprometido, estableciendo un canal C2 para enviar datos robados antes del cifrado.

## Prevención:

- Detectar C2 con herramientas como Zeek.
- Escanear red con un EDR.
- Capacitar en detección de archivos sospechosos.

Etapa 1

Etapa 2

Etapa 3

Etapa 4

Etapa 5

Etapa 6

Etapa 7

Etapa 8

# Impacto

Los atacantes ejecutan el ransomware, cifran datos y exigen rescate. El 30% de los ataques en 2022 incluyeron extorsión de datos (Sophos). Es el primer indicio para muchas empresas.



Cifrado  
masivo de  
archivos.

Bloqueo de  
sistemas

Nota de  
rescate con  
instrucciones

## Prevención:

- Backups offline regulares.
- Usar EDR para detección temprana.
- Capacitar en respuesta a incidentes.

Ejemplo: El ransomware Clop cifra servidores, cambia extensiones a “.clon” y muestra una nota exigiendo Bitcoin para descifrar y no filtrar datos.

Etapa 1

Etapa 2

Etapa 3

Etapa 4

Etapa 5

Etapa 6

Etapa 7

Etapa 8

# Ejercicio



En colab cifra un .txt usando cifrado cesar

## Objetivo:

Entender el funcionamiento básico de un ransomware al cifrar un archivo con el algoritmo César, simulando cómo los atacantes bloquean datos y exigen rescate. Esto ilustra etapas como ejecución e impacto, fomentando la concienciación sobre prevención.

Escribe un programa en Python que:

- Cree un archivo original con texto personalizado.
- A partir del txt cree un archivo cifrado en cesar.
- Opción de descifrado condicional.

**Advertencia Ética:** Este es un ejercicio simulado solo para fines educativos. Nunca uses código similar para dañar sistemas o datos reales. Ransomware es ilegal y causa daños graves; enfócate en aprender prevención



# Cómo detectar el Ransomware

**Herramientas de  
seguridad**

**Tráfico de red**

**Auditorías de  
seguridad**

**Educación y  
formación**

**Plan de respaldo y  
recuperación**

# Cómo detectar el Ransomware



Herramientas de  
seguridad

Tráfico de red

Auditorías de

Educación  
formal

Utilice software antimalware u otras herramientas de seguridad capaces de detectar y bloquear variantes conocidas de ransomware. Estas herramientas pueden usar firmas, heurística o algoritmos de aprendizaje automático para identificar y bloquear archivos o actividades sospechosas.



# Cómo detectar el Ransomware

**Herramientas de  
seguridad**

**Tráfico de red**

**Auditorías de  
seguridad**

Supervise el tráfico de la red y busque indicadores de compromiso, como patrones de tráfico de red inusuales o comunicación con servidores de comando y control conocidos.

# Cómo detectar el Ransomware

**Herramientas de  
seguridad**

Realice auditorías y evaluaciones de seguridad periódicas para identificar vulnerabilidades de la red y del sistema y garantizar que todos los controles de seguridad estén implementados y funcionen correctamente.

