

Actividad 1 – Prototipo y librerías biométricas de Android

Desarrollo de aplicaciones biométricas

Ingeniería en Desarrollo de Software

Tutor:

Marco Alonso Rodríguez Tapia

Alumno:

Alejandro Abarca Gerónimo

Fecha:

27 de enero de 2025

Índice

Introducción	3
Descripción	4
Justificación	5
Desarrollo	5
Diseño de prototipo	7
Conclusión	9
Referencias bibliográficas	9

Introducción

La autenticación biométrica es una tecnología utilizada en el proceso de verificación de identidad digital que se basa en las características físicas o el comportamiento único de cada persona. Dichas funciones se utilizan para verificar la identidad de una persona, lo que garantiza un nivel de seguridad muy alto a diferencia de las contraseñas o pin tradicionales, que pueden olvidarse, robarse o descifrarse, los datos biométricos son extremadamente difíciles de copiar o falsificar.

Existen varios tipos de autenticación por biometría, y cada uno de ellos se basa en un conjunto diferente de características personales diferentes.

- **Reconocimiento facial**

Este tipo utiliza la geometría facial y las características únicas, como la forma de los ojos, la nariz y la boca, para confirmar la identidad de una persona.

- **Huella dactilar**

Los sensores utilizan tecnología avanzada para capturar y comparar estos patrones con los que se han registrado previamente.

- **Reconocimiento del iris**

Esta tipología se basa en el reconocimiento de la estructura única del iris del ojo, y proporciona una autenticación extremadamente precisa.

- **Reconocimiento de la voz**

El reconocimiento de la voz se centra en las características únicas del habla de una persona, como la tonalidad, el ritmo y la pronunciación.

- **Reconocimiento de las venas de la mano**

También conocida como biometría vascular, esta tipología puede sonar un poco extraña, ya que utiliza la distribución única de las venas o en el dorso de la palma de la mano para verificar la identidad de una persona. Se trata de una técnica altamente segura y difícil de falsificar.

- **Reconocimiento de patrones de comportamiento**

Esta tipología está basada en determinados patrones de comportamiento, como la forma en que una persona escribe en un teclado, su estilo de navegación en la web o el ritmo y la forma en que camina, el sistema la identifica simplemente con acciones que está llevando a cabo de forma cotidiana.

Algunas librerías a utilizar:

1. BiometricPrompt: está disponible a partir de Android 9 (API 28), Google proporciona la clase BiometricPrompt como parte de la biblioteca de Jetpack, lo que facilita la integración de autenticación biométrica (huella dactilar, reconocimiento facial, etc.) sin tener que manejar directamente el hardware.
2. OpenCV: OpenCV es una librería muy popular para procesamiento de imágenes que puedes utilizar para crear tus propios algoritmos de biometría, como reconocimiento facial, detección de huellas dactilares, entre otros.

Descripción

Durante el desarrollo de la actividad utilizaremos el software Figma para la elaboración del prototipo de una aplicación móvil la cual será con un diseño biométrico para acceder a la pantalla de inicio. De acuerdo a lo anterior se procederá a utilizar las librerías de Android Studio, las cuales facilitaran el desarrollo de la aplicación de forma biométrica.

Desarrollo de la actividad 1:

Realizar un prototipo para la interfaz de la aplicación móvil con dos pantallas de muestra, la primer pantalla solicitara el dato biométrico y la segunda pantalla será de inicio una vez capturada la información del dato biométrico que se haya utilizado.

