Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | #3 | Pantalla de autenticación Desarrollo de aplicaciones Móviles I

Ingeniería en Desarrollo de Software

TUTOR: Humberto Jesús Ortega Vázquez

ALUMNO: Pilar Barajas Cervantes

FECHA: 11/08/2024

índice

Introducción

El registro de aplicaciones proporciona a los usuarios un procedimiento gráfico para localizar la aplicación, tras la instalación queda registrada en el gestor de aplicaciones y consta de un grupo de aplicaciones propio. La pantalla para que las personas usuarias se autentiquen, es la puerta de entrada a una web o una app, tener en cuenta una serie de requisitos en el diseño de la interfaz y la experiencia del usuario son la clave para que funcione. Cuenta la leyenda que antes de la llegada del ordenador personal existía un todo poderoso llamado Mainframe un enorme y potente cerebro mecánico, usado por los principales negocios para procesar cantidades ingentes de datos. Con el paso del tiempo este cerebro evoluciono, permitiendo la interactividad con los humanos y convirtiéndose en un sistema multiusuario, el humano ingresaba su usuario y contraseña. Tras validar los datos, mainframe le abría la barrera de paso para que pudiera programar las tareas que luego procesaría, devolviéndole finalmente su resultado al humano. Es así como la aparatosa máquina se convirtió en del tan conocido proceso de autenticación.

Después de tantos años de uso, las personas están sobradamente acostumbradas a rellenar formularios de registro y Login. Quizás sea esta familiaridad con la autenticación la razón por la que esta parte suele ser la menos atractiva en el diseño de interfaces. Aún, resultado monótonos, estos formularios son generalmente una pieza clave a nivel de negocio Marketing, y no hay que subestimarlos ya que son la puerta de entrada a un producto digital y a que este funcione.

Descripción

A la hora de desarrollar aplicaciones siempre encontramos componentes que se repiten, tal es el caso del módulo que permite validar un usuario para así conceder o restringir su acceso al contenido de una aplicación debido a esta circunstancia Android Studio nos da la opción de crear una actividad prescrita para proporcionar esta funcionalidad, evitándonos caer en una frase muy popular entre desarrolladores. Una vez creado nuestro Login Activity, analizaremos la interfaz activity_logi_xml que viene por defecto y procesaremos a modificarla. Cuando un usuario desea ingresar a una aplicación la pantalla siempre pedirá la autenticación por medio de sus datos personales, es decir, nombre, correo electrónico y lo más importante su contraseña esto para validar y posterior evitar mal uso de ella.

Esta es una función de seguridad avanzada que generalmente es útil solo si sus requisitos indican que el compromiso del proceso de la aplicación después de la generación o importación de la clave, no puede omitir el requisito por el cual se debe autenticar para que este pueda usar la clave. Una aplicación de autenticación es un método seguro y fácil de verificación de identidad que funciona mediante la generación de códigos, la autenticación es una medida de seguridad importante que protege las cuentas en caso de que las contraseñas se vean comprometidas. En el actual entorno de seguridad cibernética, las contraseñas son vulneradas con frecuencia debido a violaciones de datos y sofisticados ataques de Psishing, entre otros tipos de ciber amenazas.

