Diploma Programme
Programme du diplôme
Programa del Diploma

# Informática
# Estudio de caso: Enfoque ético de la piratería informática

Para usar en mayo y noviembre de 2026

---

**Instrucciones para el alumnado**

- Para la prueba 3 de Nivel Superior se requiere el cuadernillo del estudio de caso.

5526 – 4412


8 páginas

## Escenario

*CyberHealth Security* es una empresa especializada en análisis de ciberseguridad. Un equipo de esta empresa ha sido contratado recientemente para revisar los sistemas de ciberseguridad del *Hospital MedTechPro* (*MTPH*). El hospital depende en gran medida de la tecnología, concretamente de las historias clínicas electrónicas (HCE), las comunicaciones internas y los dispositivos médicos que utilizan Internet de las Cosas (IoT, por sus siglas en inglés).

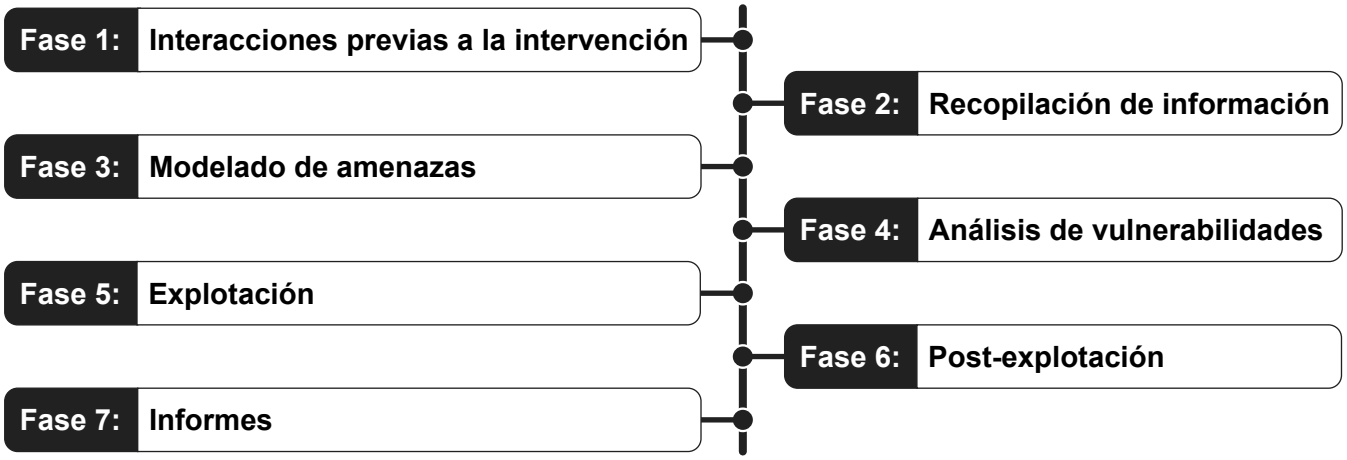
## Problemas por resolver

La tarea del equipo de *CyberHealth Security* consiste en realizar *pruebas de penetración* en profundidad para descubrir cualquier vulnerabilidad en la red del hospital. Tendrán que navegar por la red de *MTPH*, evaluando la seguridad del sistema y la privacidad de los datos de los pacientes en todos los departamentos. Para ello, utilizarán la norma de ejecución de pruebas de penetración (PTES, por sus siglas en inglés).

## La norma de ejecución de pruebas de penetración

PTES es un marco completo para realizar pruebas de penetración. Está diseñado para proporcionar un enfoque estructurado de realización de pruebas y notificación de resultados. El proceso PTES consta de siete fases (véase la **figura 1**).

**Figura 1: Las siete fases del proceso PTES**




1. **Interacciones previas a la intervención**. El proceso comienza con la preparación, la obtención de la aprobación de los documentos y el montaje de las herramientas necesarias.
2. **Recopilación de información**. Los datos se recogen de fuentes externas, como las redes sociales y los registros oficiales, y luego se analizan, lo que se clasifica como *inteligencia de fuente abierta* (*OSINT*, por sus siglas en inglés).
3. **Modelado de amenazas**. Se identifican las amenazas y vulnerabilidades potenciales y se desarrollan estrategias para mitigarlas.
4. **Análisis de vulnerabilidades**. Se identifican y confirman las vulnerabilidades que podrían ser explotadas por un *pirata informático*.
5. **Explotación.** Se intenta violar el sistema utilizando las vulnerabilidades previamente identificadas y confirmadas.
6. **Post-explotación**. Si se consigue el acceso, el objetivo pasa a ser mantener el control del sistema y extraer datos de él.
7. **Informes**. Todo el proceso de prueba se documenta y los resultados se presentan en un informe al cliente.

