# 1.1-INVESTIGACIÓN 1: LEYES

Hecho por: Izan Navarro

# ÍNDICE

**INTRODUCCIÓN AL HACKING ÉTICO**

**1. Responde a estas preguntas en un documento:**

• ¿Qué consecuencias legales tendría un acceso sin autorización a un sistema en España?

Partimos de 2 Artículos importantes:

· **Artículo 197:** Castiga con penas de prisión de seis meses a dos años al que, sin autorización, acceda o mantenga el acceso a todo o parte de un sistema de información.

· **Artículo 264:** Si además se manipulan o dañan datos, programas o sistemas, la pena puede elevarse a entre seis meses y tres años.

• ¿Qué obligaciones tiene una empresa si sufre una fuga de datos personales bajo el RGPD?

Si una empresa sufre una fuga de datos, el Reglamento General de Protección de Datos dictamina que se obliga a:

· **Notificar a la autoridad competente** (AEPD en España) en un plazo de 72 horas

· **Notificar a los afectados** (usuarios o clientes) si puede implicar un riesgo para sus derechos y libertades
· **Registrar y documentar** la fuga y sus incidentes de seguridad

• ¿Qué diferencia hay entre un test de intrusión autorizado y uno no autorizado?

Test de Intrusión **Autorizado**: Este Test se realiza con permiso formal de propietario del Sistema cuyo objetivo es el de evaluar la seguridad del sistema de forma ética y respaldada como una actividad legítima pactada mediante contrato

Test de Intrusión **NO Autorizado**: Este Test se realiza SIN permiso formal y por lo tanto es Ilegal, cuya finalidad es la de sustraer información. Este está constituido como delito informático

**2. Ejercicio práctico: redacta un mini-contrato de autorización de pentesting (máx. media página) que incluya:**

• Alcance del test (ejemplo: los equipos de red, servidores, web, aplicación).

• Limitaciones (ejemplo: no atacar la red interna, no usar herramientas de fuerza bruta).

• Responsabilidades (ejemplo: el pentester informará de los hallazgos, ANTES DE EXPLOTARLOS).

## AUTORIZACIÓN DE PRUEBAS DE INTRUSIÓN (PENTEST)

Entre Indra S.A. e Izan Navarro Luján se acuerda lo siguiente para la realización de pruebas de seguridad:

**¿Qué se prueba (alcance)?**
Probamos únicamente los activos listados por Indra S.A: equipos de red (firewalls, routers, switches), servidores indicados, y las aplicaciones web y API ‘s cuyas URL’s/dominios se han facilitado. Todo lo que no esté en esa lista **queda fuera**.

**Lo que NO se puede hacer (limitaciones)**

- No atacar redes o equipos que no estén en el alcance (p. ej. la red interna de oficinas).
- No usar fuerza bruta masiva sobre cuentas reales en producción.
- No borrar ni manipular datos de forma irreversible sin permiso escrito previo.

**Responsabilidades del pentester (qué haré yo):**

- Avisar **de inmediato** al contacto técnico de Indra S.A. si encuentro algo crítico.
- Documentar todos los hallazgos en un informe técnico y un resumen ejecutivo.
- No explotar vulnerabilidades más allá de pruebas no destructivas sin autorización escrita previa.
- Mantener la confidencialidad de la información a la que acceda.

**Responsabilidades de Indra S.A (qué tienen que facilitar):**

- Proveer la lista de activos, accesos necesarios y una persona de contacto.
- Autorizar por escrito cualquier cambio en el alcance o en las técnicas a emplear.

**Fechas y firmas:**
Período de pruebas: desde **7/10/2025** hasta **08/10/2025.**
Firmado por: _____ (Indra S.A) Fecha: **//**____
Firmado por: _____ (Izan Navarro Lujan) Fecha: **//**____

## 3. BIBLIOGRAFÍA

https://www.dexiaabogados.com/blog/delitos-informaticos/#:~:text=Da%C3%B1o%20inform%C3%A1tico,inform%C3%A1ticos%20o%20documentos%20electr%C3%B3nicos%20ajenos.