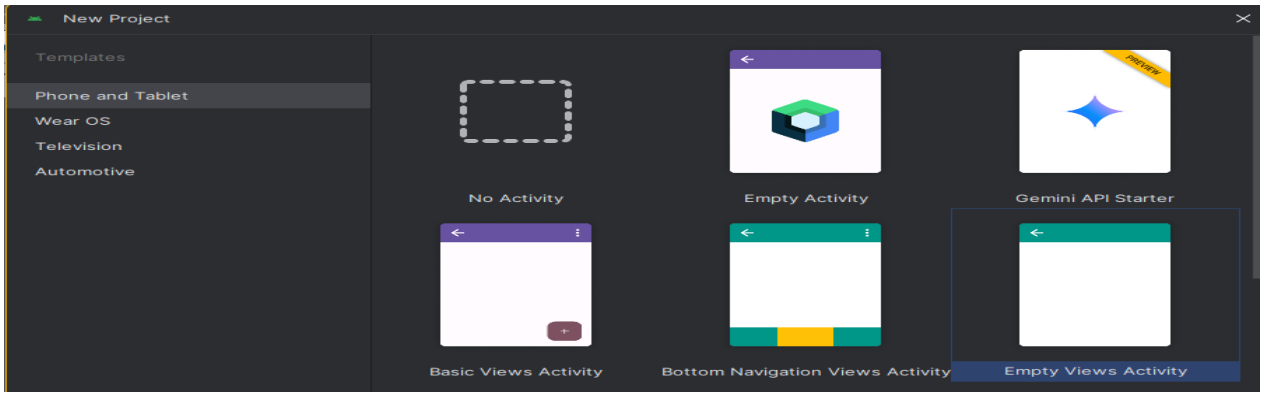
Justificación

Que un usuario se autentique en una web o app significa que le interesa lo que le ofrece, creando un vínculo con esta a través de la aportación de sus datos para poder hacer uso de los servidores. Evidentemente, no siempre se necesita la información del usuario para hacer uso de lo que les brinda un producto digital, pero, ¿Cuántas webs y app han pedido los datos sin necesidad alguna? Seguro que en demasiadas y en la mayoría los usuarios han salido corriendo de ahí. Una aplicación móvil o una app es un software informático diseñado para ejecutarse en teléfonos inteligentes, los registros del dispositivo tienen información que gravaron el sistema y las apps del dispositivo. Estos registros se almacenan temporalmente y se borran de manera continua.

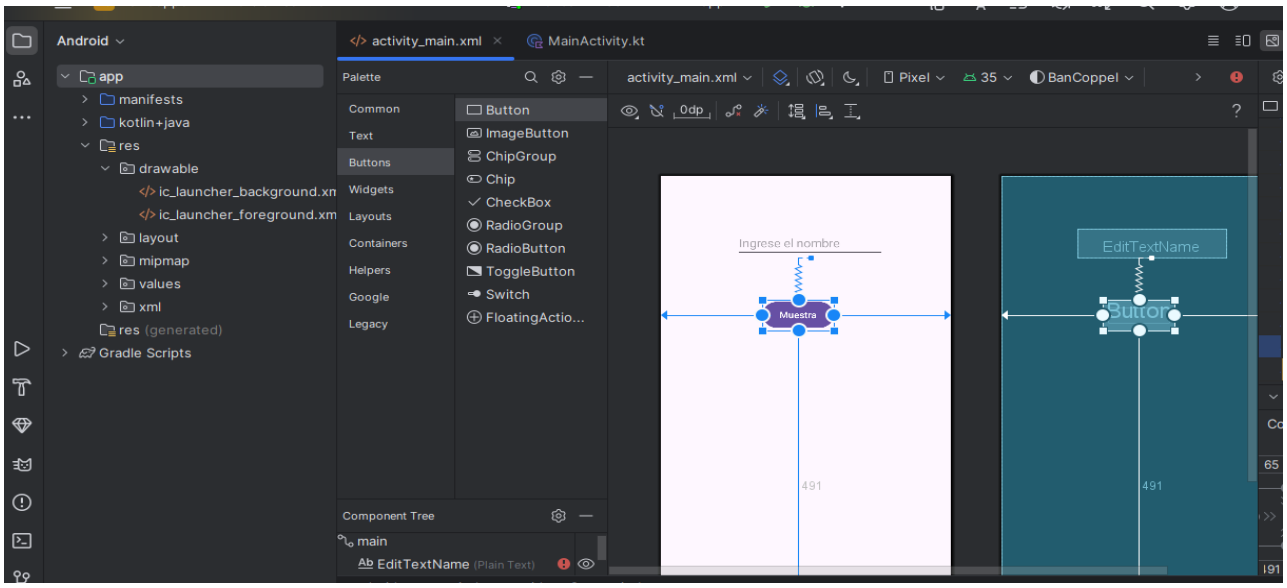
De forma predeterminada todas las apps tienen acceso a los registros de apps que crean, y Google y el fabricante del dispositivo también pueden acceder a la información necesaria para fines como rendimiento del sistema, actualizaciones, mantenimiento y seguridad. Importante: Solo se debe permitir que accedan al registro todas las apps que sean de confianza. Los registros del dispositivo generalmente contienen información técnica limitada, pero es posible que contengan información como las apps que se instalaron en el dispositivo, cuando se usa una app identificadores de usuarios o de dispositivos y otra información de la actividad en apps. En un registro se puede permitir o rechazar una solicitud de una app para acceder a todos los registros del dispositivo.

