Universidad Corporativa | Programas Académicos | Ingeniería en Desarrollo de Software

Actividad 3 – Codificación de la aplicación de lector de huella

Desarrollo de aplicaciones biométricas

Ingeniería en Desarrollo de Software

Tutor:

Marco Alonso Rodríguez Tapia

Alumno:

Alejandro Abarca Gerónimo

Fecha:

03 de febrero de 2025

Indice

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.

El diseño para la autenticación biométrica requiere una cuidadosa consideración del contexto, las expectativas y las preferencias del usuario. A la hora de tomar decisiones, los diseñadores deben evaluar las compensaciones y los beneficios de cada modalidad biométrica y ofrecer opciones o alternativas al usuario. También es importante proporcionar comentarios claros y coherentes al usuario sobre el estado y el resultado de la autenticación, mediante iconos, colores, sonidos o vibraciones.

La autenticación biométrica no está exenta de desafíos y limitaciones. Ya que los datos biométricos son confidenciales y personales, es por esto que los diseñadores deben asegurarse de que se almacenen y transmitan de forma segura y que el usuario tenga control sobre sus datos y dé su consentimiento para su uso.

Descripción

Realizar la programación de la aplicación que desarrollamos durante la actividad 1 y 2 para que funcione al iniciar sesión con las huellas dactilares previamente registradas en el teléfono. La interfaz de la app deberá contar con dos pantallas:

1. Pantalla de inicio de sesión.
2. Pantalla de bienvenida.

La aplicación deberá realizar las siguientes funciones:

- Cuando se ingrese una huella dactilar que no esté registrada, deberá mostrar un ícono que represente un escaneo fallido, acompañado de un mensaje de error que diga lo siguiente: “Escaneo fallido, huella dactilar no registrada”.
- Cuando se ingrese la huella correcta, se deberá mostrar un ícono que represente un escaneo exitoso, acompañado del siguiente mensaje: “¡Escaneo de huella dactilar exitoso! Iniciando sesión…”
- Una vez confirmada la huella digital correcta, deberá pasar a la segunda pantalla de bienvenida.

Realizar la codificación de la aplicación que se ha realizado desde la Actividad 1 y 2. Generar los métodos necesarios para la ejecución, así como los mensajes que se mostrarán dependiendo de la huella digital que se escanee. Además, programar la aplicación para que permita acceder a la pantalla de bienvenida cuando se escanee la huella digital correcta.

Justificación

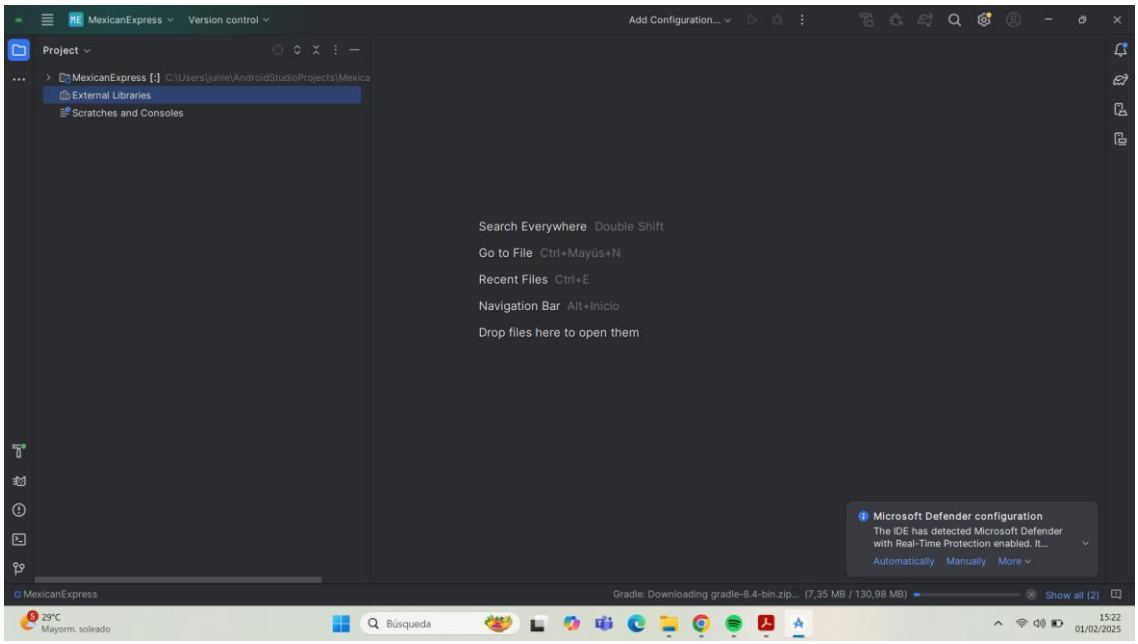
La amplia aceptación y aplicación de la biometría aporta muchos beneficios tanto en el ámbito personal como en empresas al tener un mejor manejo y control de personal y acceso de los mismos en diferentes áreas. Proporciona mayor seguridad ya que la autenticación biométrica es prácticamente imposible 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 asi 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