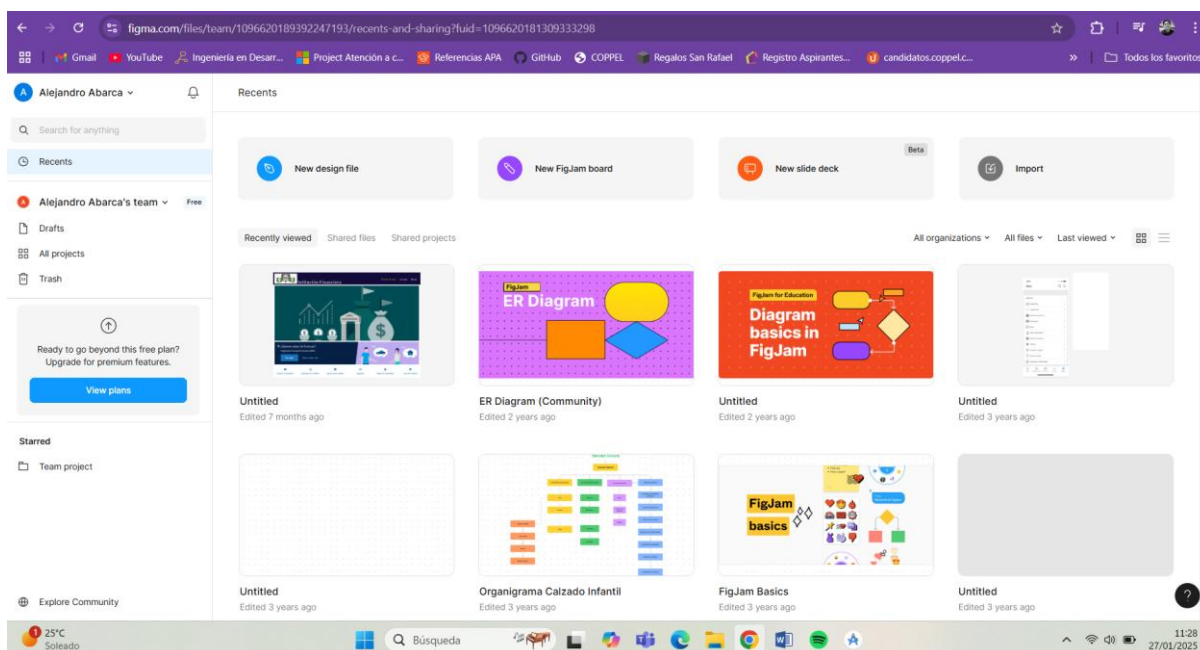
Justificación

La amplia aceptación y aplicación de la biometría aporta muchos beneficios tanto en el ámbito personal como en empresas al tener un mejor manejo y control de personal y acceso de los mismos en diferentes áreas.

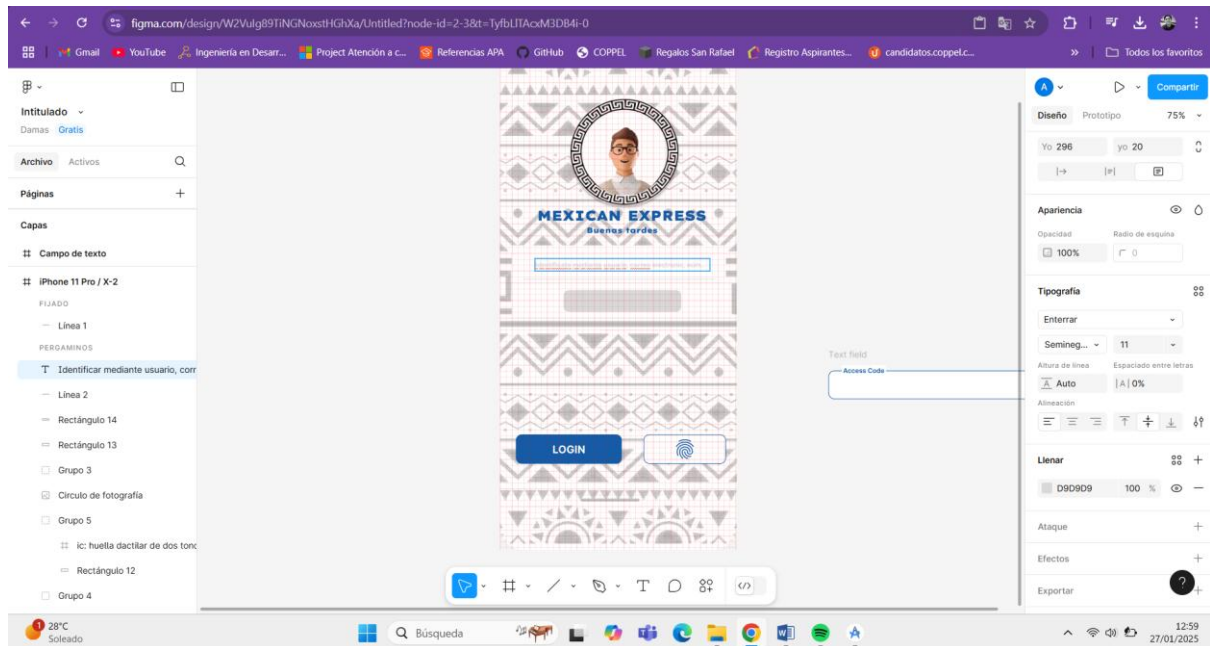
Proporciona mayor seguridad ya que la autenticación biométrica es prácticamente imposible de robar o falsificar, lo que la hace altamente segura y cómoda para los usuarios ya que no necesitan recordar contraseñas complicadas ni llevar tarjetas de identificación física. La autenticación biométrica es rápida y conveniente así como eficiente al ofrecer un tipo de autenticación más rápida y capaz de agilizar los procesos de verificación. En aplicaciones como el acceso a dispositivos móviles, ahorra tiempo y mejora la experiencia del usuario. Reduce de manera considerable el fraude y ayuda a prevenir el robo de identidad.

