**Trabajo Practico Nro. 3**

**Sistema Bancario Seguro**

**Objetivo**

Desarrollar una aplicación web segura utilizando Spring Boot y Spring Security para un sistema bancario básico. La aplicación debe incluir endpoints protegidos y públicos, gestionar autenticación y autorización basada en roles y permisos, y simular usuarios con diferentes niveles de acceso.

**Contexto**

Una entidad bancaria necesita una API REST para gestionar operaciones básicas. Los empleados del banco tendrán diferentes roles y permisos según sus funciones:

* **Administradores**: Pueden realizar todas las operaciones (consultar saldos, realizar transferencias, crear cuentas).
* **Cajeros**: Solo pueden consultar saldos y realizar transferencias.
* **Clientes**: Solo pueden consultar su propio saldo.

**Requerimientos**

1. **Endpoints**:
   * /api/public/info: Endpoint público que devuelve un mensaje de bienvenida (sin autenticación).
   * /api/secure/saldo: Endpoint protegido que devuelve un mensaje simulando la consulta de saldo (requiere permiso "READ").
   * /api/secure/transferencia: Endpoint protegido que simula una transferencia (requiere permiso "WRITE").
2. **Seguridad**:
   * Configurar Spring Security con autenticación HTTP Basic.
   * Usar una política de sesiones sin estado (stateless).
   * Deshabilitar CSRF (ya que es una API REST).
   * Definir al menos tres usuarios en memoria con roles y permisos:
     + admin (contraseña: "admin123", rol: "ADMIN", permisos: "READ", "WRITE").
     + cajero (contraseña: "cajero123", rol: "CAJERO", permisos: "READ", "WRITE").
     + cliente (contraseña: "cliente123", rol: "CLIENTE", permiso: "READ").