



Actividad [#3] - [Codificación de la Aplicación]

[Desarrollo de Aplicaciones Biométricas]

Ingeniería en Desarrollo de Software

Tutor: Marco Alonso Rodríguez Tapia

Alumno: Alan David López Rojas

Fecha: 14/09/2023

Índice

Introducción.....	pág. 3
Descripción.....	pág. 4
Justificación.....	pág. 5
Etapa 1:	
Diseño de interfaces.....	pág. 6
Etapa 2:	
Codificación.....	pág. 8
Ejecución en el teléfono.....	pág. 13
Enlace del proyecto.....	pág. 16
Desarrollo.....	pág. 17
Conclusión.....	pág. 25
Bibliografía.....	pág. 26

Introducción

En esta actividad, se abordará la codificación de la aplicación de Android diseñada durante las 2 primeras actividades, para brindar una experiencia de inicio de sesión mediante el uso de la autenticación de huellas dactilares previamente registradas en el teléfono. Esta aplicación constará de dos pantallas principales: la pantalla de inicio de sesión y la pantalla de bienvenida. Su principal funcionalidad radica en la autenticación a través de huellas dactilares y la transición entre estas dos pantallas.

El objetivo principal de esta aplicación es proporcionar una forma segura y conveniente de autenticación para los usuarios. La autenticación biométrica, en particular el escaneo de huellas dactilares, es ampliamente reconocida por su nivel de seguridad y comodidad, lo que la convierte en una opción ideal para muchas aplicaciones que requieren autenticación.

La pantalla de inicio de sesión se utilizará para recopilar la entrada del usuario en forma de escaneo de huellas dactilares. Aquí, implementaremos lógica para manejar diferentes escenarios: cuando se ingresa una huella que no está registrada, se mostrará un mensaje de error indicando que el escaneo falló. En caso de una huella dactilar registrada y autenticación exitosa, se mostrará un mensaje de bienvenida y se llevará al usuario a la pantalla de bienvenida.

La pantalla de bienvenida ofrecerá una transición suave desde la pantalla de inicio de sesión y permitirá al usuario regresar a la pantalla de inicio de sesión si lo desea. Esto proporcionará una experiencia de usuario intuitiva y fluida.

Descripción

El contexto presentado en la actividad gira en torno al desarrollo de una aplicación móvil que se enfoca en proporcionar una experiencia segura y conveniente de inicio de sesión utilizando la autenticación de huellas dactilares. Esta es una respuesta directa a la creciente necesidad de aplicaciones seguras que protejan la información personal de los usuarios sin comprometer la comodidad.

La autenticación biométrica, como el escaneo de huellas dactilares, se ha convertido en un estándar en la industria de la tecnología debido a su nivel de seguridad y facilidad de uso. Esta aplicación se alinea con esa tendencia, lo que la hace relevante y valiosa para los usuarios modernos que desean una forma más segura y rápida de acceder a sus aplicaciones.

El primer componente de la aplicación es la pantalla de inicio de sesión, que actúa como un punto de entrada. La capacidad de gestionar escenarios de autenticación exitosa y fallida es fundamental para proporcionar una experiencia de usuario sólida. Cuando una huella no registrada se presenta, el mensaje de error brinda claridad y transparencia al usuario sobre el motivo del fallo.

La pantalla de bienvenida, por otro lado, permite al usuario avanzar en el flujo de la aplicación después de una autenticación exitosa. Además, la opción de regresar a la pantalla de inicio de sesión demuestra la preocupación por la comodidad del usuario y brinda flexibilidad.

Justificación

La implementación de la autenticación de huellas dactilares en la actividad propuesta es una elección justificada y ventajosa por varias razones:

Primero, en términos de seguridad, la autenticación de huellas dactilares es altamente confiable. Cada huella digital es única, lo que hace que sea casi imposible de falsificar o duplicar. Esta característica brinda una capa adicional de protección contra el acceso no autorizado a la aplicación, lo que es crítico si se maneja información sensible o privada.

Además, la autenticación con huellas dactilares mejora significativamente la experiencia del usuario. Elimina la necesidad de recordar contraseñas complicadas y largas, lo que a menudo puede resultar frustrante para los usuarios. En cambio, pueden acceder a sus cuentas de manera rápida y sencilla, lo que mejora su satisfacción general.

En términos de eficiencia, escanear una huella digital es un proceso rápido y simplificado, lo que agiliza el acceso a la aplicación. Esto es particularmente beneficioso cuando los usuarios desean acceder rápidamente a la información o realizar tareas sin demoras innecesarias.

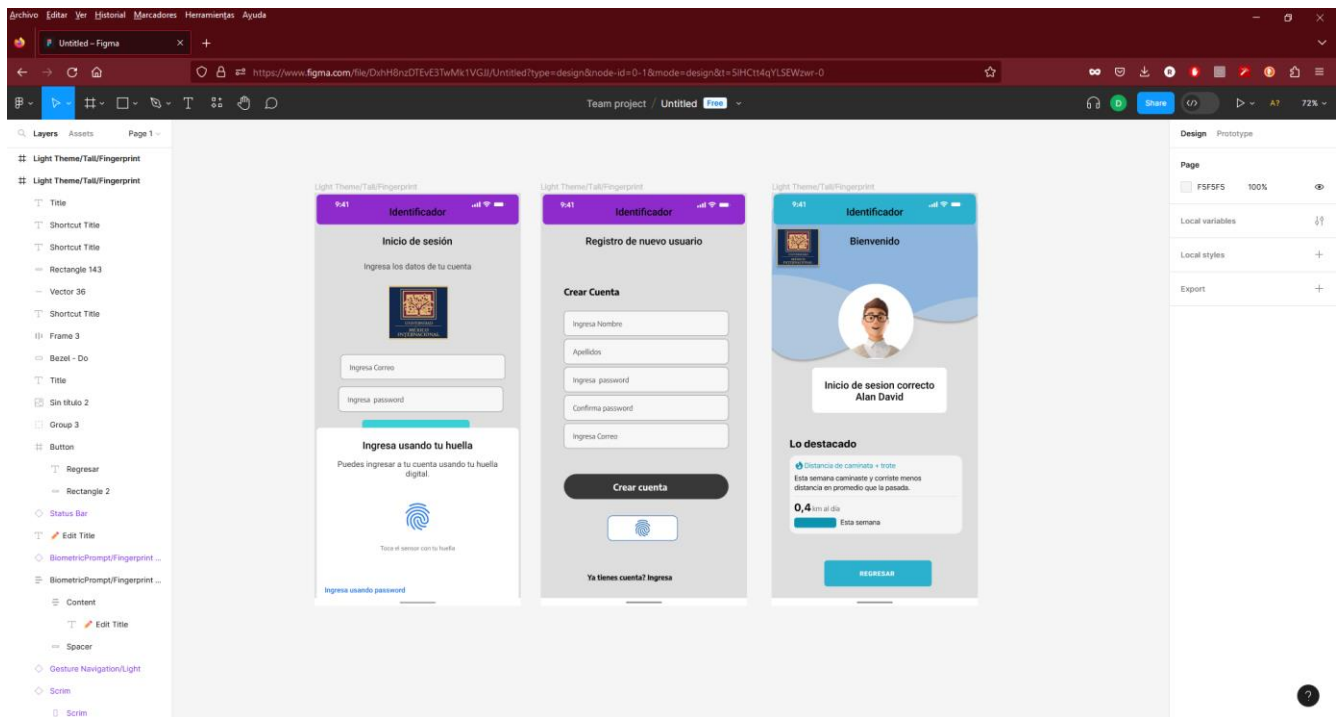
La autenticación biométrica, como el escaneo de huellas dactilares, también es efectiva para prevenir ataques de suplantación de identidad, ya que es difícil falsificar una huella digital.

Además, esta solución cumple con regulaciones de seguridad en muchas industrias, garantizando la protección de datos personales y la integridad de la información.

Finalmente, la autenticación de huellas dactilares se alinea con las tendencias tecnológicas actuales, lo que puede mejorar la percepción de la marca y mantener a la aplicación relevante en el mercado.

Etapa 1:

- Diseño de interfaces




9:41

Identificador


Inicio de sesión

Ingresa los datos de tu cuenta



Ingresa usando tu huella

Puedes ingresar a tu cuenta usando tu huella digital.