Desarrollo

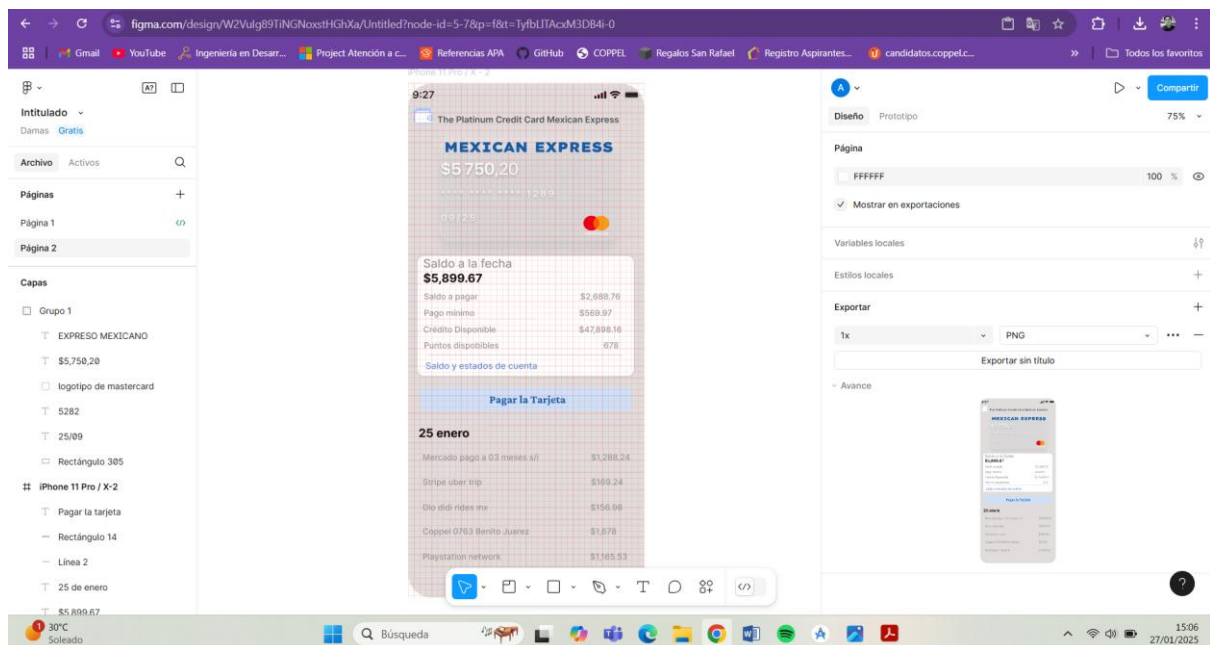
Para iniciar la elaboración de nuestro prototipo nos registramos en la página oficial de Figma.



Realizamos la búsqueda de una plantilla para poder visualizar y ejecutar el desarrollo del prototipo, visualizando así cada detalle y características de los elementos utilizados.

