ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

CREACIÓN DE UN PROTOTIPO DE UN SISTEMA DE AUTENTICACIÓN DE DOS FACTORES UTILIZANDO ONE-TIME PASSWORD (OTP)

CREACIÓN DE UN PROTOTIPO DE APLICACIÓN MÓVIL DE UN SISTEMA DE AUTENTICACIÓN DE DOS FACTORES UTILIZANDO ONE-TIME PASSWORD, PARA DISPOSITIVOS ANDROID

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO INGENIERO EN CIENCIAS DE LA COMPUTACIÓN

ANTHONY ISRAEL ALMACHI CHASI
anthony.almachi@epn.edu.ec

DIRECTOR: PhD. SANG GUUN YOO
sang.yoo@epn.edu.ec

DMQ, enero 2023

CERTIFICACIONES

Yo, ANTHONY ISRAEL ALMACHI CHASI declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

Anthony Israel Almachi Chasi

Certifico que el presente trabajo de integración curricular fue desarrollado por ANTHONY ISRAEL ALMACHI CHASI, bajo mi supervisión.

PhD. SANG GUUN YOO
DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

ANTHONY ISRAEL ALMACHI CHASI

PhD. SANG GUUN YOO

BRAYAN ALEXIS FERNÁNDEZ GONZA

DALIANA ZAMBRANO PEREDA

HILTON BLADIMIR PILLAJO ANAGUANO

LUIS ERNESTO ALMEIDA ZAMBRANO

DEDICATORIA

Dedico este trabajo a todas las personas que me han apoyado a lo largo del transcurso de mi carrera universitaria. En especial a mi abuelo, quien siempre fue una figura de admiración. A mis padres que gracias a su apoyo incondicional y esfuerzo me han dado fuerzas de seguir adelante sin importar cuantas veces haya tropezado

Anthony Almachi

AGRADECIMIENTO

Agradezco a la Escuela Politécnica Nacional por todo el conocimiento brindado a través de sus profesores quienes me han formado y guiado profesionalmente.

Gracias a mi tutor, Sang Guun Yoo, por su paciencia y apoyo incondicional en el desarrollo y culminación del presente documento.

Gracias a mi abuelo Euclides Almachi y a mis padres Marco Almachi y Lorena Chasi quienes han depositado su confianza en mí.

Gracias en especial a mi pareja Jhael Toapanta y a mis compañeros Efer Diaz y Bladimir Pillajo por acompañarme y apoyarme en los momentos más difíciles.

ÍNDICE DE CONTENIDO

RESUMEN

El presente proyecto propone la creación de un prototipo que utilice one-time password (OTP) en un sistema de autenticación de dos factores. Para lo cual se realizó, en primera instancia, un estudio sistemático de la literatura con el objetivo de conocer los diferentes protocolos de OTP, sus principales ventajas y desventajas. Una vez hecho esto, se seleccionó el protocolo de OTP a utilizarse y se definieron los diferentes métodos de entrega del OTP al usuario. A continuación, se inició la fase desarrollo definiendo en primer lugar los requerimientos necesarios para cumplir los objetivos del presente trabajo, posteriormente se realizó un mockup de alto nivel y se seleccionaron las herramientas y frameworks necesarios para completar el prototipo (e.g. lenguajes de programación, gestor de base de datos, metodologías agiles para desarrollo de software, entre otros). Finalmente, se realizaron las pruebas de funcionamiento con el objetivo de evaluar el desempeño del prototipo detallando los criterios bajos los cuales se realizaron estas pruebas. Además de especificar el criterio de selección de individuos que se utilizó para llevar a cabo estas evaluaciones, estas pruebas se enfocaron principalmente en discernir cuál es el método de entrega preferido por los usuarios finales.

PALABRAS CLAVE: Autenticación de dos factores, One-Time Password, (OTP), Desarrollo de software, Metodologías agiles.