Interfaz

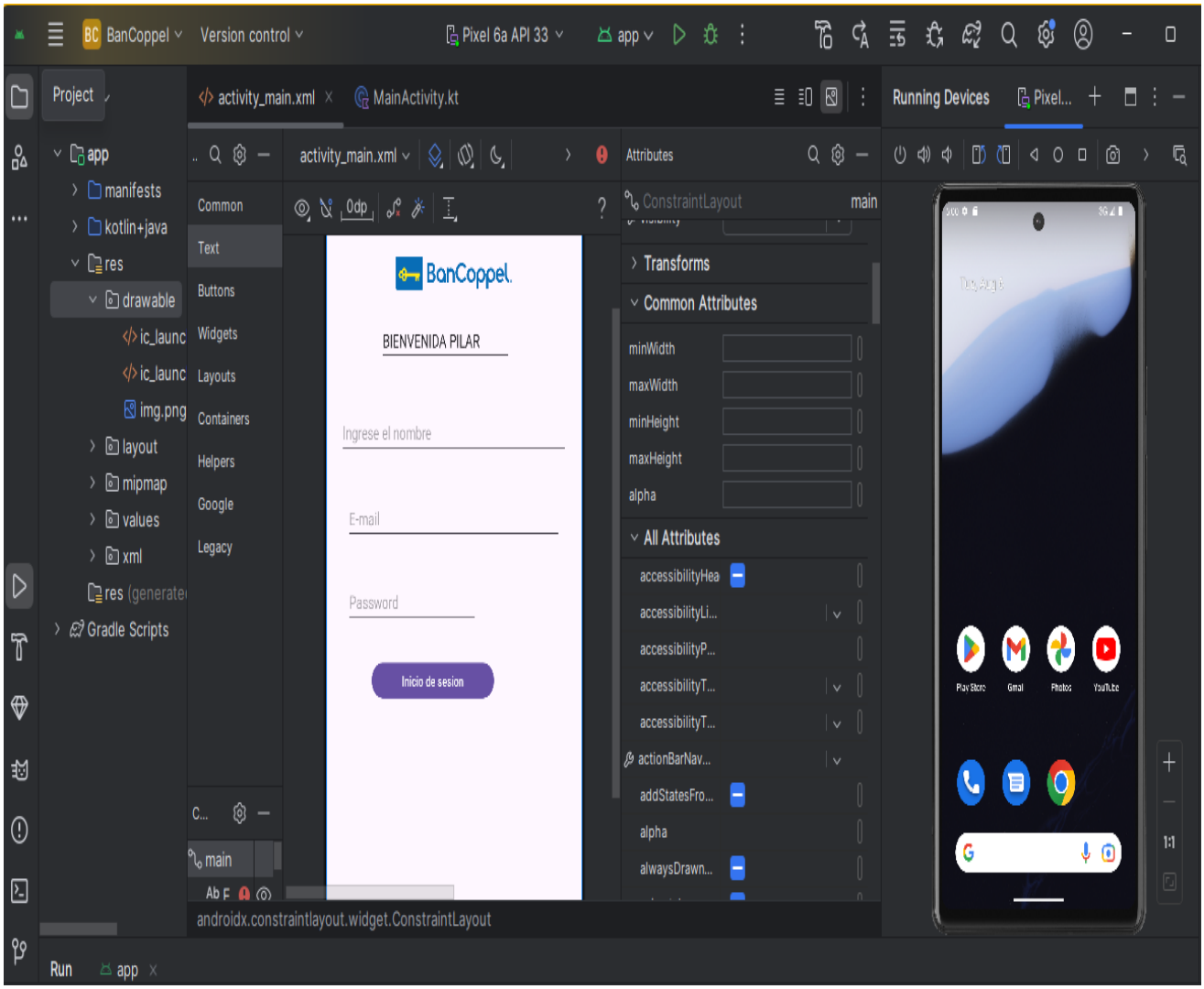
Primero vamos a crear nuestro proyecto en Android Studio para ello lo abrimos y seleccionamos la opción Empty Views Activity.