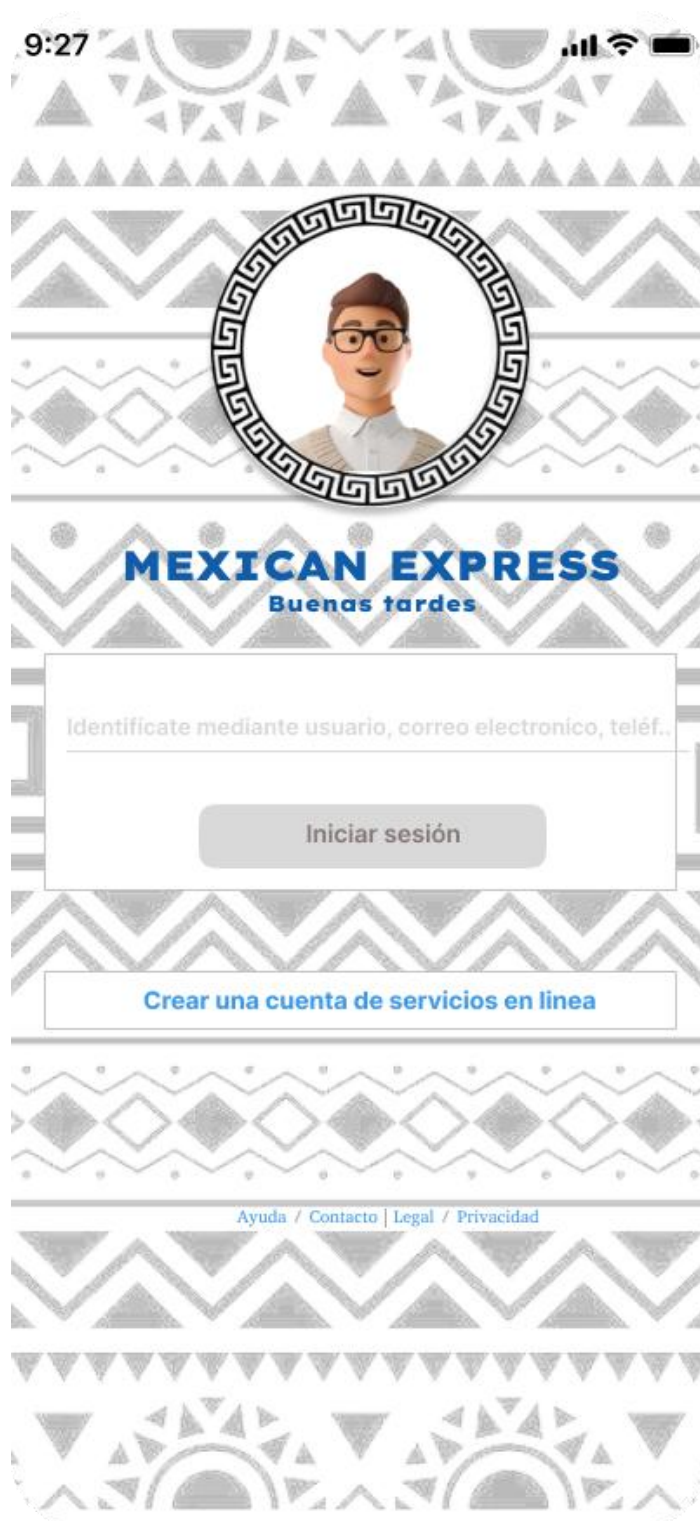


En esta captura se está trabajando en la elaboración de la segunda pantalla y se pueden ver los tipos de elementos utilizados.

