Instituto Politécnico Nacional

Escuela Superior de Cómputo

Programa académico / Plan de estudios
Ingeniería en Sistemas Computacionales / 2020

Unidad de aprendizaje
Desarrollo de aplicaciones móviles nativas

Práctica 2: Aplicación móvil básica para operaciones CRUD con un servicio REST

Objetivo: Desarrollar una aplicación móvil nativa en Android que permita realizar operaciones CRUD (Crear, Leer, Actualizar, Borrar) sobre un servicio REST, implementando un sistema de autenticación con roles (Administrador y Usuario), con contraseñas encriptadas y sesiones seguras. El Administrador tendrá permisos completos para gestionar el sistema, mientras que el Usuario podrá visualizar y modificar su perfil.

Ejercicio 1: Configuración inicial y diseño de la aplicación

1. **Diseño del Menú de Navegación:**
   - Implementar un menú de navegación (DrawerLayout, BottomNavigationView o similar) que permita acceder a:
     - **Inicio de Sesión**
     - **Registro de Usuario**
     - **Operaciones CRUD (Administrador)**
     - **Perfil (Usuario)**
2. **Interfaz de Usuario:**
   - Diseñar una interfaz atractiva y responsiva utilizando los componentes nativos de Android.
   - Implementar XML layouts bien estructurados.
   - Aplicar temas y estilos coherentes para mantener una apariencia consistente.
   - Utilizar diferentes métodos de diseño:
     - **Asistente**: Usar el asistente de Android Studio para generar componentes base.
     - **XML**: Configurar y personalizar componentes en XML.
     - **Código**: Añadir comportamientos mediante Kotlin/Java.

Ejercicio 2: Implementación del servicio REST para operaciones CRUD y roles

1. **Operaciones CRUD:**
   - Desarrollar un servicio REST que permita:
     - **POST:** Crear un nuevo registro.
     - **GET:** Leer uno o varios registros.
     - **PUT:** Actualizar un registro existente.
     - **DELETE:** Borrar un registro.
   - Publicar el servicio en un repositorio público de GitHub.
2. **Autenticación de Usuarios:**
   - Implementar un sistema de autenticación con:
     - Registro de usuarios con contraseñas encriptadas.
     - Inicio de sesión para usuarios existentes.
   - Roles:
     - **Administrador:** Acceso completo a operaciones CRUD sobre cualquier registro.

        - **Usuario:** Visualización y actualización de su perfil, sin acceso a datos de otros usuarios.
3. **Sesiones Seguras:**
    - Implementar manejo de sesiones seguras para usuarios autenticados.
    - Proteger contra vulnerabilidades como robo de sesión.

Ejercicio 3: Implementación del sistema en la aplicación móvil nativa

1. **Registro de Usuario y Login:**
    - Desarrollar Activities o Fragments para inicio de sesión y registro.
    - Conectar con el servicio REST para autenticación.
    - Implementar encriptación para las contraseñas enviadas.
2. **Conexión a la API REST:**
    - Utilizar Retrofit u otra biblioteca para realizar solicitudes HTTP.
    - Implementar modelos de datos utilizando las clases nativas de Android.
3. **Gestión de Fotos de Perfil:**
    - **Usuario**: Permitir subir y modificar su foto de perfil desde su cuenta.
    - **Administrador**: Capacidad de ver y modificar las fotos de perfil de todos los usuarios.
4. **Implementación de Roles:**
    - **Administrador**: Menú de administración con operaciones CRUD completas.
    - **Usuario**: Menú de perfil para visualizar y actualizar su información.
5. **Estructura y Organización:**
    - Organizar el proyecto siguiendo las convenciones de Android:
        - Activities y Fragments para la interfaz de usuario.
        - Uso de Intents para la navegación entre pantallas.
        - Implementar Fragmentos para interfaces modulares y flexibles.
        - Estructura clara de paquetes (models, views, controllers, adapters, etc).
6. **Pruebas en Emulador o Dispositivo Físico:**
    - Verificar el funcionamiento correcto de todas las funcionalidades.
    - Probar los diferentes roles y permisos.

Entrega de la Práctica:

1. **Código fuente:**
    - Repositorio GitHub con el código de la aplicación móvil y del servicio REST.
    - Asegurar que los endpoints y sesiones sean seguros, y las contraseñas estén encriptadas.
2. **Informe de la práctica:** Siguiendo esta estructura:
    - **Portada:** Nombre completo, número de boleta, asignatura, profesor y fecha.
    - **Introducción:** Explicación general del código y lógica utilizada.
    - **Desarrollo:** Código fuente con pruebas de funcionamiento (capturas de pantalla).
    - **Conclusiones:** Resumen de retos y logros.
    - **Bibliografía:** Fuentes consultadas en formato APA.

Formato:

- **Tipo de letra:** Arial
- **Tamaño:** 12
- **Espaciado:** 1.5
- **Márgenes:** Estándar

Fecha de Entrega: La fecha límite para la entrega de esta práctica es el lunes 17 de marzo de 2025. No se aceptarán entregas fuera de tiempo y forma.