## Fase 1: Interacciones previas a la intervención

En esta fase, el equipo de *CyberHealth Security* colaborará con *MTPH* para definir los objetivos de la prueba de penetración, el alcance, las normas de intervención, los enfoques logísticos y de *pruebas*, y el calendario general. Este proceso de colaboración es crucial para garantizar que las pruebas se ajusten a los requisitos operativos y las preocupaciones de seguridad del hospital, respetando al mismo tiempo las normas éticas profesionales, sobre todo teniendo en cuenta la naturaleza sensible de los datos sanitarios.

**Fijación de objetivos e identificación de metas**

- Se establecerán objetivos claros para la prueba tras identificar las principales preocupaciones de *MTPH*. Estas preocupaciones clave pueden incluir la integridad de los datos de los pacientes, la prestación ininterrumpida de servicios y el cumplimiento de la normativa del sector sanitario.
- Se identificarán objetivos específicos dentro de la red del hospital. Se determinará cualquier área de alto riesgo que requiera una atención especial, como las bases de datos de registros de pacientes o los dispositivos médicos habilitados para IoT.

**Definir el alcance y las normas de intervención**

- Los límites de la prueba se confirmarán para evitar cualquier interrupción inesperada de las operaciones críticas del hospital. Esto incluye los sistemas que se van a probar y los límites de las pruebas.
- Se acordarán las normas de intervención para garantizar que tanto el equipo de *CyberHealth Security* como los administradores de *MTPH* comprendan los métodos y el alcance de las actividades de las pruebas de penetración.

**Enfoques de las pruebas**

El equipo de *CyberHealth Security* tendrá que considerar las implicaciones de tres enfoques diferentes de las pruebas, *pruebas de caja negra*, *pruebas de caja blanca* y *pruebas de caja gris*, y evaluar los riesgos y beneficios potenciales de cada uno en un entorno sanitario.

- **Pruebas de caja negra**. En este enfoque, el equipo simularía un ataque desde la perspectiva de un pirata informático externo sin información y consideraría las vulnerabilidades inmediatamente aparentes.
- **Pruebas de caja blanca**. En este enfoque, el equipo realizaría un análisis en profundidad con pleno conocimiento de la infraestructura informática del hospital. Este enfoque requeriría acceso a diagramas de red, configuraciones de sistemas y vulnerabilidades conocidas.
- **Pruebas de caja gris**. Es una mezcla de pruebas de caja negra y pruebas de caja blanca. Este enfoque supondría un conocimiento parcial de los sistemas del hospital, simulando una amenaza interna o un pirata informático externo con información interna parcial.

**Véase al dorso**

## Fase 2: Recopilación de información

Esta fase consiste en recopilar toda la información pública disponible sobre *MTPH* para identificar posibles vulnerabilidades. El equipo de *CyberHealth Security* empleará diversas técnicas de inteligencia de fuente abierta (OSINT), utilizando herramientas y fuentes como motores de búsqueda, redes sociales, foros y otros recursos de Internet para recopilar datos procesables sobre la huella digital del hospital. Esta información ayudará al equipo a crear un mapa de la presencia externa del hospital y se utilizará para encontrar puntos débiles que puedan ser explotados.

Entre los ejemplos de información que el equipo podría recopilar utilizando técnicas OSINT se incluyen:

- **Datos del personal**. Información obtenida mediante el análisis de la presencia en redes sociales del personal, en particular el que desempeña funciones informáticas y administrativas.
- **Uso de la tecnología**. Información sobre las soluciones de software y hardware del hospital procedente de fuentes públicas.
- **Políticas de seguridad**. Examen de las políticas y procedimientos de seguridad del hospital a disposición del público.

El equipo de *CyberHealth Security* también tiene la intención de emplear otras técnicas de reconocimiento para obtener un conocimiento más profundo de la red de *MTPH*:

- **Recopilación de información específica**. El equipo utilizará técnicas de búsqueda avanzadas, como el *hacking de motores de búsqueda*, para encontrar archivos sensibles expuestos o portales de acceso.
- ***Análisis de redes* y *cartografía de redes***. El equipo empleará herramientas avanzadas de mapeo de redes para identificar *topologías de red*, incluidos servidores internos y externos, cortafuegos y otros dispositivos de red. Algunas de las principales actividades de cartografía y análisis de redes son el *análisis de puertos*, la *detección de sistemas operativos* y la cartografía de la topología de la red. Durante el análisis y la cartografía de la red, se catalogarán las *direcciones IP* de todos los dispositivos de la red del hospital para conocer a fondo el alcance de la red.
- **Reconocimiento de ingeniería social**. El equipo utilizará *vishing (phishing de voz)* o *pretextos engañosos* para recabar información de los empleados que podría ayudar en la prueba de penetración.

