

Actividad 3 - Pantalla de Autenticación.

Desarrollo de Aplicaciones Móviles 1.

Ingeniería en Desarrollo de Software

Tutor: Humberto Jesús Ortega Vázquez.

Alumno: Homero Ramirez Hurtado.

Fecha: 27 de Noviembre del 2023.



Índice.

. Introducción.

. Descripción.

. Justificación.

. Desarrollo.

- Interfaz.
- Codificación.
- Prueba de Aplicación.

. Conclusión.

. Referencias.



Introducción.

A continuación, retomaremos la actividad pasada para por fin poder concluir con nuestro proyecto final el cual realizaremos una pantalla de Autenticación para poder ingresar a nuestra aplicación de banco y de esta manera poder finalizar nuestro proyecto con ello también analizaremos para que sirve y como nos puede ayudar a incorporar una Autenticación ya que esta nos brinda seguridad.

Descripción.

La autenticación es el proceso de verificar la identidad de una persona, una aplicación o un servicio que solicita acceder a un recurso o un sistema digital. La autenticación sirve para proteger la información y los datos confidenciales de accesos no autorizados o malintencionados. Por ejemplo, cuando inicias sesión en tu cuenta de correo electrónico, debes proporcionar tu nombre de usuario y tu contraseña, que son tus credenciales de autenticación. Estas credenciales se comparan con las que están almacenadas en el sistema de correo electrónico, y si coinciden, se te permite acceder a tu bandeja de entrada.

Existen diferentes tipos y métodos de autenticación, que pueden variar en su nivel de seguridad y complejidad. Algunos de los más comunes son:

- Autenticación por contraseña: Es el método más simple y más usado, que consiste en introducir una combinación de nombre de usuario y contraseña para acceder a un servicio o sistema. Sin embargo, este método también es el más vulnerable, ya que las contraseñas pueden ser robadas, adivinadas o reutilizadas por los atacantes. Por eso, se recomienda usar contraseñas fuertes y únicas para cada servicio.
- Autenticación de dos factores (2FA): Es un método que añade una capa extra de seguridad a la autenticación por contraseña, al requerir un segundo factor de verificación, además de la contraseña. Este factor puede ser algo que el usuario posee (como un teléfono móvil o un token), algo que el usuario sabe (como una pregunta de seguridad o un PIN) o algo que el usuario es (como una huella dactilar o un escaneo facial). De esta forma, se dificulta el acceso no autorizado, incluso si la contraseña es comprometida.
- Autenticación multifactor (MFA): Es un método que combina varios factores de autenticación, como los mencionados anteriormente, para aumentar el nivel de seguridad y confianza. Cuantos más factores se requieran, más difícil será que un atacante pueda suplantar la identidad del usuario legítimo.
- Autenticación sin contraseña: Es un método que elimina la necesidad de usar contraseñas, y en su lugar, utiliza otros mecanismos de autenticación, como el reconocimiento biométrico, los códigos de un solo uso (OTP) o los certificados digitales. Este método pretende mejorar la experiencia de usuario y reducir los riesgos asociados a las contraseñas.

Justificación.