Toca el sensor con tu huella

[Ingresa usando password](#)


9:41

Identificador

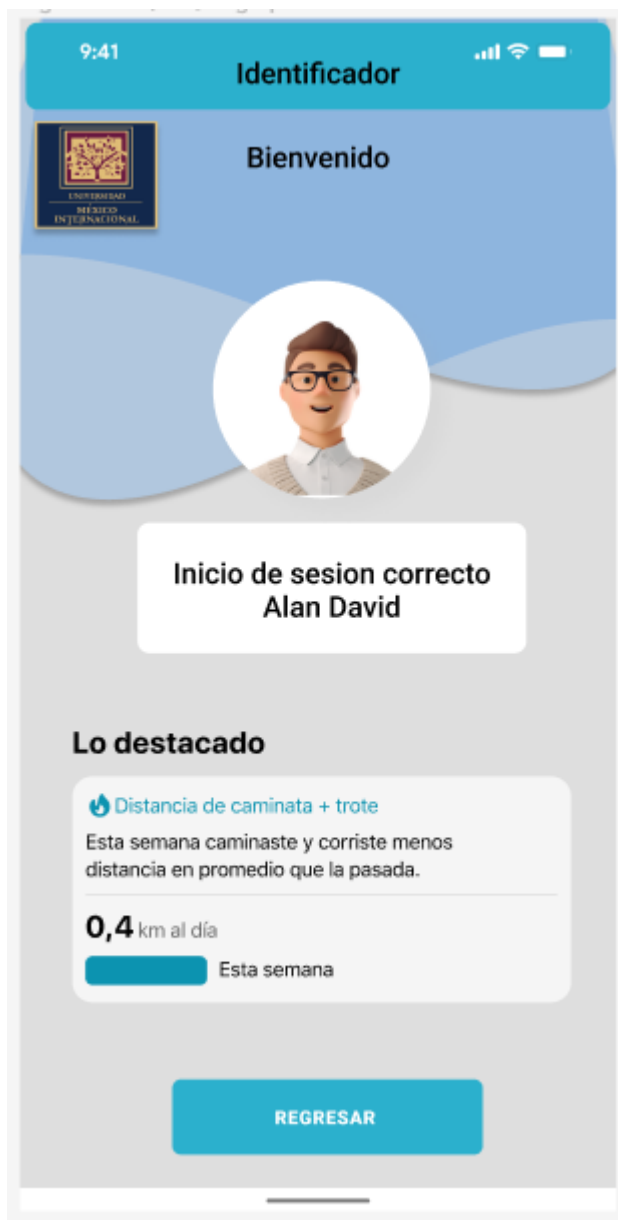
Registro de nuevo usuario

Crear Cuenta

Crear cuenta



[Ya tienes cuenta? Ingresa](#)



Etapa 2:

- Codificación

Se adjunta parte del código de la aplicación biométrica llamada identificador en donde se observa cómo se aplicó el código para que se pudiera usar la verificación biométrica.

LoginActivity.java

```
package com.example.aplicacionbiometrica;
import android.app.AlertDialog;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Toast;
import androidx.annotation.Nullable;
import androidx.appcompat.app.AppCompatActivity;
import androidx.biometric.BiometricPrompt;
import androidx.core.content.ContextCompat;
import com.example.aplicacionbiometrica.databinding.ActivityLoginBinding;
import com.google.android.material.textfield.TextInputLayout;
```



```

import java.util.Calendar;
import java.util.regex.Pattern;
import androidx.core.util.PatternsCompat;
import android.widget.Button;
import android.widget.ImageButton;
import android.util.Log;
import androidx.annotation.NonNull;

public class LoginActivity extends AppCompatActivity {

    private ActivityLoginBinding binding;
    private BiometricPrompt biometricPrompt;
    private BiometricPrompt.PromptInfo promptInfo;

    @Override
    protected void onCreate(@Nullable Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        binding = ActivityLoginBinding.inflate(getLayoutInflater());
        View view = binding.getRoot();
        setContentView(view);

        Button registrarButton = findViewById(R.id.btnRegistrar);
        registrarButton.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                Intent intent = new Intent(LoginActivity.this,
Sign_inActivity.class);
                startActivity(intent);
            }
        });

        binding.btnIngresar.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                validate();
            }
        });

        ImageButton huellaButton = findViewById(R.id.huella);
        huellaButton.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                showBiometricPrompt();
            }
        });

        String saludo = getGreeting();
        Toast.makeText(this, saludo, Toast.LENGTH_SHORT).show();
    }

    private String getGreeting() {
        Calendar fecha = Calendar.getInstance();
        int hours = fecha.get(Calendar.HOUR_OF_DAY);

        if (hours > 0 && hours < 12) {
            return "Buenos días";
        } else if (hours >= 12 && hours < 18) {
            return "Buenas tardes";
        }
    }
}

```

```

    } else {
        return "Buenas noches";
    }
}

private void validate() {
    boolean[] result = {validateEmail(), validatePassword()};
    if (!containsFalse(result)) {
        Intent intent = new Intent(this, WelcomeActivity2.class);
        startActivity(intent);
        finish();
    }
}

private boolean containsFalse(boolean[] array) {
    for (boolean item : array) {
        if (!item) {
            return true;
        }
    }
    return false;
}

private boolean validateEmail() {
    String email = binding.textFieldEmail.getText().toString();
    if (email.isEmpty()) {
        showAlertDialog("Advertencia", "El campo Email no puede estar vacío.  
Ingrese correo.");
        return false;
    } else if (!PatternsCompat.EMAIL_ADDRESS.matcher(email).matches()) {
        showAlertDialog("Advertencia", "Correo no válido, debe tener estructura  
de correo electrónico.");
        return false;
    } else {
        binding.textFieldEmail.setError(null);
        return true;
    }
}

private boolean validatePassword() {
    String password =
binding.textFieldPassword.getText().toString();
    Pattern passwordRegex = Pattern.compile("(?=.*[0-9]) (?=.*[a-z]) (?=.*[A-
Z]) (?=.*[@#$$%^&!_+=]) (?!\\S+$)\\. {4,}$");

    if (password.isEmpty()) {
        showAlertDialog("Advertencia", "El campo Password no puede estar vacío.  
Ingrese contraseña.");
        return false;
    } else if (!passwordRegex.matcher(password).matches()) {
        showAlertDialog("Advertencia", "La contraseña debe contener al menos  
una mayúscula, una minúscula, un número, un carácter especial y tener al menos 4  
caracteres.");
        return false;
    } else {
        binding.textFieldPassword.setError(null);
        return true;
    }
}

```

```

private void showBiometricPrompt() {
    Log.d("MyApp", "showBiometricPrompt() llamado");
    // Crea una instancia de BiometricPrompt para la autenticación por huella
    BiometricPrompt fingerprintBiometricPrompt = new BiometricPrompt(this,
        ContextCompat.getMainExecutor(this),
        new BiometricPrompt.AuthenticationCallback() {
            @Override
            public void onAuthenticationSucceeded(
                BiometricPrompt.AuthenticationResult result) {
                super.onAuthenticationSucceeded(result);

                Toast.makeText(LoginActivity.this, "Autenticación
biométrica exitosa", Toast.LENGTH_SHORT).show();

                Intent intent = new Intent(LoginActivity.this,
WelcomeActivity2.class);
                startActivity(intent);
            }
        });

    // Crea la información para la autenticación por huella
    BiometricPrompt.PromptInfo fingerprintPromptInfo = new
BiometricPrompt.PromptInfo.Builder()
        .setTitle("Autenticación biométrica")
        .setSubtitle("Usa tu huella digital para iniciar sesión")
        .setNegativeButtonText("Cancelar")
        .build();

    // Inicia la autenticación por huella
    fingerprintBiometricPrompt.authenticate(fingerprintPromptInfo);
}

private void showAlertDialog(String title, String message) {
    AlertDialog.Builder builder = new AlertDialog.Builder(this);
    builder.setTitle(title);
    builder.setMessage(message);
    builder.setCancelable(false);
    builder.setPositiveButton("Aceptar", null);
    builder.setNegativeButton("Cancelar", null);
    builder.show();
}
}