**Auditorías de  
seguridad**

**Respaldo y  
recuperación**

# Cómo detectar el Ransomware



**Herramientas de  
seguridad**

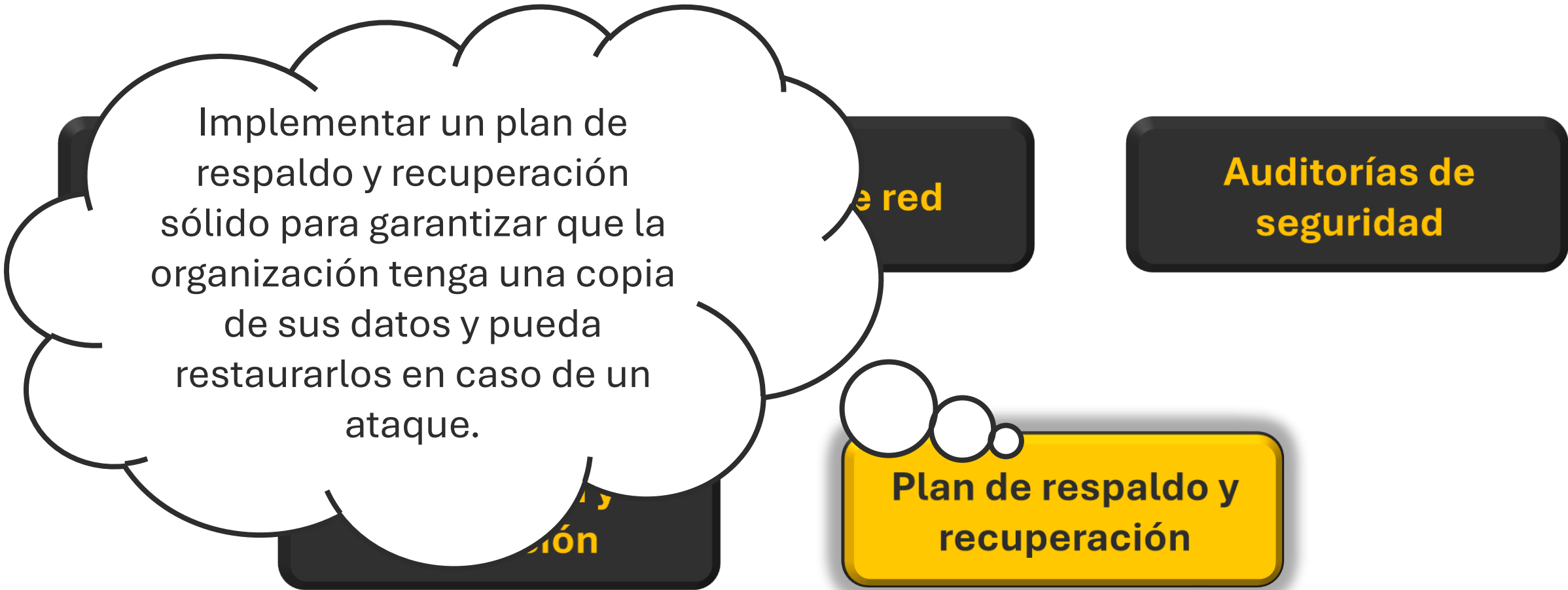
**Tr**

Educar y capacitar a los empleados sobre las mejores prácticas de ciberseguridad, incluida la identificación y el informe de correos electrónicos sospechosos u otras amenazas.

**Educación y  
formación**



# Cómo detectar el Ransomware



Implementar un plan de respaldo y recuperación sólido para garantizar que la organización tenga una copia de sus datos y pueda restaurarlos en caso de un ataque.

Seguridad de red

Auditorías de seguridad

Plan de respaldo y recuperación

Seguridad

# Cómo mitigar el Ransomware

**Educación a los  
empleados**

**Implementar  
contraseñas seguras**

**Habilitar la  
autenticación  
multifactor**

**Actualizar y parchar  
sistemas**

**copias de seguridad  
y recuperación**





# Ataques de ingeniería social

Técnicas que usan la manipulación psicológica para obtener información o acceso.

## Ejemplos comunes

### Phishing

Correo falso solicitando datos bancarios.

### Vishing

Llamadas telefónicas para engañar.

### Pretexting

Inventar escenarios falsos para obtener información.

# Cómo reconocer los ataques de Ingeniería Social?



Los estafadores intentan crear una sensación de urgencia utilizando expresiones como «lo antes posible», «de inmediato» o «ahora mismo».

**Tono urgente**

Solicitudes que requiera información confidencial, transferencia de fondos o descargas inusuales, aunque siga los canales de comunicación y estilos de conversación habituales.

**Peticiones extrañas**

Mensajes que empiezan con un tono informal, como «¿Tienes tiempo ahora mismo?» o «¿Puedes hacerme un favor?», aunque sean de alguien a quien conoces

**Familiaridad engañosa**

Los estafadores inventan excusas para evitar una comunicación continua y hacen que la víctima se muestre reacia a cuestionar o verificar sus peticiones.