Una vez creado nuestro proyecto se abrirá la pantalla principal analizaremos la interfaz activity_main.xml que viene por defecto y procederemos a modificarla para darle la apariencia de la interfaz

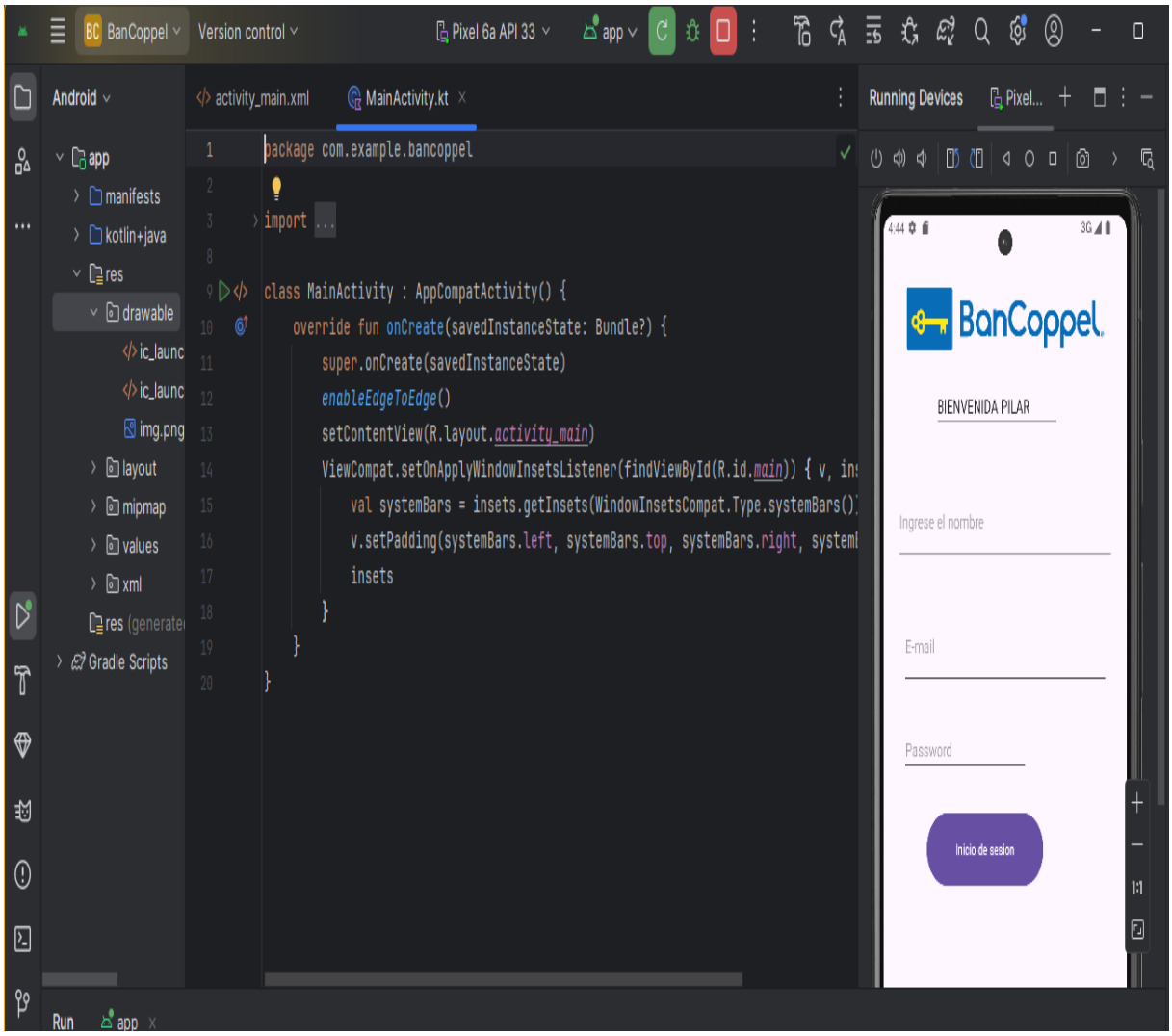


Ahora vamos a crear los correspondientes para el mensaje de bienvenida y el registro de usuario.