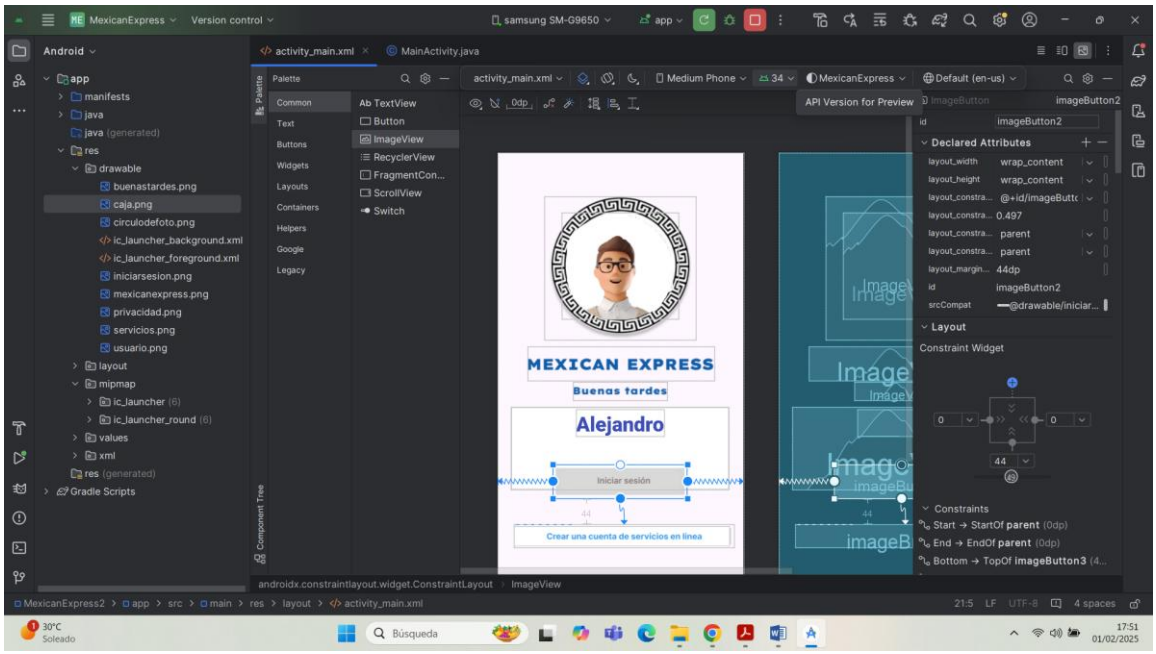
Etapa 1:

Diseño de interfaces

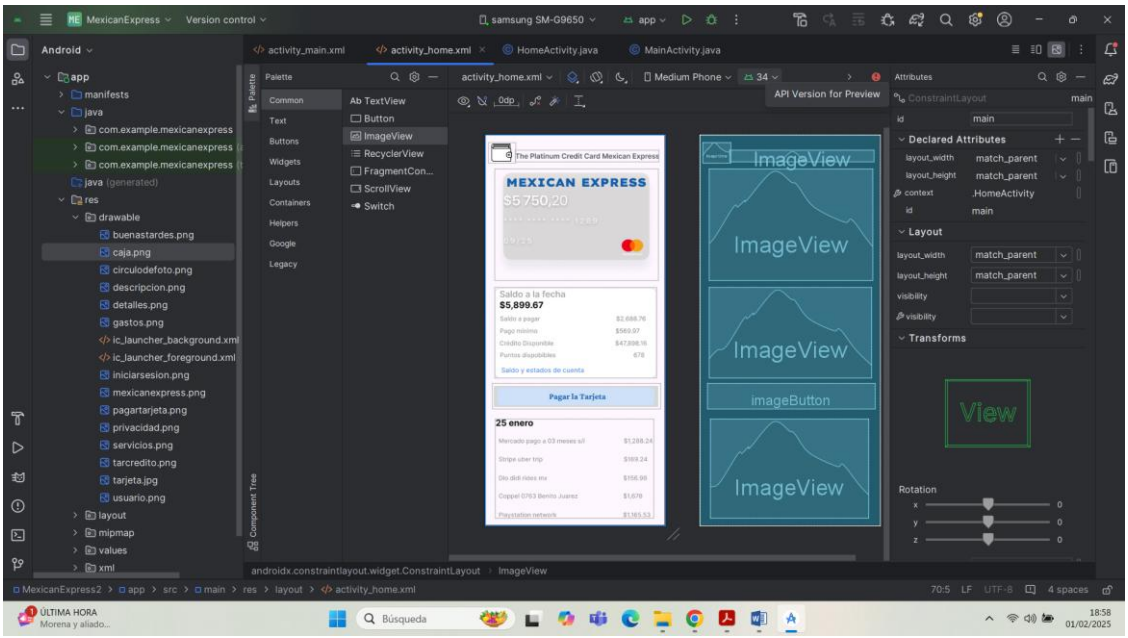
Selección del tipo de diseño en las plantillas que arroja en automático la plataforma de Android Studio.



