# Trabajo Práctico - Opción 1

## Sistema de Login Seguro

### Objetivos

Diseñar y **(opcional)** implementar un sistema de autenticación web seguro para una aplicación web mínima, integrando:

- Hashing seguro de contraseñas.
- Gestión de sesiones segura con **cookies** (HttpOnly, Secure, SameSite) **o** tokens JWT con rotación de refresh y revocación.
- Controles preventivos de seguridad.

### Entregables

1. Informe PDF (A4, Arial tamaño 12, hasta 12 páginas) con: requisitos, arquitectura, modelo de datos, flujos, decisiones.
2. *Opcional extra*: Código en un repositorio con README, scripts y evidencias (tests, capturas). Documentación relacionada.

### Criterios de evaluación

- Se evaluará el diseño del sistema, los controles aplicados y los criterios utilizados en cada caso.
- Opcional: modelado de amenazas e implementación de la solución.

### Requisitos del informe

1. Requisitos funcionales y no funcionales.
2. Modelo de datos.
3. Flujos: registro, login, logout, refresh/rotación, cambio de contraseña.
4. Decisiones relacionadas con cripto.
5. Gestión de sesiones.
6. Privacidad: minimización de datos, retención y borrado.

# Trabajo Práctico - Opción 2

## Autoridad certificante

### Objetivos

Diseñar y **(opcional)** implementar una estructura de una PKI (Root CA, CA intermedia, RA) integrando:

- Diseño de una política de certificación (CP/CPS) y validación de la identidad de los solicitantes.
- Mecanismos de prueba de posesión de clave pública (key ownership).
- Emisión, revocación y validación de certificados digitales X.509.
- Integración de la PKI en un escenario de autenticación TLS/mTLS.

### Entregables

1. Informe PDF con: requisitos, arquitectura, modelo de datos, flujos, decisiones.
2. *Opcional extra*: Código en un repositorio con README, scripts y evidencias (tests, capturas). Documentación relacionada.

### Criterios de evaluación

- Se evaluará el diseño del sistema, los controles aplicados y los criterios utilizados en cada caso.
- Opcional: modelado de amenazas e implementación de la solución.

### Requisitos del informe

1. Requisitos funcionales y no funcionales.
2. Diseño de la infraestructura y decisiones asociadas.
3. Política de certificación (CP/CPS) y flujo de validación de la identidad de los solicitantes.
4. Mecanismos de prueba de posesión de clave pública (key ownership).
5. Flujos: emisión, revocación y validación de certificados digitales X.509.
6. Flujo detallado de integración de la PKI en un escenario de autenticación TLS/mTLS.