**Evitar la comunicación continua**

# Ejemplos habituales de ataques



## Ataque de Ingeniería Social: Phishing Bancario

Un atacante envía un email falso que parece provenir de un banco conocido (e.g., "Banco XYZ").

- Asunto: "¡Urgente! Verifique su cuenta o será bloqueada".
- El email incluye un enlace a un sitio web fraudulento que imita la página del banco, solicitando usuario, contraseña y datos de tarjeta.
- El usuario, alarmado por la urgencia, ingresa sus credenciales sin verificar el dominio (e.g., "banco-xyz-login.com" en lugar de "bancoxyz.com").

### Consecuencias:

- Robo de credenciales: El atacante accede a la cuenta, realiza transacciones fraudulentas (e.g., transferencias de dinero).
- Pérdidas económicas: Víctimas pueden perder miles de dólares; en casos masivos (e.g., phishing global), daños superan los \$1 millón.
- Daño adicional: Exposición de datos personales, identidad robada, estrés emocional y pérdida de confianza en instituciones.





## Mitigación y Soluciones:

- **Mitigación:** Implementar filtros anti-phishing en correos (e.g., usando AI para detectar URLs falsas).
- **Soluciones:**
  - Educación: Capacitar usuarios para verificar remitentes y enlaces (e.g., hover sobre URL).
  - Tecnología: Usar autenticación multifactor (MFA) y VPN para cifrar conexiones.
  - Respuesta: Cambiar contraseñas inmediatamente y monitorear cuentas con herramientas como Have I Been Pwned.



# Ejemplo





# Ejercicio 1: Clasifica las amenazas

**Instrucción:** Lee cada situación y clasifícala como virus, gusano, troyano, spyware, ransomware o ingeniería social.

1. Descargas un programa gratuito para editar PDF y tu navegador empieza a mostrar anuncios excesivos.
2. Recibes un correo de tu banco pidiendo tus credenciales de acceso urgentemente.
3. Tus archivos están cifrados y aparece un mensaje exigiendo pago en bitcoin.
4. Recibes un archivo Word de un remitente desconocido y, al abrirlo, tu computador se vuelve más lento.
5. Un software se copia automáticamente en todos los equipos de la red sin permiso.





## Ejercicio 2: Reflexión grupal

¿Cuál de estas amenazas consideras más peligrosa y por qué? Relaciona tu respuesta con el modelo CIA.

1. Virus
2. Gusano
3. Troyano
4. Spyware
5. Ransomware
6. Ingeniería social.





## Ejercicio 3: Mini caso

### Situación:

Una empresa de salud sufre un ataque de ransomware que cifra todos los historiales médicos de pacientes, dejando el sistema inutilizable durante dos días.

### Preguntas:

- ¿Qué principios del modelo CIA se ven afectados?
- ¿Qué consecuencias éticas y legales puede tener para la empresa?

# Troyanos



Mas información: <https://www.youtube.com/watch?v=U-2LfJclafM>

# Troyanos





# Referencias

1. Bishop, M. (2003). *Computer Security*.
2. Briceño, E. (2021). *Seguridad De La Información*
3. Kremer, E. Et al. (2019). *Ciberseguridad*
4. Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*
5. Burdova, C. (2023, mayo 19). Pretexting: definición, ejemplos y cómo prevenirlo. Pretexting: definición, ejemplos y cómo prevenirlo; Avg. <https://www.avg.com/es/signal/what-is-pretexting>
6. Pasado, presente y futuro de la seguridad de la información. (s/f). Incibe.es. Recuperado el 12 de agosto de 2025, de <https://www.incibe.es/empresas/blog/pasado-presente-y-futuro-de-la-seguridad-de-la-informacion>
7. Petersen, B. (2023, septiembre 20). Las 8 etapas de un ataque de ransomware. Proofpoint. <https://www.proofpoint.com/es/blog/email-and-cloud-threats/eight-stages-of-the-ransomware-attack-chain>
8. Usa, I. T. G. (2024, abril 24). Zero-day exploits: What they are, and how to mitigate the risk. IT Governance USA Blog. <https://www.itgovernanceusa.com/blog/zero-day-exploits-what-they-are-and-how-to-mitigate-the-risk>