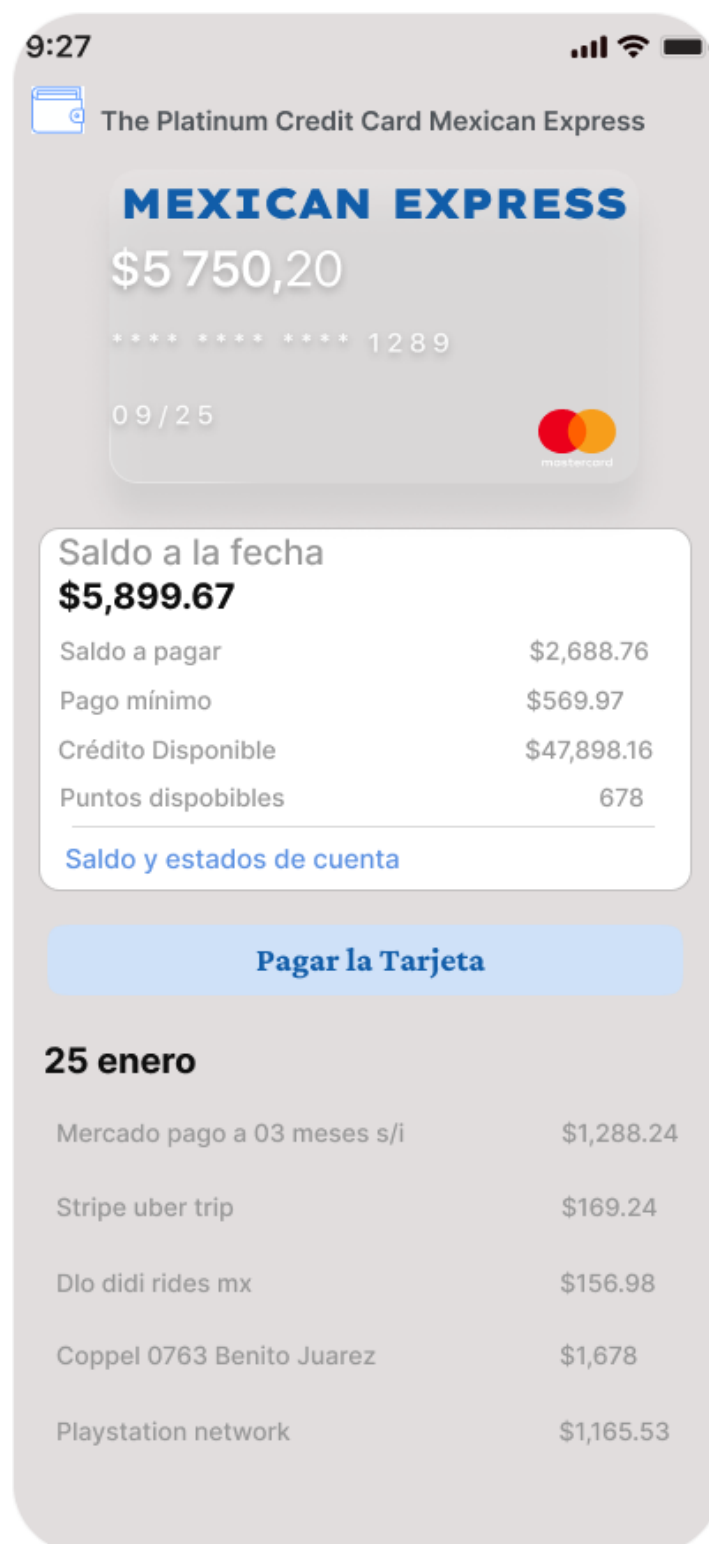


Diseño de prototipo

Pantalla 1 para el acceso a la aplicación bancaria mediante huella digital o Face Id, estos dos son los metodos mas utilizados para la verificación de identidad hasta el momento.



Pantalla 2, esta segunda pantalla mostrará el acceso una vez que haya sido aprobado exitosamente. Ambas pantallas estarán conectadas entre sí para mostrar el resultado final al usuario.



Conclusión

El desarrollo de aplicaciones biométricas ha tenido un impacto significativo en diversas industrias al mejorar la seguridad, la eficiencia y la experiencia del usuario. Tecnologías como el reconocimiento facial, la huella dactilar, el escaneo del iris y la voz, han permitido la creación de sistemas más confiables para la autenticación y la protección de datos personales.

Sin embargo, este desarrollo también ha planteado desafíos en términos de privacidad y ética, dado que la recopilación de datos biométricos puede generar preocupaciones sobre el uso indebido de dicha información. Además, la precisión y la seguridad de los sistemas biométricos deben seguir evolucionando para reducir el riesgo de errores o vulnerabilidades.

El futuro de las aplicaciones biométricas promete ofrecer soluciones más avanzadas y accesibles, pero es fundamental garantizar que se implementen con medidas adecuadas de protección de la privacidad y con un enfoque ético que respete los derechos de los usuarios.

Referencias bibliográficas

1. Mitek. (2023, 19 diciembre). Autenticación biométrica: qué es, beneficios y aplicaciones - Mitek Systems. *Mitek*. Recuperado 23 de enero de 2025, de <https://www.miteksystems.com/es/blog/biometria-que-es-aplicaciones>