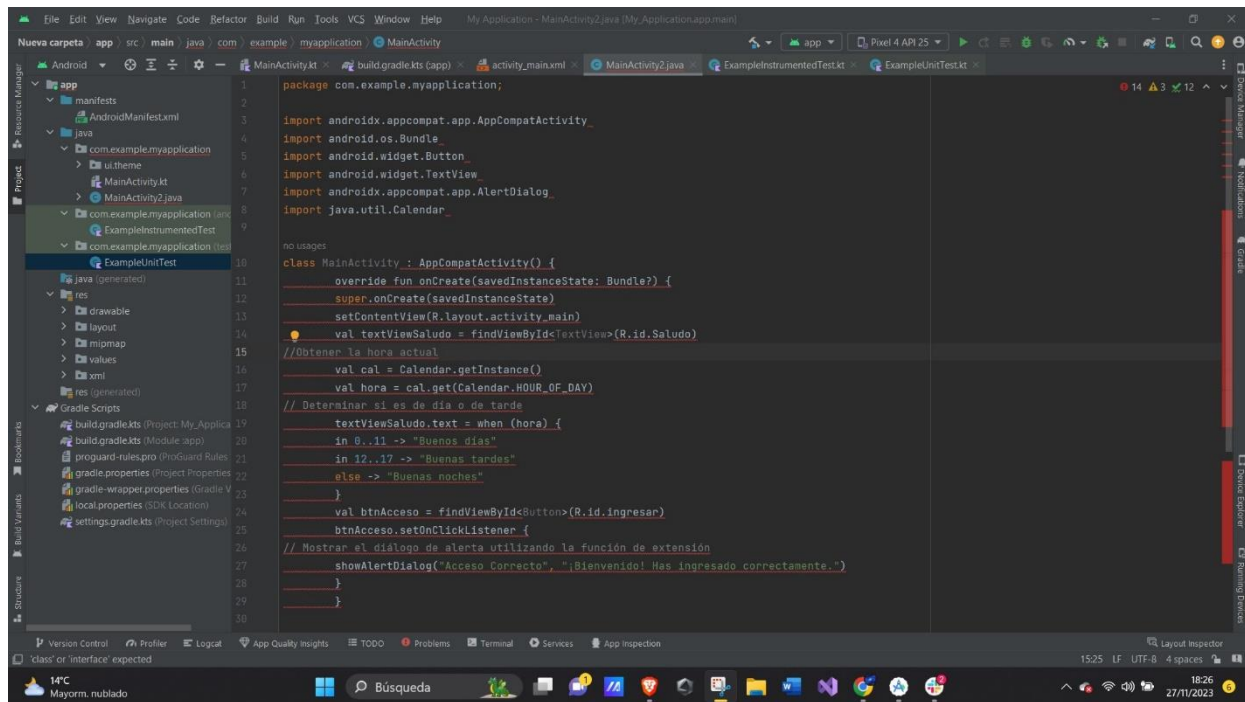
La autenticación es un proceso muy importante para garantizar la seguridad y la privacidad de las personas y las organizaciones que utilizan servicios o sistemas digitales. La autenticación tiene muchos beneficios, tanto para los usuarios como para los proveedores de estos servicios o sistemas. Algunos de estos beneficios son:

- Reduce el fraude y el robo de identidad: Al requerir más de un factor de verificación, se dificulta que los ciberdelincuentes puedan acceder a las cuentas o los datos de los usuarios legítimos. Por ejemplo, si alguien roba o adivina una contraseña, no podrá entrar en la cuenta si también necesita un código enviado por SMS o una huella dactilar.
- Incrementa la confianza del cliente: Al ofrecer un nivel de seguridad más alto, se genera una mayor confianza entre los clientes y los proveedores de servicios o sistemas. Los clientes se sienten más seguros al realizar transacciones en línea, como operaciones bancarias o compras, y los proveedores se benefician de una mayor fidelidad y satisfacción de los clientes.
- Cumple con la normativa: Algunos sectores, como el financiero o el sanitario, tienen normativas específicas que exigen el uso de la autenticación de varios factores para proteger la información sensible de los clientes. Al cumplir con estas normativas, se evitan posibles sanciones o multas, y se mejora la reputación de la empresa.
- Reduce los costes operativos: Al implementar la autenticación de varios factores, se reduce la necesidad de tener personal dedicado a resolver problemas relacionados con el acceso a las cuentas o los sistemas, como el restablecimiento de contraseñas o la recuperación de datos. Además, se ahorra en costes de hardware o software adicionales, ya que se pueden utilizar dispositivos móviles o biométricos para la autenticación.
- Optimiza las transacciones móviles seguras: Al utilizar la autenticación de varios factores, se facilita el uso de dispositivos móviles para realizar transacciones en línea, como pagos o transferencias. Los usuarios no tienen que recordar o introducir contraseñas complejas, sino que pueden usar métodos más rápidos y cómodos, como el reconocimiento facial o los códigos de un solo uso. Esto mejora la experiencia de usuario y aumenta la conversión.
- Combate la fatiga de las contraseñas: Al eliminar o reducir el uso de contraseñas, se evita que los usuarios tengan que recordar o gestionar múltiples contraseñas para diferentes servicios o sistemas. Esto reduce el riesgo de que los usuarios usen contraseñas débiles o repetidas, o que las anoten o las compartan con otras personas. También se evita que los usuarios se olviden o pierdan sus contraseñas y tengan que solicitar su recuperación.

