PRÁCTICA 2025 (PROVISIONAL)

SEGURIDAD EN EL DISEÑO DEL SOFTWARE

CONDICIONES GENERALES

- El desarrollo se realizará en Go a partir de la base de código proporcionada.
- Se realizará en grupo (salvo excepciones consensuadas).
- Se evitarán interfaces de usuario complejas, utilizando esencialmente el terminal y concentrando el esfuerzo en el problema y la seguridad.
- Respecto a la evaluación, habrá dos revisiones (una a mitad de cuatrimestre y otra al final) además de la entrega final.
- Se publicará una guía sobre los elementos de documentación a entregar más adelante.

SISTEMA DE VOTACIÓN ELECTRÓNICA

El objetivo consistirá en la creación de un sistema de votación electrónica, que permita la gestión de las diferentes propuestas a votar, la votación secreta en sí, así como la comunicación e interacción entre distintos usuarios de forma asíncrona y segura.

Las características que se deben incluir en el diseño para aprobar son:

- Arquitectura cliente/servidor, realizándose ambos en Go a partir del código proporcionado.
- Mecanismo de autentificación seguro (gestión de contraseñas, identidades y sesión).
- Transporte de red seguro entre cliente y servidor (HTTPS).
- Almacenamiento seguro (cifrado en descanso) en el servidor.
- Sistema de gestión y votación secreta de propuestas.
- Sistema de comunicación privado (cifrado) entre usuarios.

Algunos desafíos adicionales (aspectos extra u opcionales para subir nota) podrían ser, entre otros:

- Cifrado punto a punto (el servidor no conoce las claves ni la información, todo el cifrado/descifrado se realiza en el cliente de forma local).
- Gestión de categorías de propuestas o grupos de usuarios (incluyendo seguridad adicional).
- Gestión de diferentes roles de usuarios (administradores, moderadores, etc.).
- Incorporación de clave pública en la autentificación de usuarios.
- Incorporación de firma digital para garantizar el origen de los datos.
- Sistema de registro de eventos *(logging)*, para mejorar la trazabilidad (remoto).
- Sistema de copia de seguridad *(backup)*, para recuperarse ante incidentes (remoto).
- Otros relacionadas con la seguridad y privacidad a consensuar con el profesorado.