Diseño de la pantalla principal de la aplicación para ingresar y solicitar el método biométrico de acceso a la aplicación. Se está utilizando un dispositivo físico para realizar las pruebas de la aplicación.



Elaboración de la segunda pantalla de la aplicación, se creó dentro del Main principal para poder realizar la conexión por medio del código una vez que se soliciten los datos biométricos para acceder.



Etapa 2:

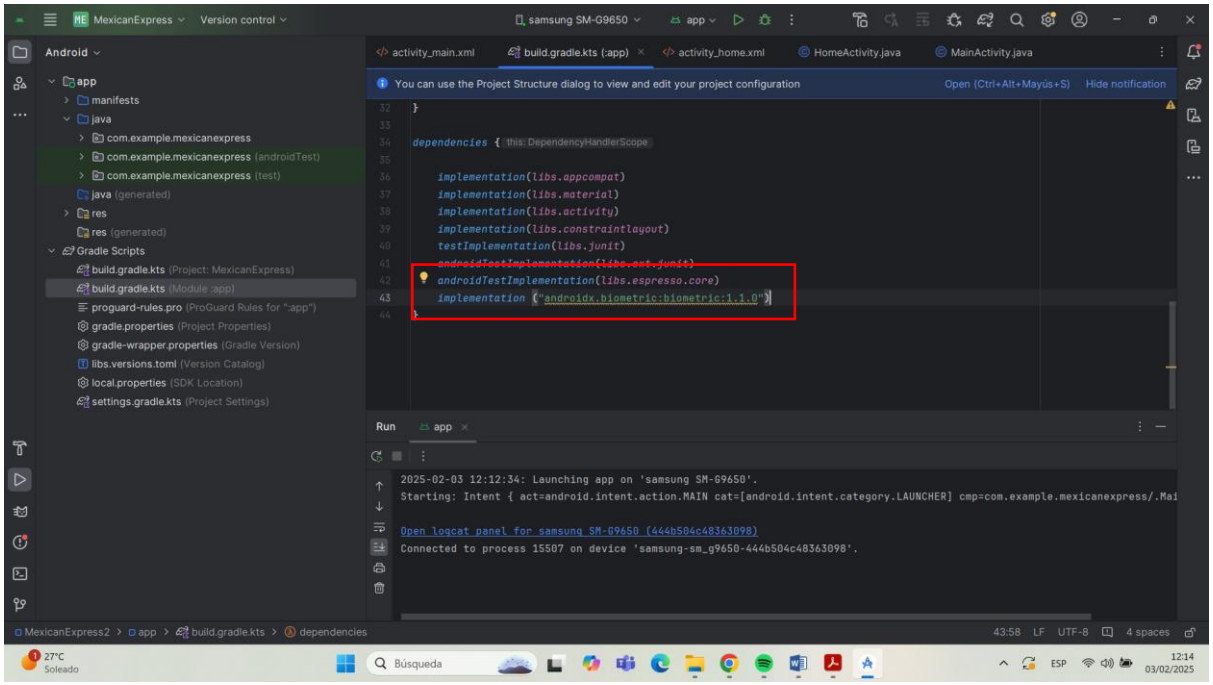
Codificación

En esta captura se muestra la implementación de la declaración para configurar el proyecto en Android Studio en el archivo build.gradle:

implementation("androidx.biometric:biometric:1.1.0")