- Simplifica el proceso de inicio de sesión: Al usar la autenticación de varios factores, se simplifica el proceso de inicio de sesión para los usuarios, ya que solo tienen que proporcionar uno o dos factores de verificación, en lugar de tener que introducir datos personales o responder a preguntas de seguridad. Esto reduce la fricción y el tiempo de espera, y mejora la usabilidad y la accesibilidad.

Como puedes ver, la autenticación tiene muchos beneficios que pueden mejorar la seguridad, la confianza, el cumplimiento, el ahorro, la optimización, la comodidad y la simplicidad de los servicios o sistemas digitales.

Desarrollo.



```
package com.example.myapplication;

import androidx.appcompat.app.AppCompatActivity
import android.os.Bundle
import android.widget.Button
import android.widget.TextView
import androidx.appcompat.app.AlertDialog
import java.util.Calendar

no usages

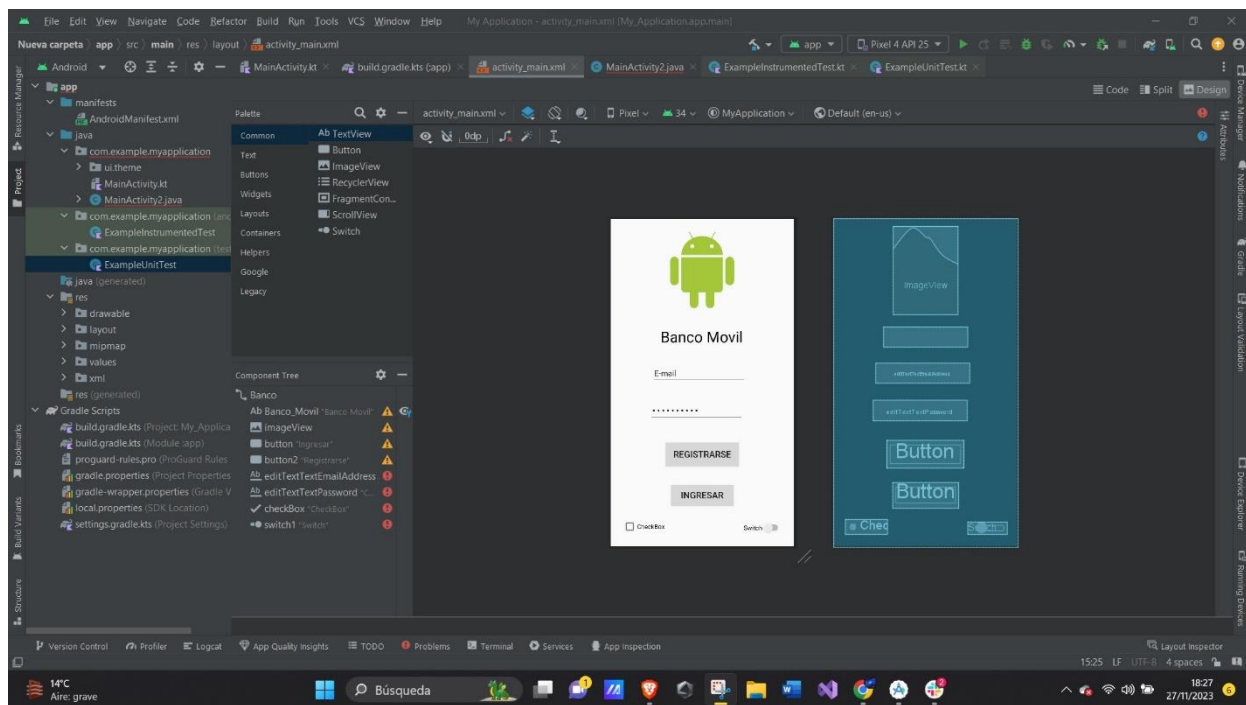
class MainActivity2 : AppCompatActivity() {
    override fun onCreate(savedInstanceState: Bundle?) {
        super.onCreate(savedInstanceState)
        setContentView(R.layout.activity_main)
        val textViewSaludo = findViewById<TextView>(R.id.Saludo)

        //Obtener la hora actual
        val cal = Calendar.getInstance()
        val hora = cal.get(Calendar.HOUR_OF_DAY)