```

Gradle

```
plugins {
    id 'com.android.application'
}

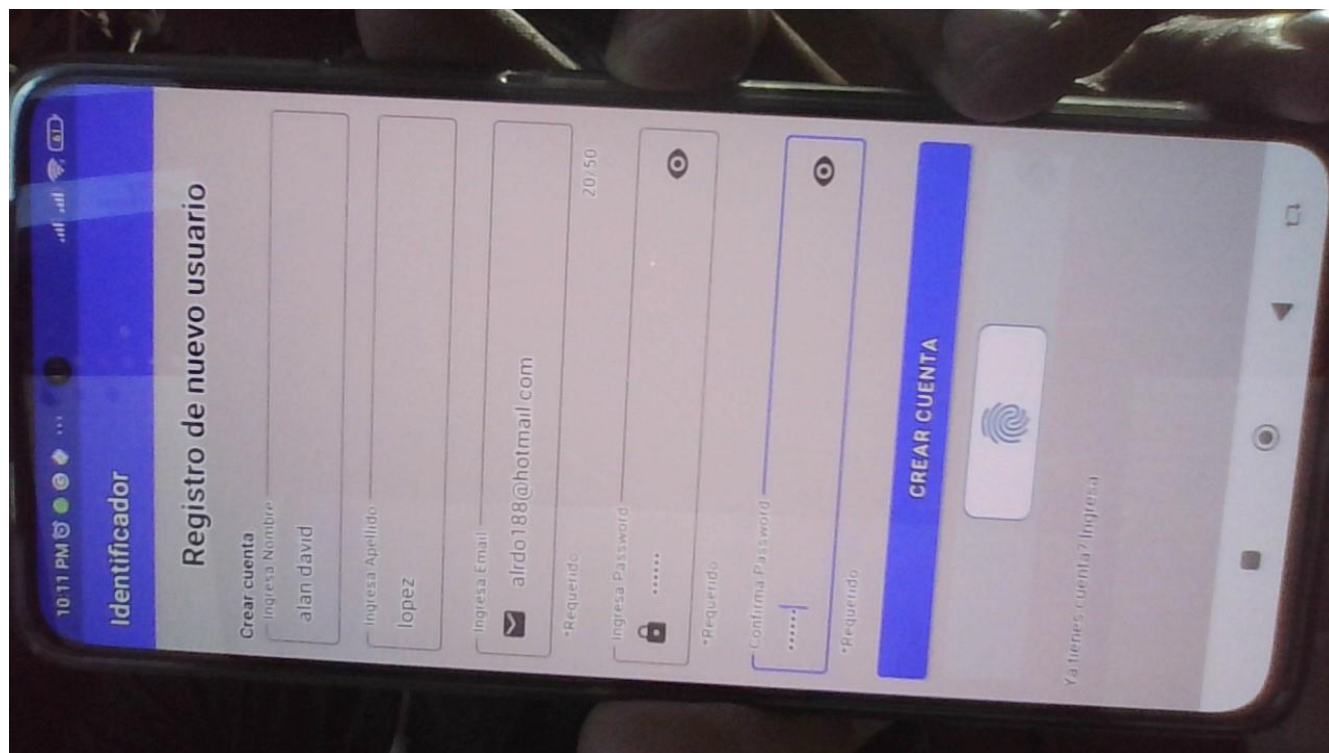
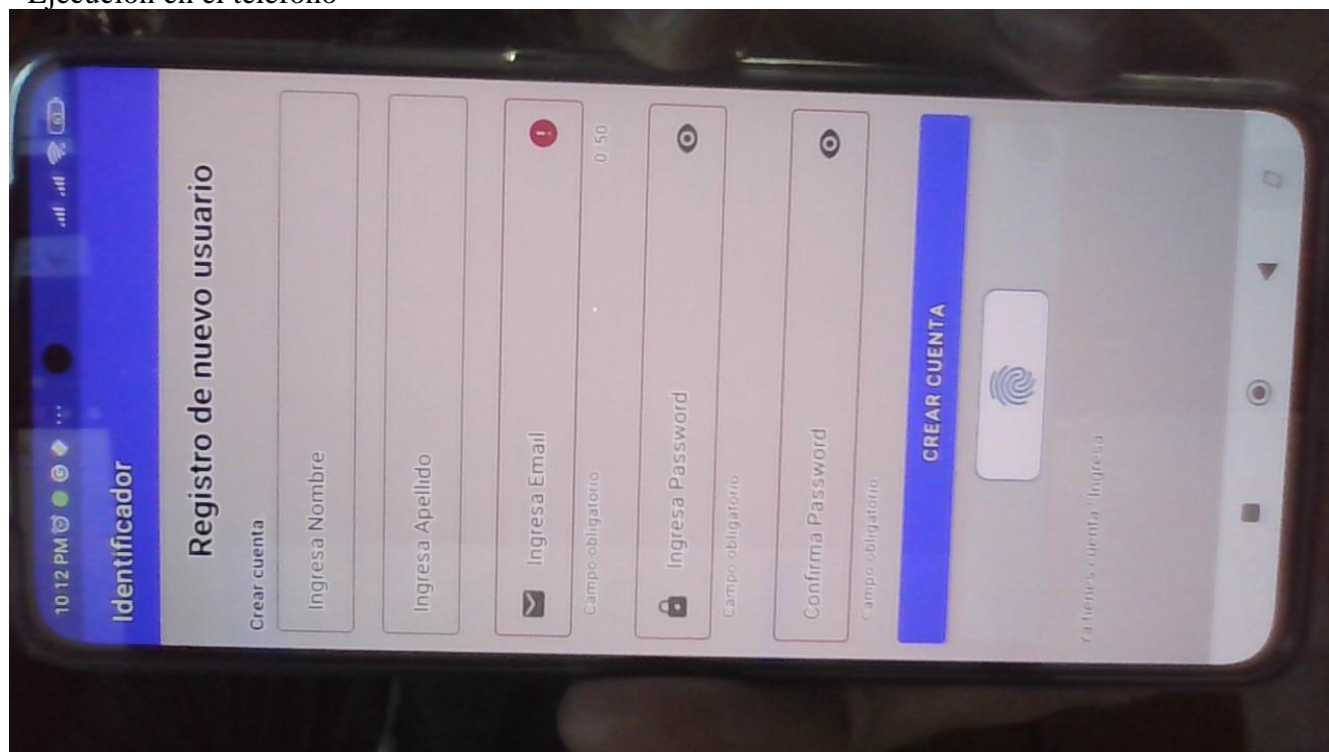
android {
    namespace 'com.example.aplicacionbiometrica'
    compileSdk 33
    dataBinding {
        enabled = true
    }
    viewBinding {
        enabled = true
    }
    defaultConfig {
        applicationId "com.example.aplicacionbiometrica"
        minSdk 26
        targetSdk 33
        versionCode 1
        versionName "1.0"

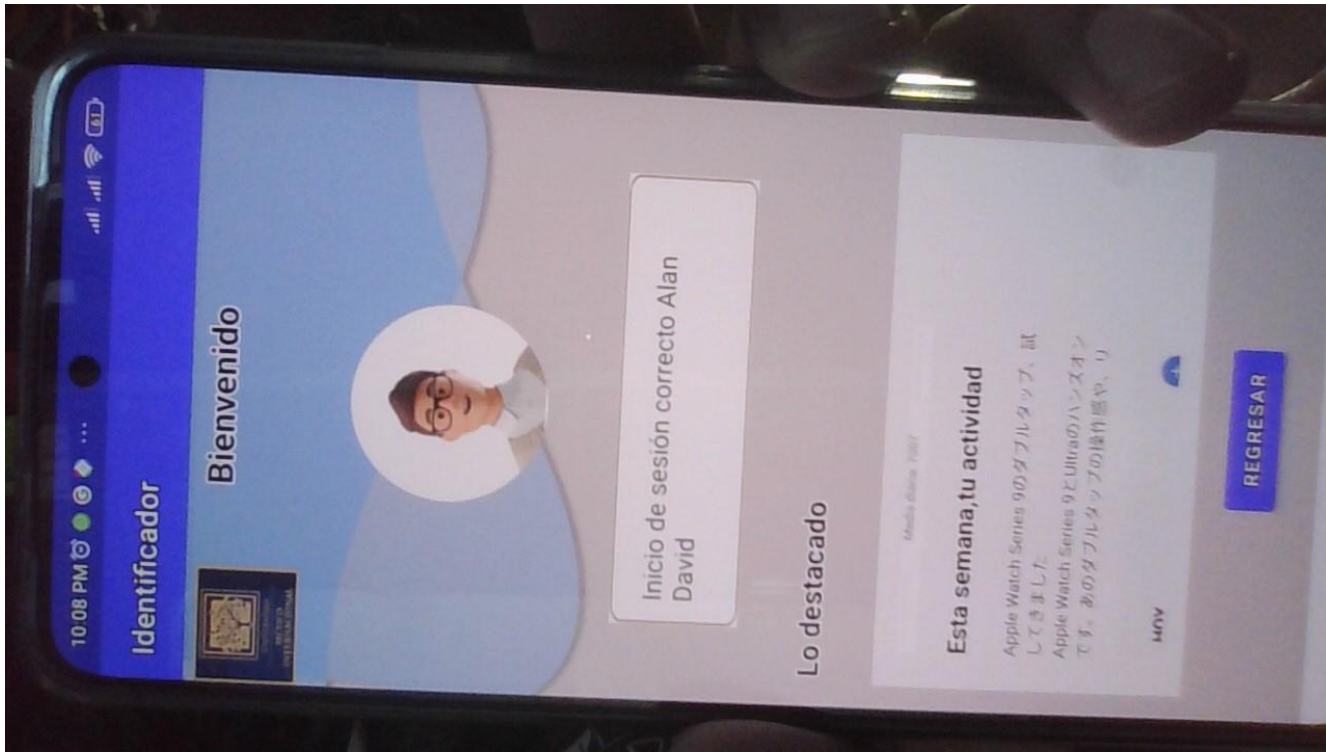
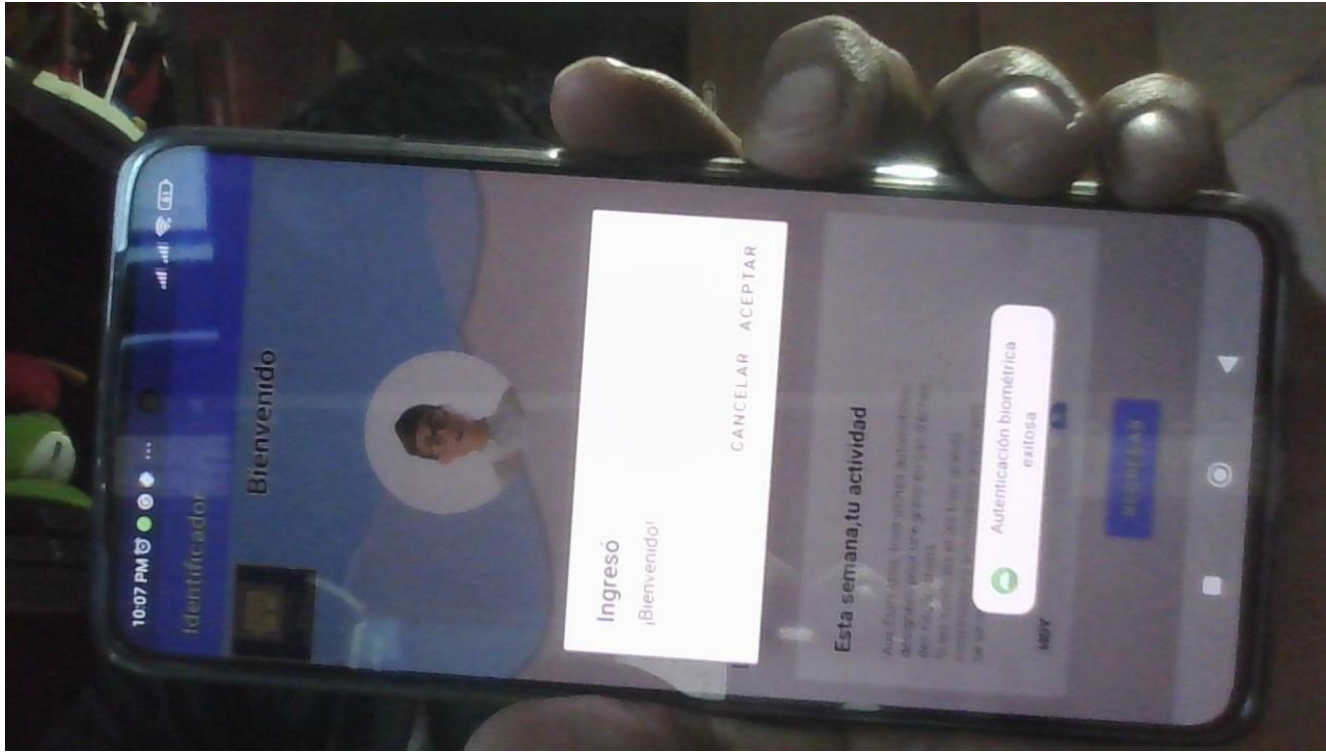