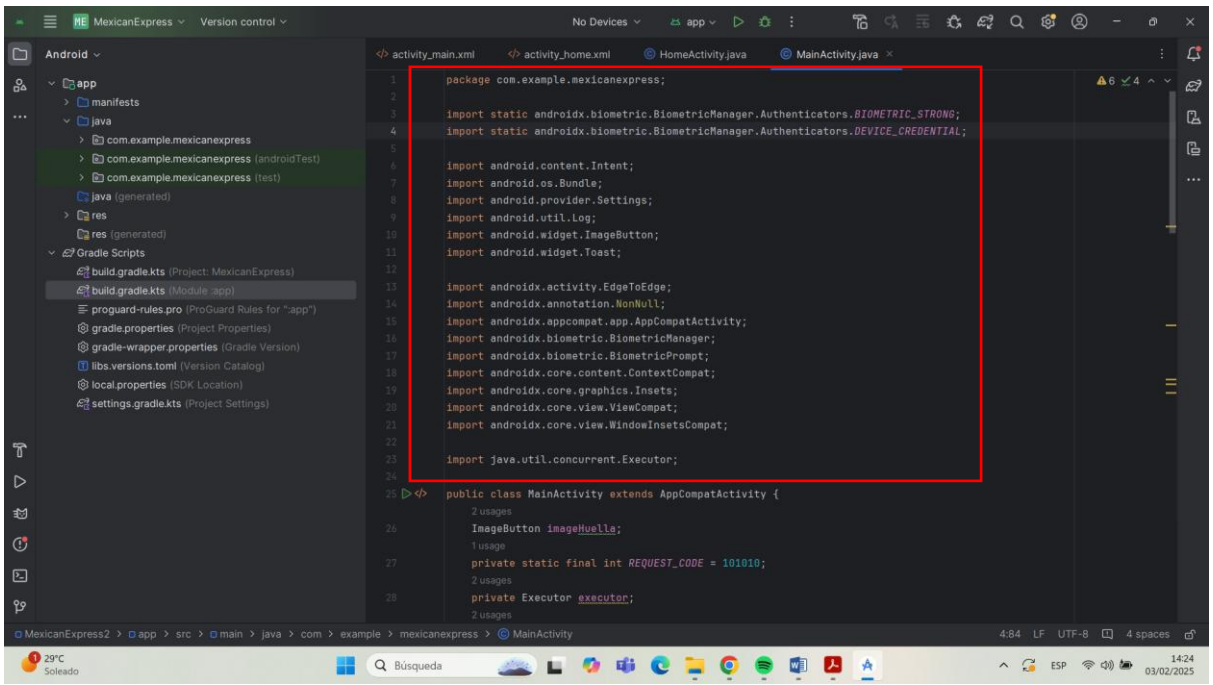
Esta biblioteca se utiliza para implementar funciones de autenticación biométrica en aplicaciones Android. Esto incluye autenticación mediante huella digital, reconocimiento facial y otras formas de biometría soportadas por el dispositivo.

La biblioteca proporciona una interfaz sencilla para integrar estas funcionalidades en tu aplicación, utilizando los servicios de biometría proporcionados por Android de manera segura y con la mejor compatibilidad.



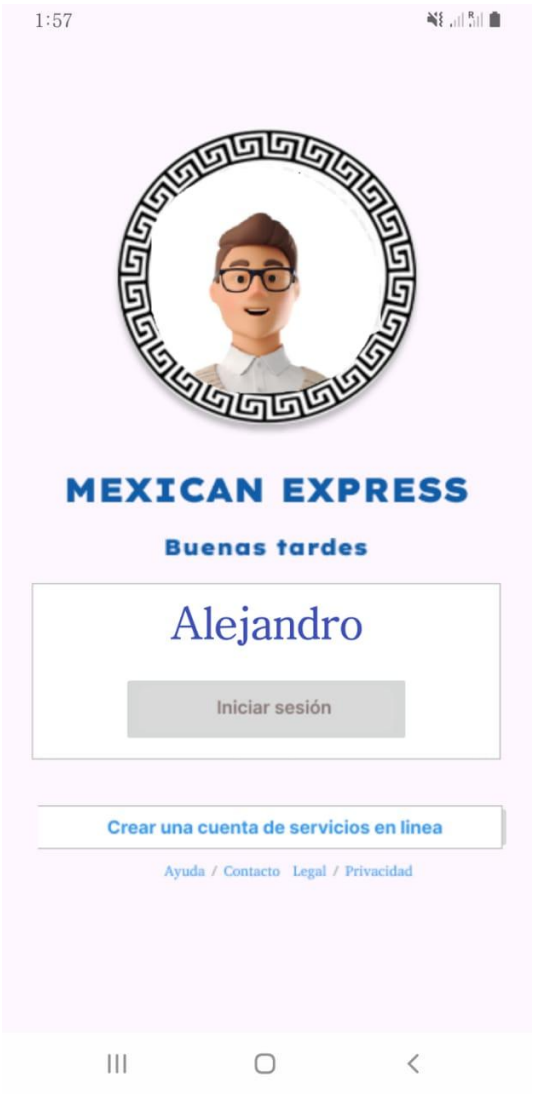
Código de la aplicación: https://github.com/SoyAlejandroAbarca/Desarrollo-de-aplicaciones-biom-tricas/blob/main/CODIGO%20APP%20MEXICAN%20EXPRESSmd

