

# Actividad – Caso real: Ataque de Ransomware en una clínica privada

Alejandro molina de haro

01/10/25

## Tabla de contenido

|  |   |
|--|---|
| 1.Identificación de activos .....            | 2 |
| 2.Identificación de amenazas.....            | 2 |
| 3.Identificación de vulnerabilidades .....   | 2 |
| 4.Valoración de impacto y probabilidad ..... | 3 |
| 5.Priorización de riesgos .....              | 3 |
| 6.Control de riesgos .....                   | 3 |
| 7. Plan de contingencia .....                | 3 |

# 1. Identificación de activos

Los activos más importantes de la clínica son:

- Los historiales médicos de los pacientes, con datos sensibles.
- El servidor central donde se almacena toda la información.
- El correo electrónico corporativo.
- La red interna, con 80 ordenadores conectados.
- El software de gestión de la clínica.
- El personal, tanto médico como administrativo y del departamento de TI.
- La reputación de la clínica, que también es un activo clave.

# 2. Identificación de amenazas

Las amenazas más relevantes en este caso son:

- Ransomware, que ya ha afectado a un servidor.
- Phishing, mediante correos falsos que engañan a los empleados.
- Pérdida de disponibilidad de los sistemas, que puede paralizar el trabajo.
- Posibles multas por incumplir la normativa de protección de datos (RGPD) si se filtran datos de pacientes.
- Daños en la reputación de la clínica.

# 3. Identificación de vulnerabilidades

Los factores que pudieron facilitar el ataque son:

- Falta de formación del personal en ciberseguridad.
- Ausencia de filtros adecuados en el correo electrónico corporativo.
- No disponer de copias de seguridad actualizadas o protegidas.
- Servidores y equipos sin todas las actualizaciones de seguridad.
- Falta de un plan de contingencia claro y probado.

## 4. Valoración de impacto y probabilidad

| Riesgo                         | Impacto | Probabilidad | Nivel   |
|--------------------------------|---------|--------------|---------|
| Ransomware en servidor central | Crítico | Alto         | Crítico |
| Phishing a empleados           | Alto    | Alto         | Alto    |
| Multa por RGPD                 | Alto    | Medio        | Alto    |
| Daño reputacional              | Alto    | Medio        | Alto    |

## 5. Priorización de riesgos

El riesgo más grave es el **ransomware en el servidor central**, porque:

- Deja sin acceso los historiales médicos.
- Puede paralizar por completo la clínica.
- Conlleva sanciones legales y pérdida de confianza de los pacientes.

## 6. Control de riesgos

- **Ransomware en el servidor central** → **Mitigar**: hacer copias de seguridad periódicas, segmentar la red, instalar sistemas de protección avanzados.
- **Phishing a empleados** → **Mitigar**: formar al personal, realizar simulacros de phishing y reforzar filtros de correo.
- **Multas** → **Mitigar/Transferir**: cumplir la normativa y contratar un seguro de ciberseguridad.
- **Daño reputacional** → **Mitigar/Aceptar**: mantener comunicación clara y transparente con pacientes y medios.

## 7. Plan de contingencia

- **Medidas inmediatas**: aislar los equipos infectados, desconectar el servidor afectado, avisar al responsable de seguridad informática y a las autoridades, iniciar la recuperación desde las copias de seguridad.
- **Comunicación**: informar al personal para que no abra correos sospechosos y dar un mensaje transparente a los pacientes, explicando la situación sin alarmar.
- **Recuperación de servicios**: restaurar los datos desde las copias de seguridad, revisar que los sistemas estén limpios y actualizados antes de volver a utilizarlos.
- **Lecciones aprendidas**: formar mejor a los empleados, reforzar la seguridad del correo y de los servidores, probar el plan de contingencia y mejorar los sistemas de detección y alerta.