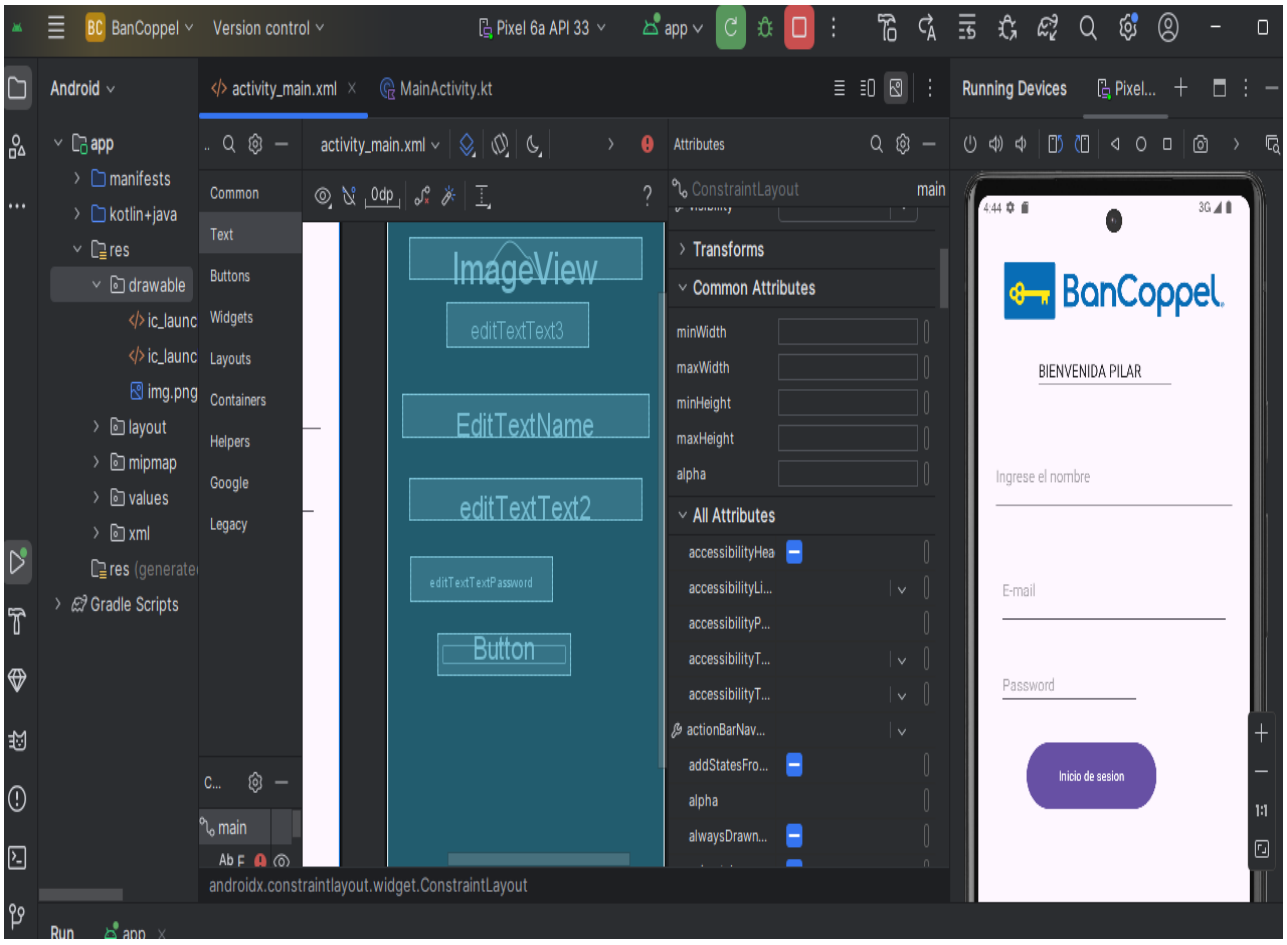
Codificación

Ahora que tenemos lista toda la interfaz de nuestra aplicación procederemos a analizar el código generado por nuestro Login Activity.