Librerías utilizadas a lo largo del desarrollo de la actividad.

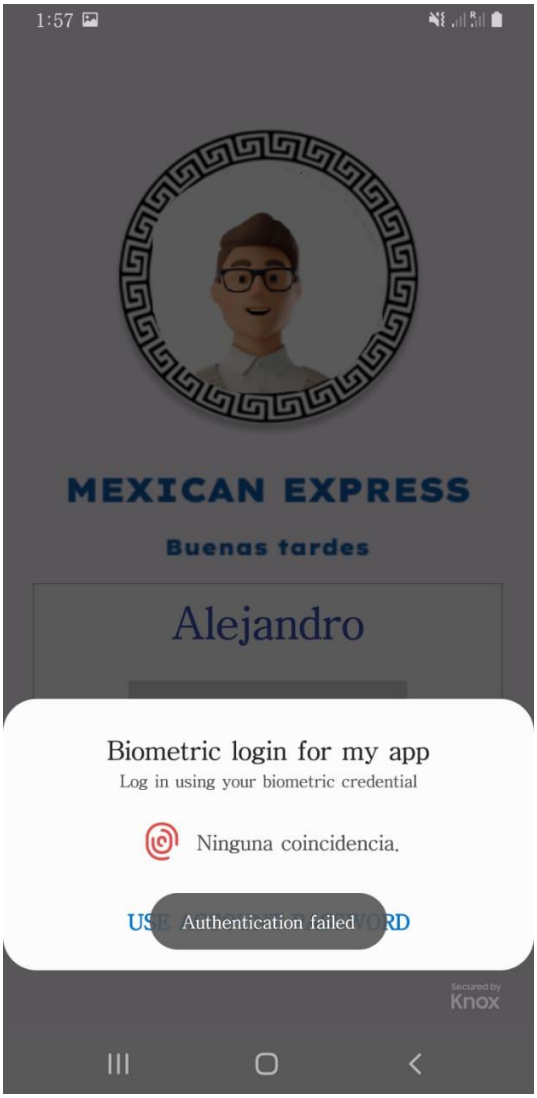


Ejecución en el teléfono

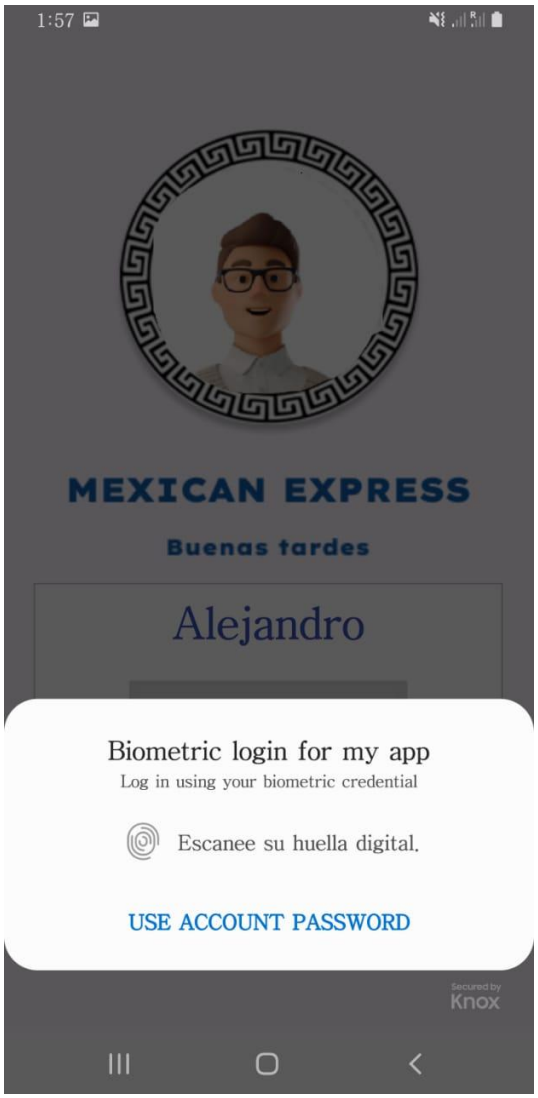
Inicio de la aplicación para verificación con biometría.