        testInstrumentationRunner "androidx.test.runner.AndroidJUnitRunner"
    }

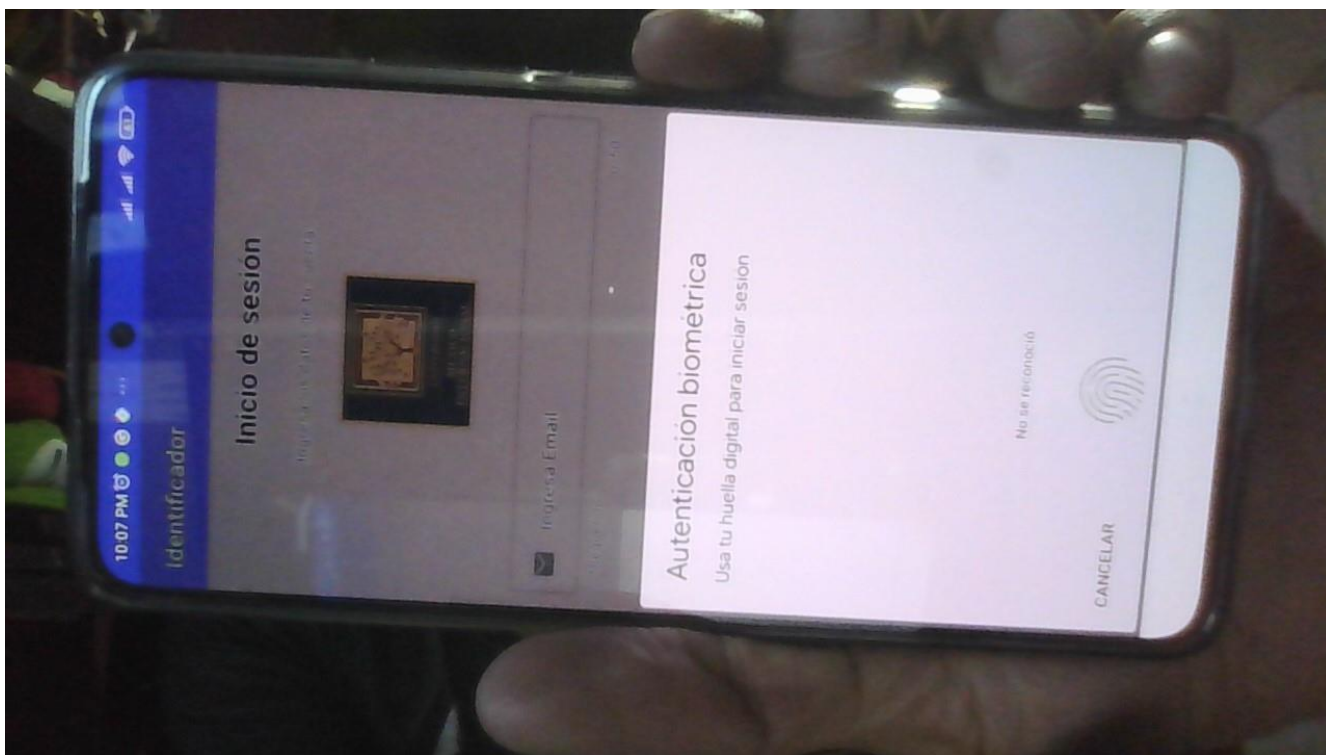
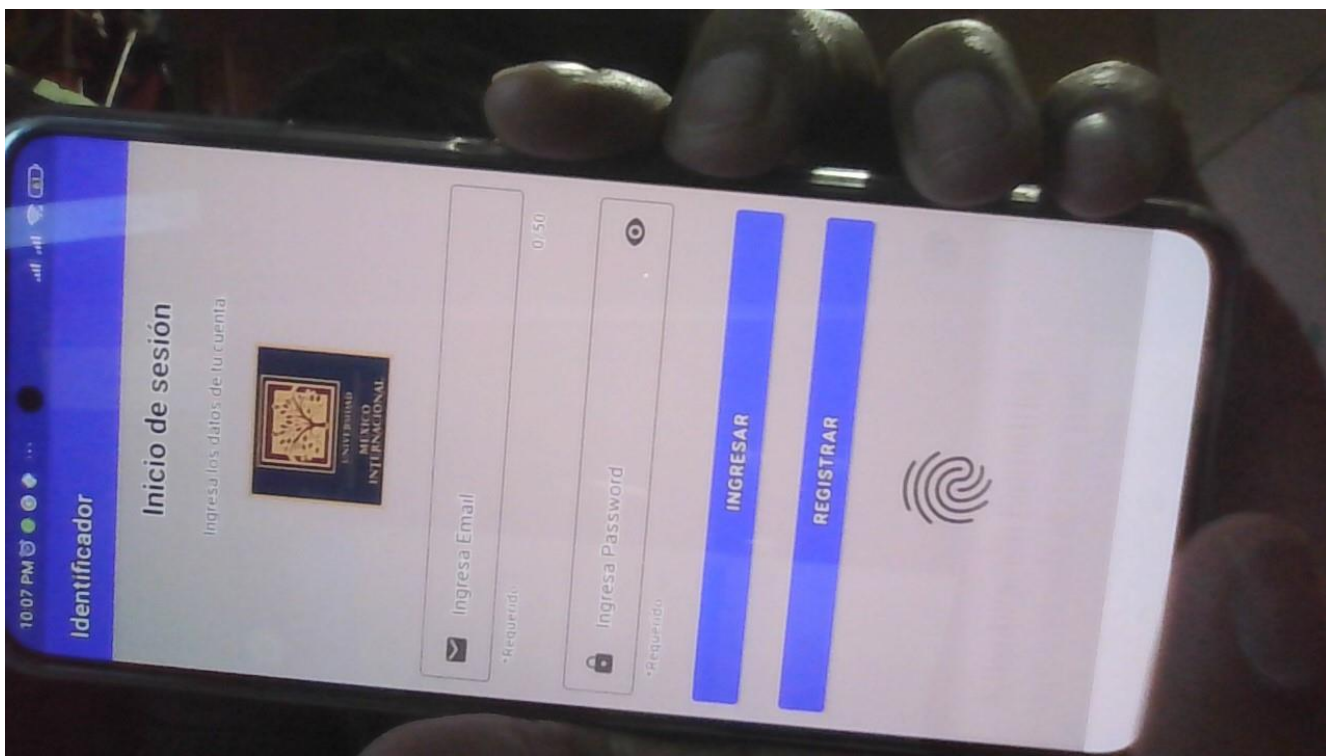
    buildTypes {
        release {
            minifyEnabled false
            proguardFiles getDefaultProguardFile('proguard-android-optimize.txt'),
'proguard-rules.pro'
        }
    }
    compileOptions {
        sourceCompatibility JavaVersion.VERSION_1_8
        targetCompatibility JavaVersion.VERSION_1_8
    }
}

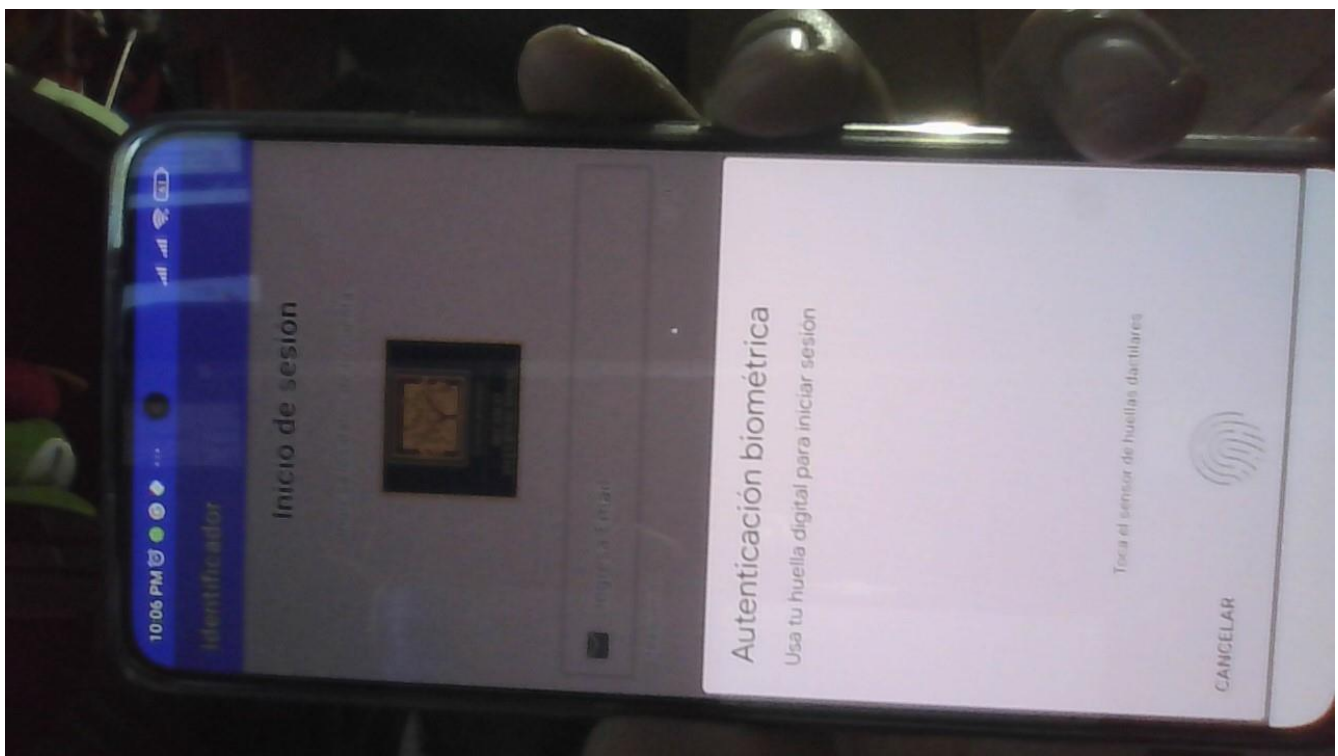
dependencies {
    implementation 'androidx.appcompat:appcompat:1.6.1'
    implementation 'com.google.android.material:material:1.9.0'
    implementation 'androidx.constraintlayout:constraintlayout:2.1.4'
    testImplementation 'junit:junit:4.13.2'
    implementation 'com.github.bumptech.glide:glide:4.12.0'
    annotationProcessor 'com.github.bumptech.glide:compiler:4.12.0'
    androidTestImplementation 'androidx.test.ext:junit:1.1.5'
    androidTestImplementation 'androidx.test.espresso:espresso-core:3.5.1'
    implementation 'androidx.biometric:biometric:1.1.0'
}
```