La fase de recopilación de información ayuda al equipo a realizar una *evaluación de la postura de seguridad* del hospital desde una perspectiva externa, proporcionando información sobre cómo abordar las pruebas de penetración.

## Fase 3: Modelado de amenazas

En esta fase, el equipo de *CyberHealth Security* llevará a cabo un análisis detallado de las amenazas para la ciberseguridad de *MTPH*. El proceso implica:

1. **Identificación de adversarios potenciales**. El equipo determinará quién podría atacar el hospital, como ciberdelincuentes en busca de datos valiosos de los pacientes o personas con acceso a la red.
2. **Evaluación de las capacidades e intenciones de los piratas informáticos**. El equipo analizará de qué son capaces estos adversarios potenciales y cómo podrían pretender utilizar los datos o sistemas a los que han accedido.
3. **Métodos de explotación**. El equipo documentará el modo en que estos adversarios podrían explotar las vulnerabilidades, teniendo en cuenta tácticas como el despliegue de *malware*, los *ataques de ingeniería social* y los ataques a la red.
4. **Evaluación de activos valiosos**. El equipo determinará qué activos son los más críticos para el hospital, como las HCE, y evaluará el impacto potencial de su puesta en peligro.
5. **Priorización de los esfuerzos de seguridad**. El equipo utilizará este análisis para orientar el enfoque de las pruebas de penetración, garantizando que las áreas más valiosas y vulnerables reciban la máxima atención.

Este enfoque estructurado permitirá al equipo adaptar eficazmente sus estrategias de pruebas de penetración, alineándolas con el panorama de amenazas único del hospital.

## Fase 4: Análisis de vulnerabilidades

En esta fase, el equipo de *CyberHealth Security* empleará herramientas automatizadas y técnicas manuales para realizar un análisis exhaustivo de la vulnerabilidad de la red de *MTPH*. Este proceso implica:

1. **Búsqueda de vulnerabilidades**. El equipo utilizará herramientas automatizadas para identificar rápidamente vulnerabilidades conocidas en toda la red, como software sin parches o configuraciones inseguras.
2. **Examen manual**. El equipo combinará exploraciones automatizadas con comprobaciones manuales para detectar fallas de seguridad más sutiles o vulnerabilidades complejas que requieren el análisis de expertos.
3. **Evaluación de los puntos débiles**. El equipo evaluará las vulnerabilidades identificadas para comprender su impacto potencial y cómo podrían ser explotadas por los piratas informáticos.
4. **Establecer prioridades**. El equipo determinará qué vulnerabilidades son las más críticas en función de factores como la facilidad de explotación y el daño potencial para las operaciones del hospital y la seguridad de los pacientes.

El resultado de este análisis será crucial para guiar los pasos posteriores de las pruebas de penetración, lo que permitirá al equipo centrar sus esfuerzos en las brechas de seguridad más significativas.

**Véase al dorso**

## Fase 5: Explotación

Cuando se identifiquen las vulnerabilidades en la red de *MTPH*, el equipo de *CyberHealth Security* iniciará la fase de explotación. Esta etapa crucial implica las siguientes consideraciones:

- **Intentos de violación selectiva**. El equipo utilizará técnicas específicas para explotar las vulnerabilidades identificadas, poniendo a prueba las defensas del hospital.
- ***Desarrollo de comandos para explotación***. El equipo elaborará secuencias de comandos o herramientas personalizadas adaptadas a las vulnerabilidades específicas detectadas en la red del hospital.
- **Empleo de diversas técnicas**. En función de las vulnerabilidades, el equipo utilizará algunas o todas las técnicas posibles, como *inyección de SQL*, *secuencias de comandos en sitios cruzados* (*X-SS*), *ataques de desbordamiento de búfer* y *herramientas de descifrado de contraseñas*.
- **Evaluación del impacto**. El equipo tratará de comprender el daño potencial o el acceso que podría lograrse mediante una explotación exitosa, lo que es vital para evaluar la resistencia de la seguridad del hospital.

Esta fase es crucial para demostrar cómo los piratas informáticos reales podrían explotar los puntos débiles y ayudará al equipo a formular estrategias defensivas.

## Fase 6: Post-explotación

En esta fase, el equipo de *CyberHealth Security* evaluará las consecuencias de las vulnerabilidades explotadas en la red de *MTPH*. Las actividades clave incluyen:

- **Acceso a los datos y análisis**. El equipo investigará los tipos de datos sensibles accesibles tras la violación, como historiales de pacientes, datos administrativos o información confidencial.
- **Escalada de privilegios**. El equipo examinará hasta qué punto se puede aumentar el acceso dentro de la red al mejorar el nivel de los privilegios de los usuarios.
- **Establecer la persistencia**. El equipo evaluará los métodos por los que los piratas informáticos podrían mantener el acceso a la red a largo plazo, lo que es fundamental para comprender la gravedad de una brecha.
- **Evaluación del impacto operativo**. El equipo evaluará las posibles repercusiones de la violación en los servicios hospitalarios y la seguridad de los pacientes.
- ***Análisis forense de sistemas* y de malware**. El equipo analizará cualquier rastro dejado por el proceso de explotación examinando los registros del sistema, detectando implantes de malware o identificando cualquier cambio realizado en las configuraciones del sistema.