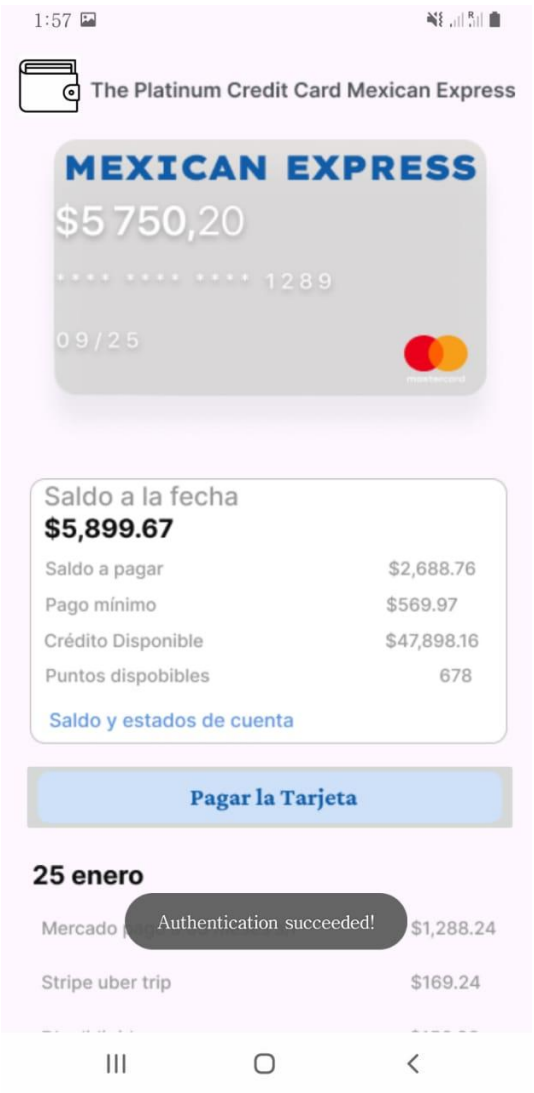
Intento de acceso con huella incorrecta.



Solicitud de huella, acceso correcto.



Segunda pantalla una vez dado el acceso.



Conclusión

El desarrollo de aplicaciones biométricas ha impactado significativamente a diversas industrias, mejorando la seguridad, la eficiencia y la experiencia del usuario. Tecnologías como el reconocimiento facial, las huellas dactilares, el escaneo del iris y la voz permiten sistemas más confiables para autenticar y proteger datos personales.

Sin embargo, este avance también plantea preocupaciones éticas y de privacidad, ya que la recopilación de datos biométricos puede generar inquietud 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 proporcionar soluciones más avanzadas y accesibles, pero es importante que garanticen la protección de la privacidad adecuadas y se implementen utilizando métodos éticos que respeten los derechos de los usuarios. Hoy en día, con tantos riesgos y amenazas que enfrentan diversas industrias, la seguridad se ha convertido en una prioridad máxima. El uso de sistemas biométricos se ha convertido en una solución cada vez más popular para mejorar la seguridad y proteger la integridad de los empleados y activos de una empresa.

La biometría se refiere al uso de características físicas únicas, como huellas dactilares, iris, voz y rostro, para verificar la identidad de una persona. Estas características no se pueden falsificar ni compartir, lo que las convierte en una herramienta de seguridad muy eficaz.

Las empresas que implementan estas tecnologías deben asegurarse de que los datos biométricos de sus empleados y usuarios estén adecuadamente protegidos mediante medidas de seguridad y privacidad efectivas.

Referencias

1. *¿Cuáles son los mejores diseños de interfaz móvil para la autenticación biométrica?* (2023, 6 noviembre). www.linkedin.com. https://www.linkedin.com/advice/0/what-best-mobile-interface-designs-biometric-authentication-uitpe?lang=es&originalSubdomain=es
2. 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