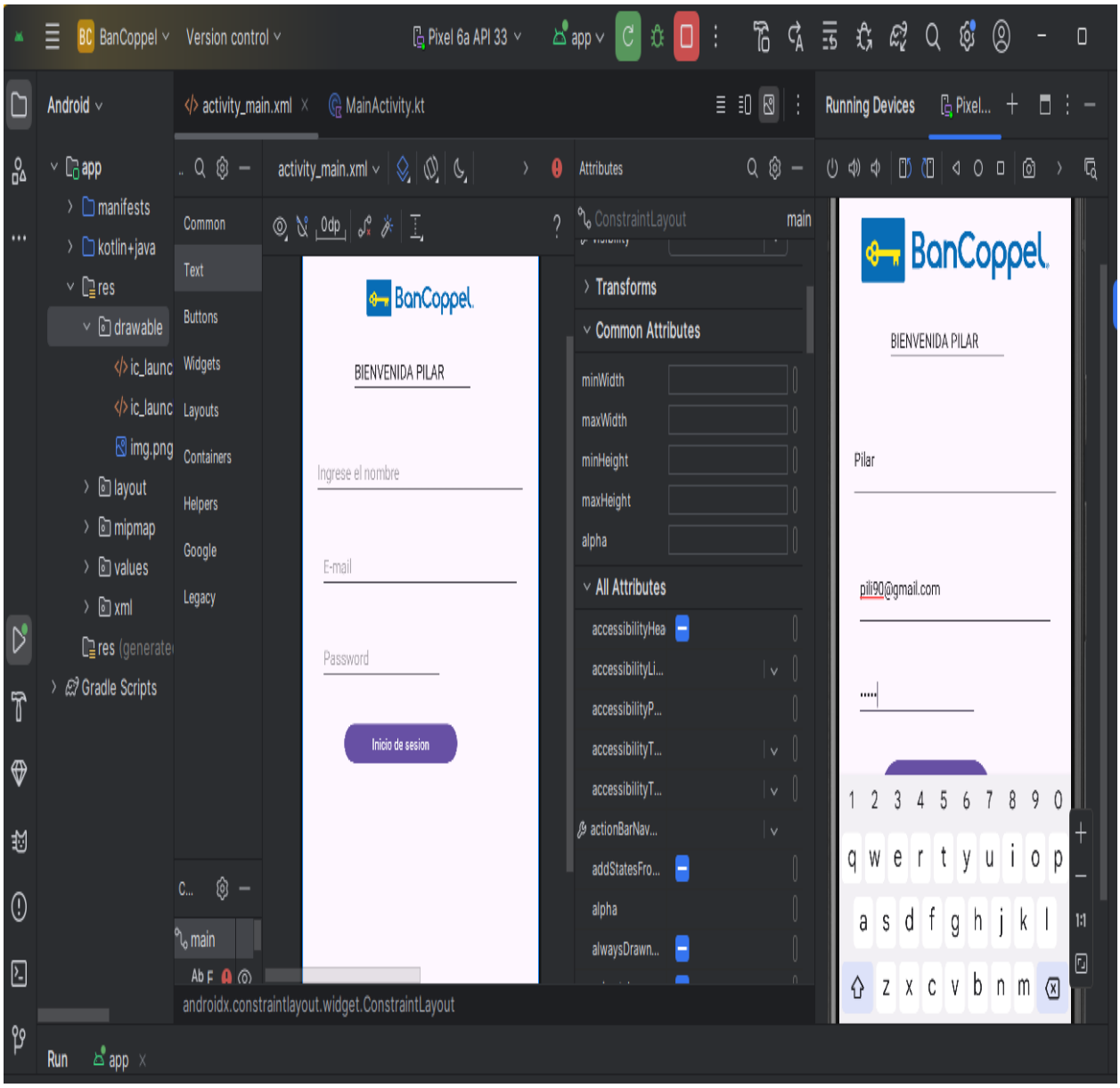


Prueba de la aplicación

En la siguiente imagen aremos la prueba de la aplicación una vez terminada y utilizando los elementos necesarios. Veremos el funcionamiento de la aplicación



En la Siguiente imagen podemos ver como nuestra aplicación fue creada utilizando Buttons para el inicio de sesión, también podemos ver cómo se puede ingresar el nombre, E_mail y el Password.



Conclusión

¿Porque se debería utilizar una aplicación de autenticación? Los expertos recomiendan utilizar MFA en cada cuenta que esté disponible para aumentar la seguridad y proteger mejor los datos personales. Las aplicaciones de autenticación son una forma gratuita, sencilla y segura de utilizar la MFA, y la mayoría de las cuentas con ajuste de seguridad la ofrecen como opción. Estas aplicaciones funcionan en función del modelo de verificación TOTP, el servidor de la cuenta creará un código QR que la aplicación de la autenticación escaneará. El código QR contiene un algoritmo secreto que utiliza la hora actual como factor para generar códigos TOTP. La aplicación de autenticación y el servidor de la cuenta serán los únicos en conocer el algoritmo secreto para generar los mismos códigos exactos al mismo tiempo, en la vida diaria cuando el usuario inicie sesión, introducirá el código que se muestra en la aplicación de autenticación, el servidor comprobará si el código introducido coincide con el código que generó. Si los códigos coinciden, el usuario tendrá acceso, de lo contrario, el acceso le será denegado.

Es poco probable que las aplicaciones de autenticación se vean comprometidas, pero ahí algunos casos raros en los que podrían estarlo, los códigos pueden ser robados cuando un hacker obtiene acceso a la aplicación en su dispositivo. Eso significa que, en el caso de que tenga una aplicación de autenticación independiente, un hacker que consiga robar y hackear un dispositivo físico podría acceder a sus códigos, en teoría, si un cibercriminal robase el propio código QR y, por lo tanto, el algoritmo secreto, podría hackear sus cuentas.

Referencia

Vault. https://www.keepersecurity.com/

Android Developers. (s. f.). Android Mobile App Developer Tools – Android Developers.

https://developer.android.com/

Google Help. (s. f.-b). https://support.google.com/

Link

Google Drive

GitHub