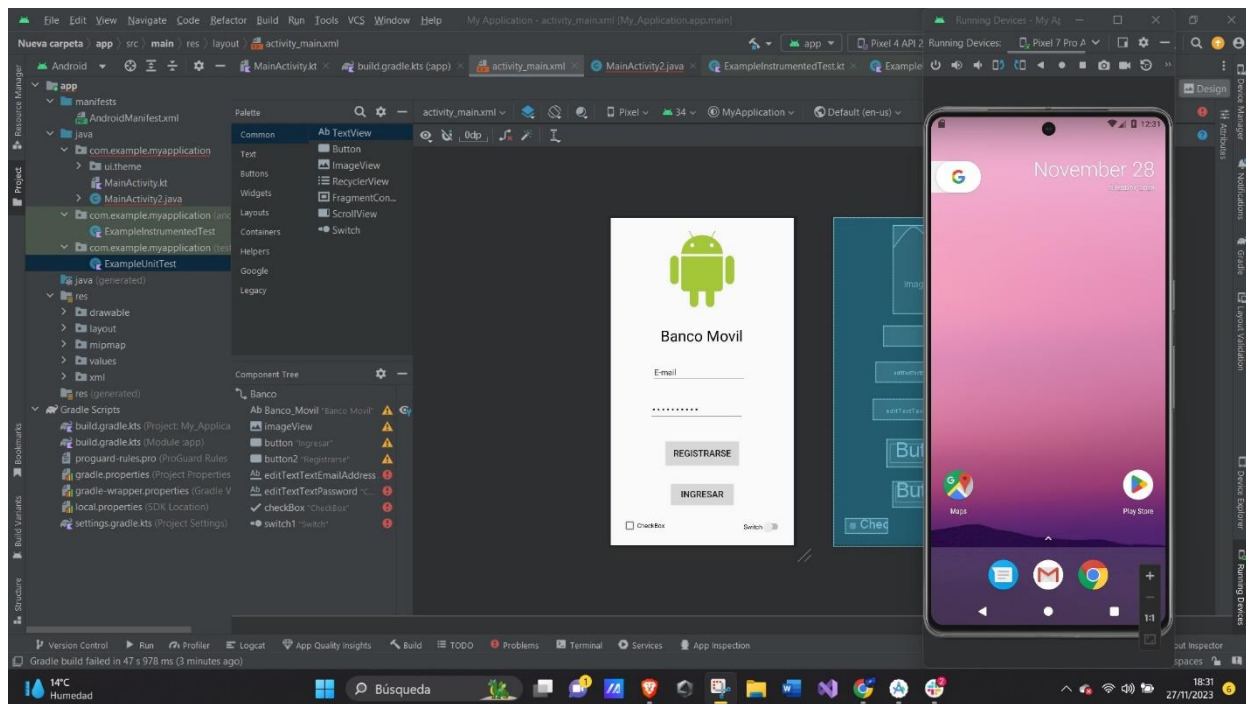
        // Determinar si es de día o de tarde
        textViewSaludo.text = when (hora) {
            in 8..11 -> "Buenos días"
            in 12..17 -> "Buenas tardes"
            else -> "Buenas noches"
        }

        val btnAcceso = findViewById<Button>(R.id.ingresar)
        btnAcceso.setOnClickListener {
            // Mostrar el diálogo de alerta utilizando la función de extensión
            showAlertDialog("Acceso Correcto", "¡Bienvenido! Has ingresado correctamente.")
        }
    }
}
```

Codificación.



Interfaz de la aplicación.



Se pone a Prueba la aplicación, pero no responde por la memoria.

Conclusión.

En conclusión aprendí a como realizar una aplicación con el software de Android Studio desde como crear el archivo hasta la codificación y la presentación de la interfaz con ello pondré en práctica los conocimientos adquiridos y de esta manera ir conociendo mas el software para poder ir mejorando con la práctica y de esta manera ser más eficiente con ella, por lo tanto hacer este tipo de autenticación es importante ya que con ella se puede mantener un nivel de seguridad eficaz para poder proteger tanto como datos personales como también de gobierno e incluso de corporaciones.

Referencias.

Videos en YouTube.

Bing.

Video de la Tutoría 3.