Esta fase ayudará al equipo a comprender todo el alcance y la escala de un posible ciberataque contra el hospital.

## Fase 7: Informes

En esta fase final, el equipo de *CyberHealth Security* elaborará un informe exhaustivo de las pruebas de penetración realizadas en *MTPH*. Los componentes clave de este informe incluyen:

- **Detalles de vulnerabilidades y explotación**. En ellos se ofrecerá una visión general de las vulnerabilidades descubiertas, los métodos utilizados para su explotación y el impacto potencial de cada una de ellas.
- **Recomendaciones prácticas**. Se darán sugerencias y se priorizará la mitigación de los riesgos de seguridad identificados, lo que permitirá al hospital reforzar sus defensas.
- ***Evaluación de la postura de seguridad***. Esto proporcionará un análisis holístico de los puntos fuertes y débiles de la ciberseguridad general del hospital, con información sobre áreas de mejora y enfoque futuro.

Este informe permitirá al equipo informático de *MTPH* desarrollar un *plan de respuesta* que incluya la detección de incidentes, estrategias de respuesta y procesos de recuperación. Esto guiará los esfuerzos del hospital para mejorar sus medidas de ciberseguridad, responder a las amenazas y protegerse contra amenazas futuras.

## Consideraciones éticas

Antes de llevar a cabo cualquier forma de prueba de penetración, es esencial abordar las consideraciones éticas, especialmente en un entorno sanitario como *MTPH*. Esto incluye:

- Autorización adecuada
- Confidencialidad e integridad de los datos
- No interrupción de los servicios
- Generación de informes y capacidad de respuesta

Este énfasis en las consideraciones éticas subraya la responsabilidad de los profesionales de la ciberseguridad para equilibrar las pruebas exhaustivas con el bienestar de la institución y sus partes interesadas.

## Desafíos

Para garantizar la seguridad del marco de ciberseguridad de *MTPH*, el equipo de *CyberHealth Security* se enfrentará a los siguientes desafíos:

- Evaluación de enfoques de pruebas de penetración de caja negra, caja blanca y caja gris
- Explicar cómo el hospital puede mantener la continuidad operativa y proteger los datos confidenciales de los pacientes mientras realiza pruebas de vulnerabilidad
- Investigar cómo se pueden utilizar el análisis de redes, la cartografía de redes y las herramientas OSINT para descubrir dispositivos activos e información sobre la red de *MTPH*
- Desarrollar un plan de respuesta que incluya la detección de incidentes, estrategias de respuesta y procesos de recuperación
- Debatir las implicaciones éticas de la realización de pruebas de penetración en *MTPH*

**No se espera que los alumnos/as investiguen el funcionamiento del equipamiento médico o revisen el cumplimiento de la legislación.**

**Véase al dorso**

## Terminología adicional

Análisis de puertos (*port scanning*)
Análisis de redes (*network scanning*)
Análisis forense de sistemas (*system forensics*)
Ataques de desbordamiento del búfer (*buffer overflow attacks*)
Ataques de ingeniería social (*social engineering attacks*)
Cartografía de red (*network mapping*)
Desarrollo de comandos para explotación (*exploit development*)
Detección de sistemas operativos (*OS detection*)
Dirección IP (*IP address*)
Evaluación de la postura de seguridad (*security posture assessment*)
Hacking de motor de búsqueda (*search engine dorking*)
Herramienta de descrifrado de contraseñas (*password cracking tool*)
Inteligencia de fuente abierta (OSINT, *open-source intelligence*)
Inyección de SQL (*SQL injection*)
Malware (*malware*)
Pirata informático (*hacker*)
Plan de respuesta (*response plan*)
Pretextos engañosos (*pretexting*)
Pruebas (*testing*)
    Caja blanca (*white box*)
    Caja gris (*grey box*)
    Caja negra (*black box*)
Pruebas de penetración (*penetration testing*)
Secuencias de comandos en sitios cruzados (X-SS, *cross-site scripting*)
Topología de red (*network topology*)
Vishing (phishing de voz) (*voice phishing*)

**Algunas empresas, productos o personas nombradas en este estudio de caso son ficticios y cualquier semejanza con entidades reales es solamente una coincidencia.**