- Ejecución en el teléfono





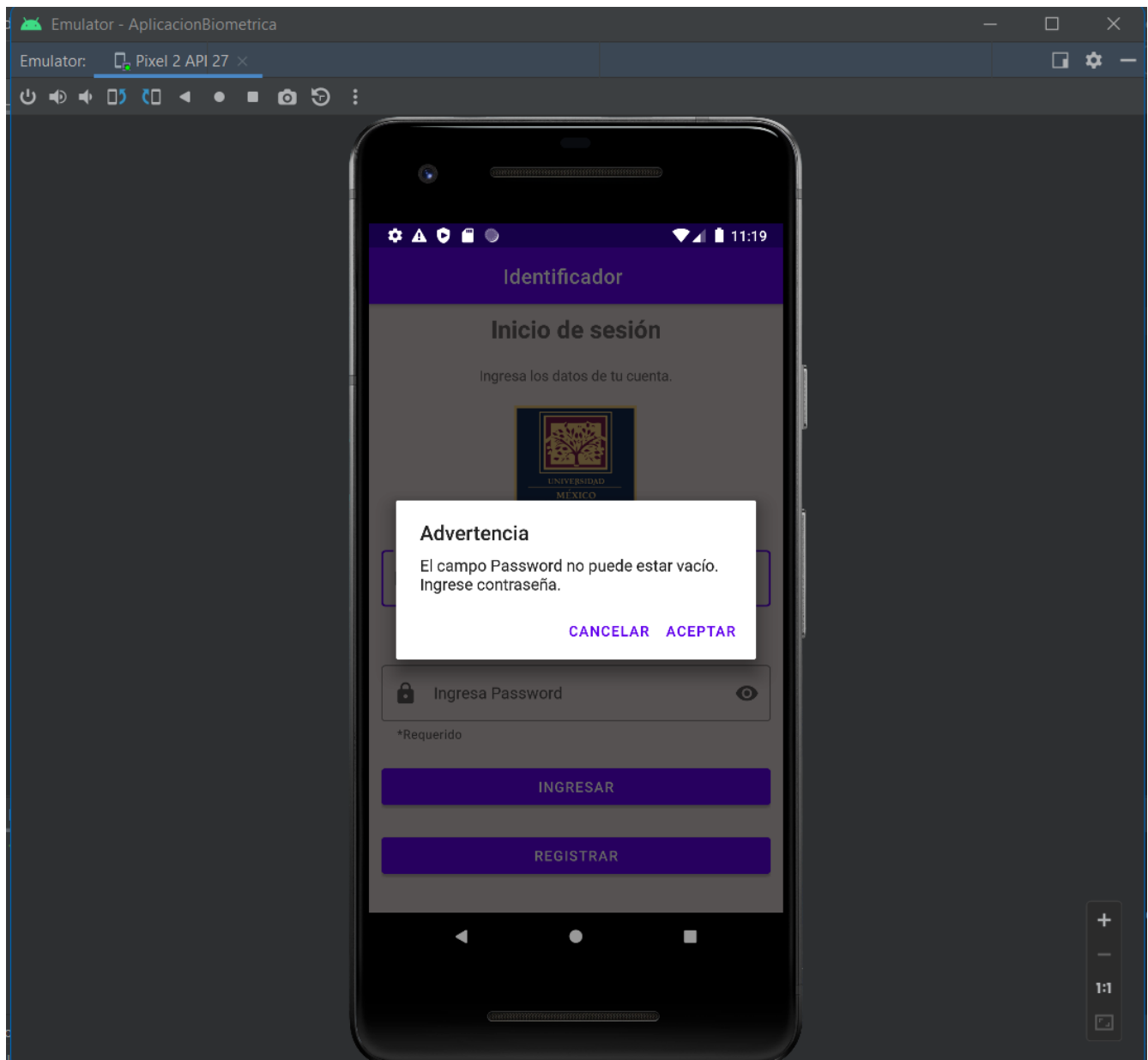


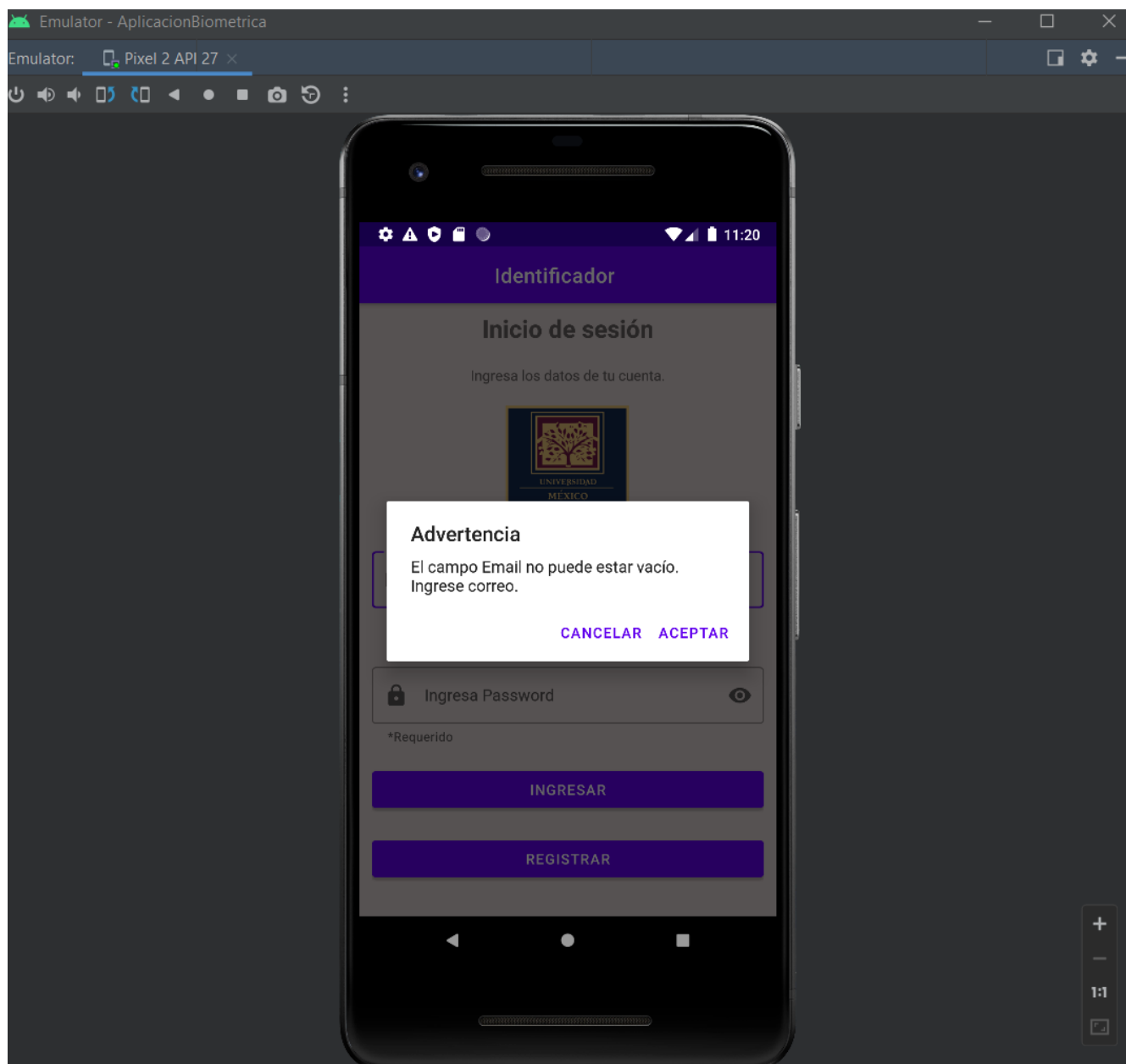


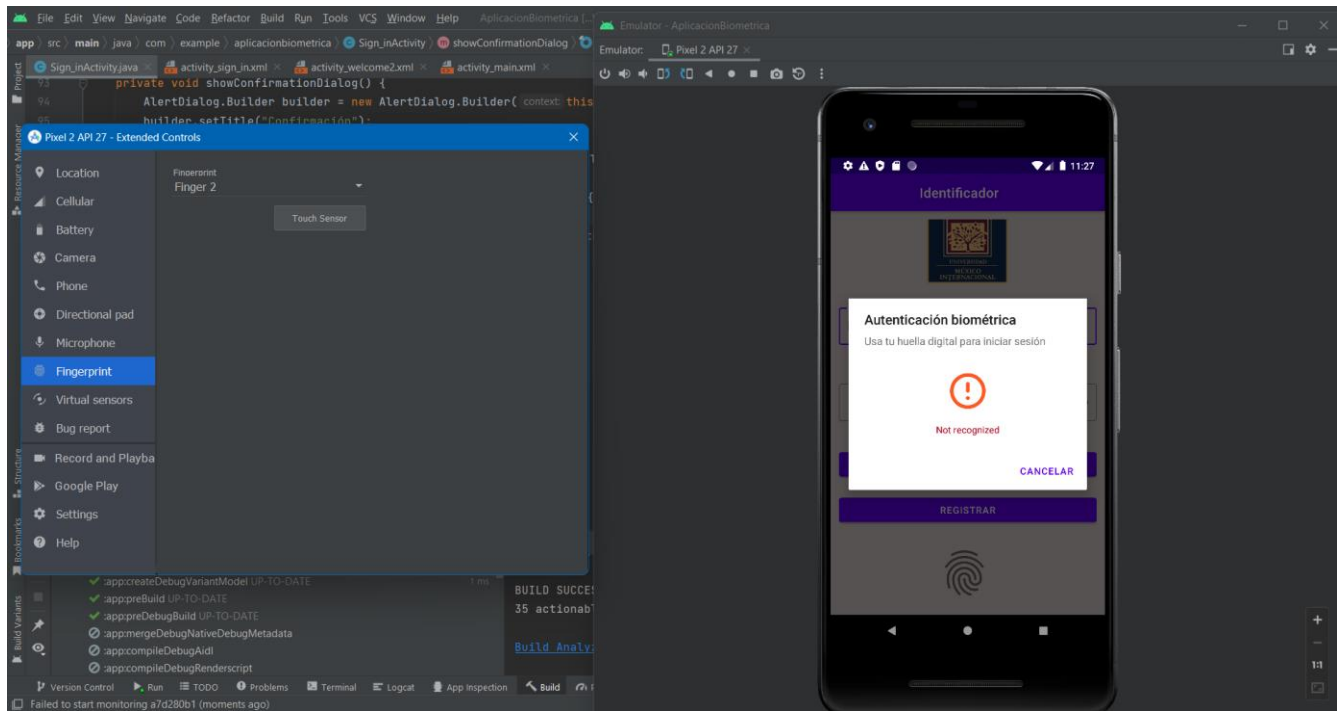
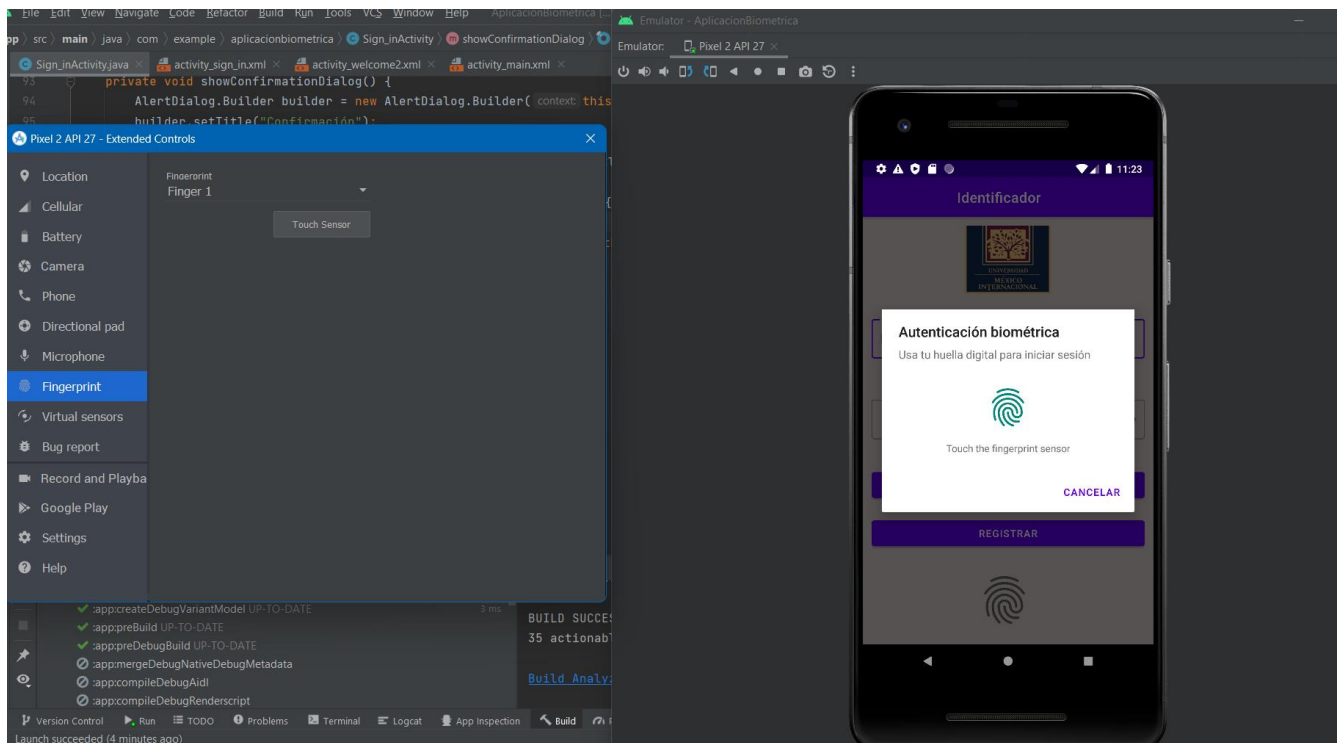
- Enlace del proyecto

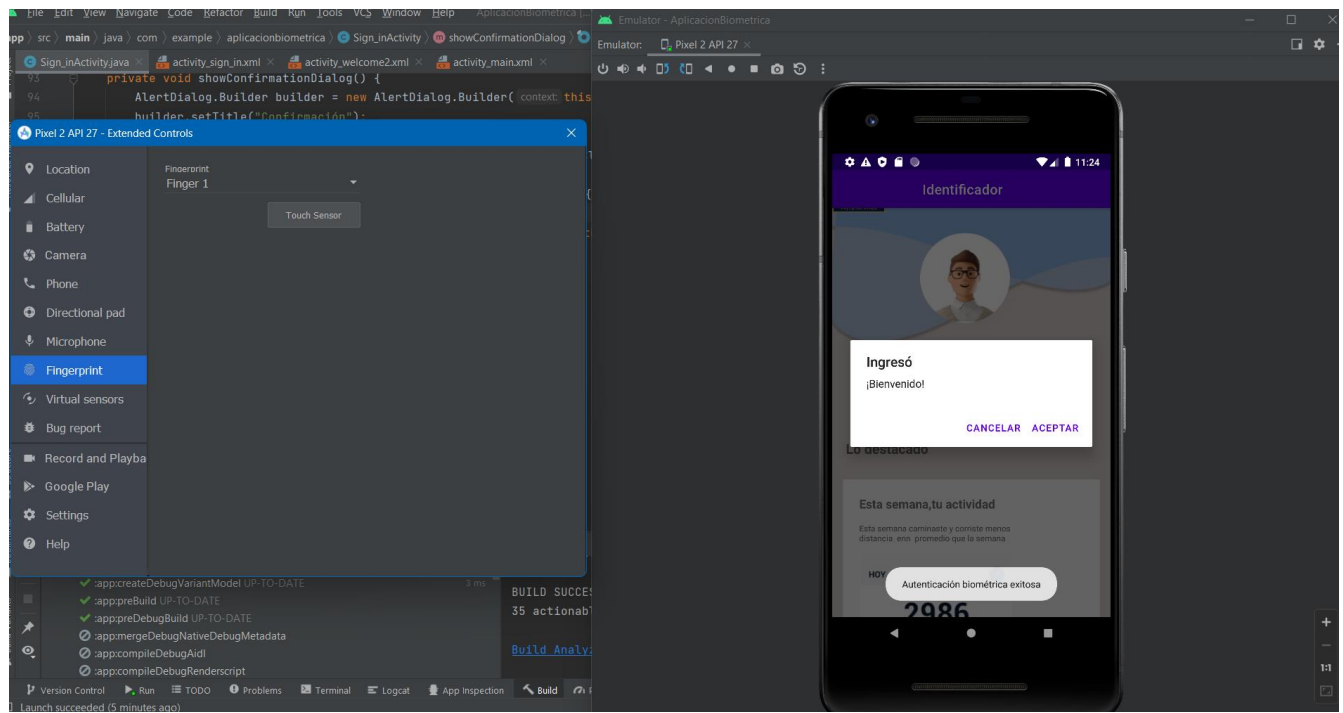
<https://github.com/AlanDavidLR/AplicacionesBiometricas.git>

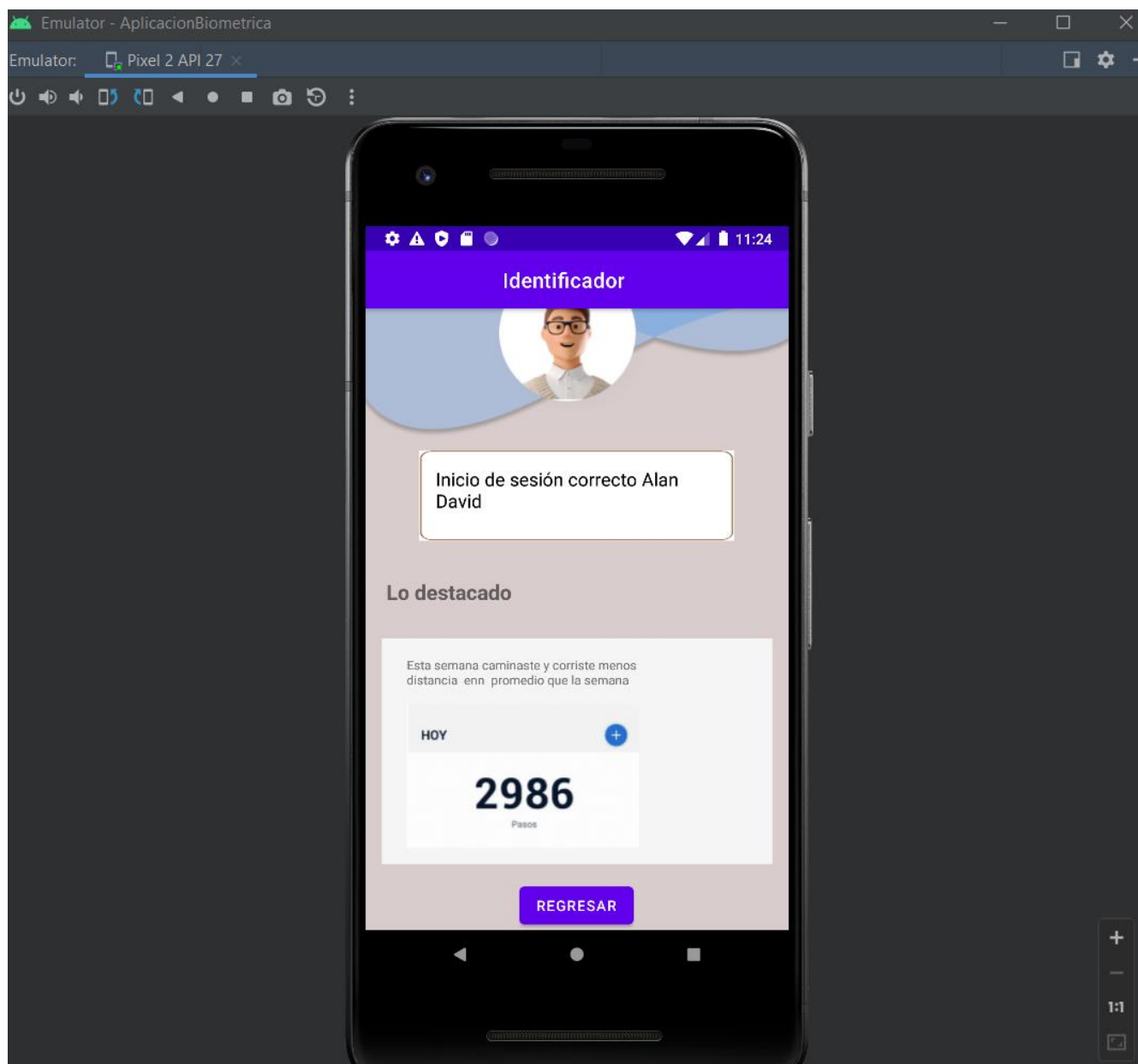
Desarrollo

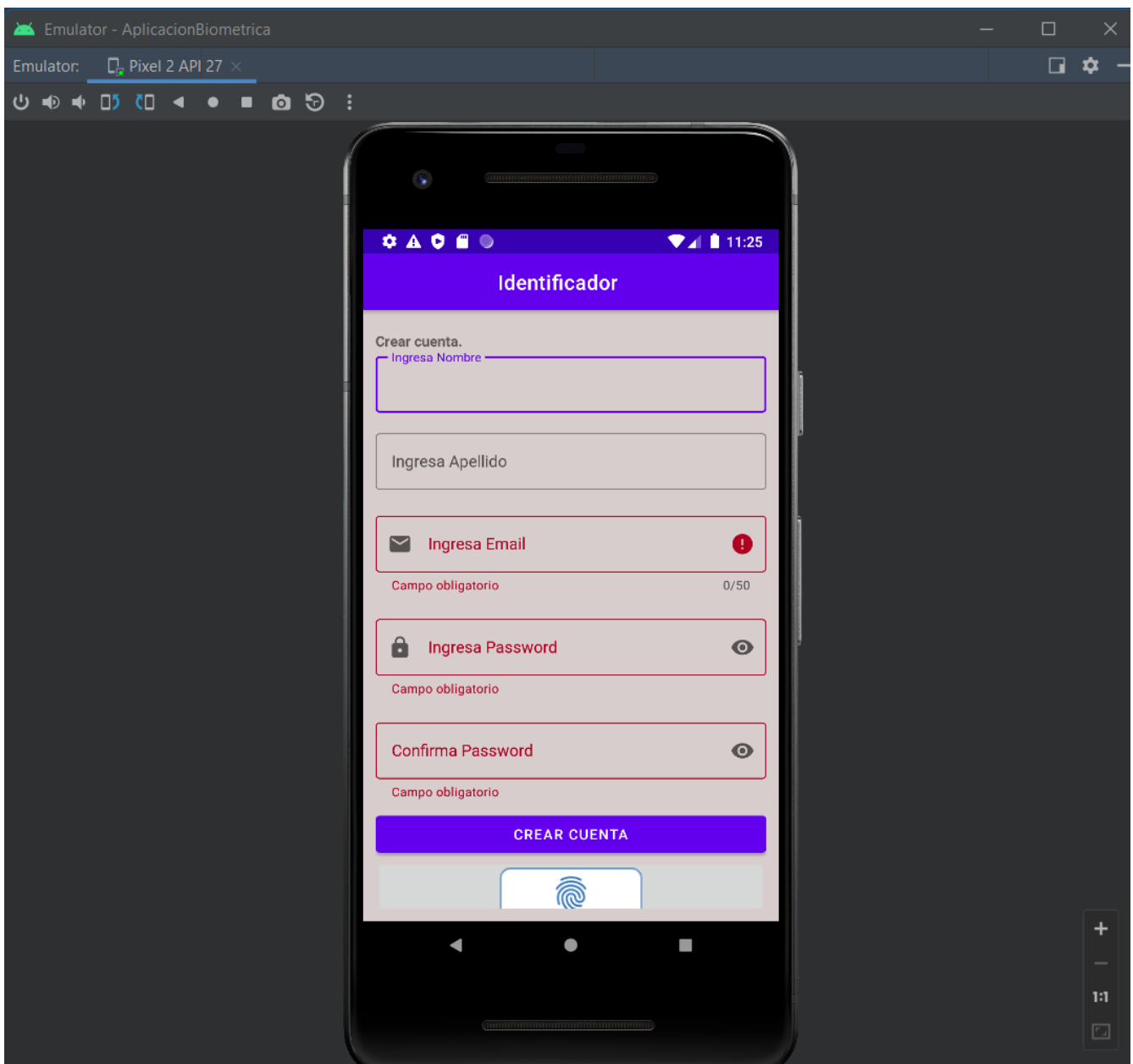


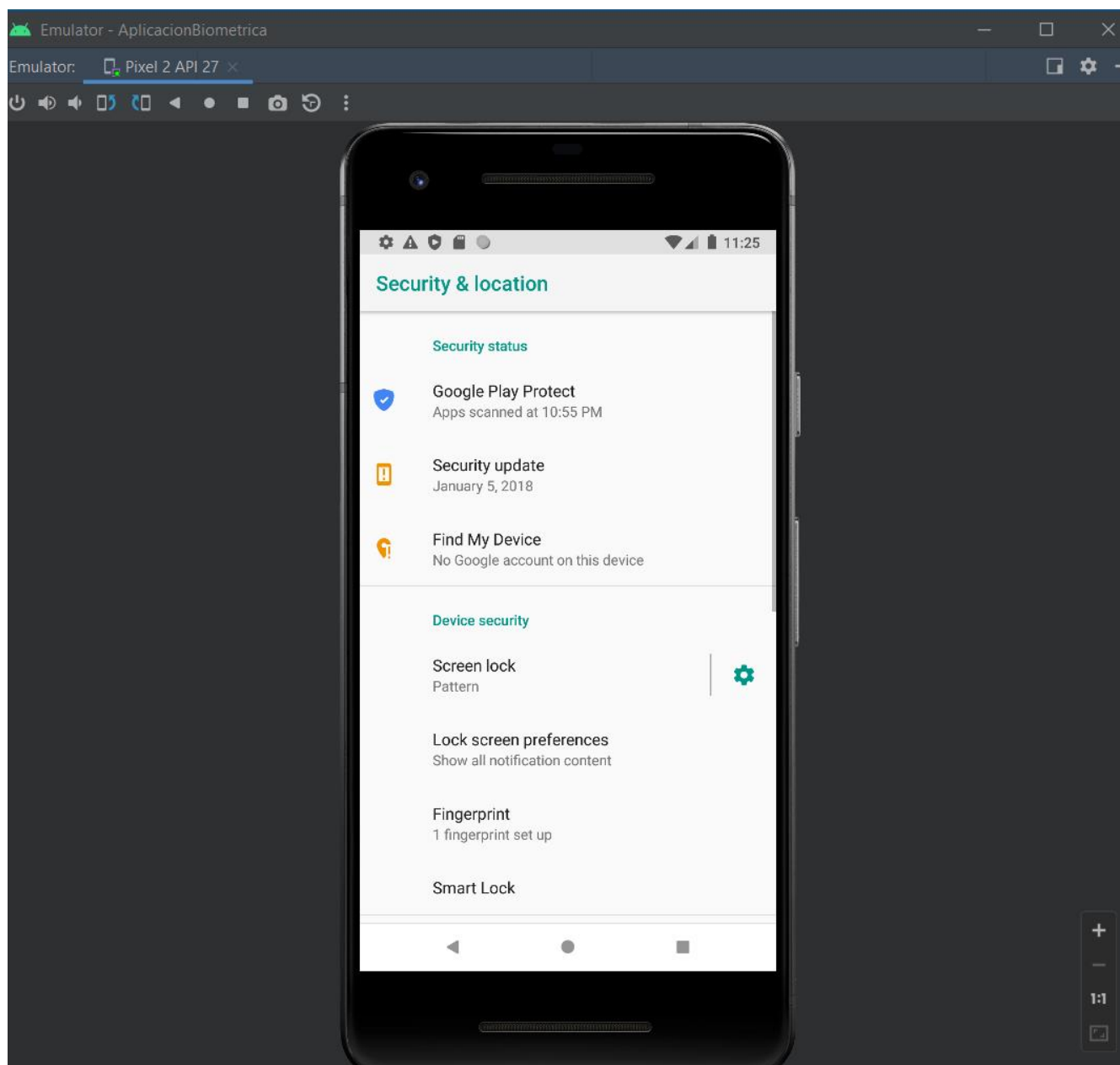












Conclusión

La implementación de la autenticación de huellas dactilares en la actividad propuesta tiene una importancia significativa en el ámbito laboral y la vida cotidiana. En un mundo cada vez más digitalizado, donde la seguridad de la información y la protección de datos personales son preocupaciones fundamentales, esta solución proporciona una herramienta valiosa para garantizar la integridad y la privacidad de las cuentas y la información personal.

En el campo laboral, especialmente en entornos empresariales o aplicaciones que manejan datos sensibles, la autenticación biométrica, como el escaneo de huellas dactilares, se ha convertido en una práctica estándar. Esto se debe a que ofrece un nivel de seguridad superior al de las contraseñas tradicionales. Las empresas pueden proteger mejor sus sistemas y aplicaciones contra el acceso no autorizado, lo que es esencial para mantener la confianza de los clientes y cumplir con regulaciones de seguridad y privacidad.

En la vida cotidiana, esta tecnología simplifica la experiencia del usuario. Ya no es necesario recordar una lista interminable de contraseñas, lo que puede resultar frustrante y llevar al olvido de credenciales. En cambio, un simple escaneo de huellas dactilares permite un acceso rápido y sin complicaciones a dispositivos móviles, aplicaciones bancarias, plataformas de redes sociales y más. Esto ahorra tiempo y reduce la frustración.

Bibliografía

Álvaro Giz Bueno , César Tolosa Borja ,Sistemas Biométricos, En línea:

https://www.dsi.uclm.es/personal/miguelfgraciani/mikicurri/docencia/bioinformatica/web_bio/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

A Turiel Charro, A Teruel Fernández – 2022 ,Implementación de mecanismos biométricos para autenticación de usuarios en aplicaciones multidispositivo, En línea :

<https://docta.ucm.es/entities/publication/68d55e33-4c0d-46f6-aa37-209c5ef5dabf>

<https://developer.android.com/training/sign-in/biometric-auth?hl=es-419#determine-how-user-authenticated>