ABSTRACT

This project proposes the creation of a prototype that uses one-time password (OTP) in a two-factor authentication system. For this purpose, a systematic study of the literature was performed in order to know the different OTP protocols, their main advantages and disadvantages. Once this was done, the OTP protocol to be used was selected and the different methods of delivering the OTP to the user were defined. Next, the development phase began by first defining the requirements needed to meet the objectives of this work, then a high-level mockup was made, and the tools and frameworks needed to complete the prototype were selected (programming languages, database manager, agile methodologies for software development, among others). Finally, tests were performed with the objective of evaluating the performance of the prototype detailing the criteria under which these tests were performed. In addition, we specified the selection criteria of individuals that were used to perform these evaluations. These tests were mainly focused on discerning which is the delivery method preferred by end users.

KEYWORDS: Two-factor authentication, One-Time Password, (OTP), Software development, Agile methodologies.

1 INTRODUCCIÓN

1.1 Descripción del proyecto

El presente trabajo busca recrear un sistema de doble factor de autenticación. El primer factor de autenticación está basado en el uso de contraseñas, mientras que para el segundo factor de autenticación se utilizaron contraseñas de un solo uso, por sus siglas en ingles One-Time Password (OTP). En la Figura 1, se muestra la arquitectura completa del sistema de doble factor de autenticación propuesta.

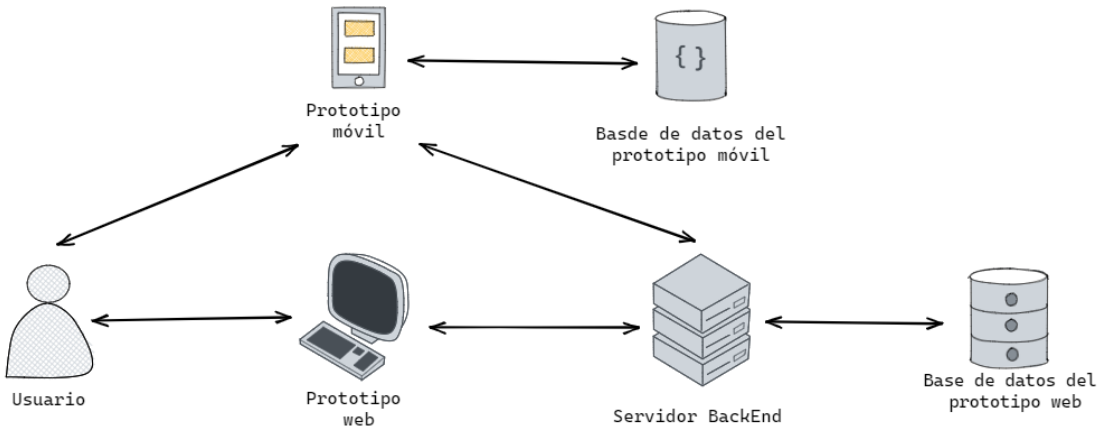


Figura 1. Arquitectura completa del sistema de doble factor de autenticación

El funcionamiento del sistema se representa en cuatro fases, las cuales se listan a continuación:

- Fase de creación de una cuenta en el prototipo web desarrollado por los colaboradores. Para la primera fase el usuario debe acceder a la sección de crear cuenta en el prototipo web completar los siguientes pasos: (1) el usuario completa el formulario de registro en el prototipo web proporcionando un nombre de usuario y contraseña, (2) el prototipo web envía los datos proporcionados por el usuario a su servidor backend, (3) el servidor verifica que la información del usuario sea válida y lo envía a su servicio de base de datos para ser almacenada, (4) la base de datos del prototipo web almacena los datos relacionados con la cuenta del usuario, (5) la base de datos notifica al servidor backend que los datos del usuario se han guardado exitosamente, (6) el servidor verifica que la creación de la cuenta del usuario se ha creado exitosamente, (7) finalmente, se muestra al usuario la interfaz de inicio en el prototipo web.

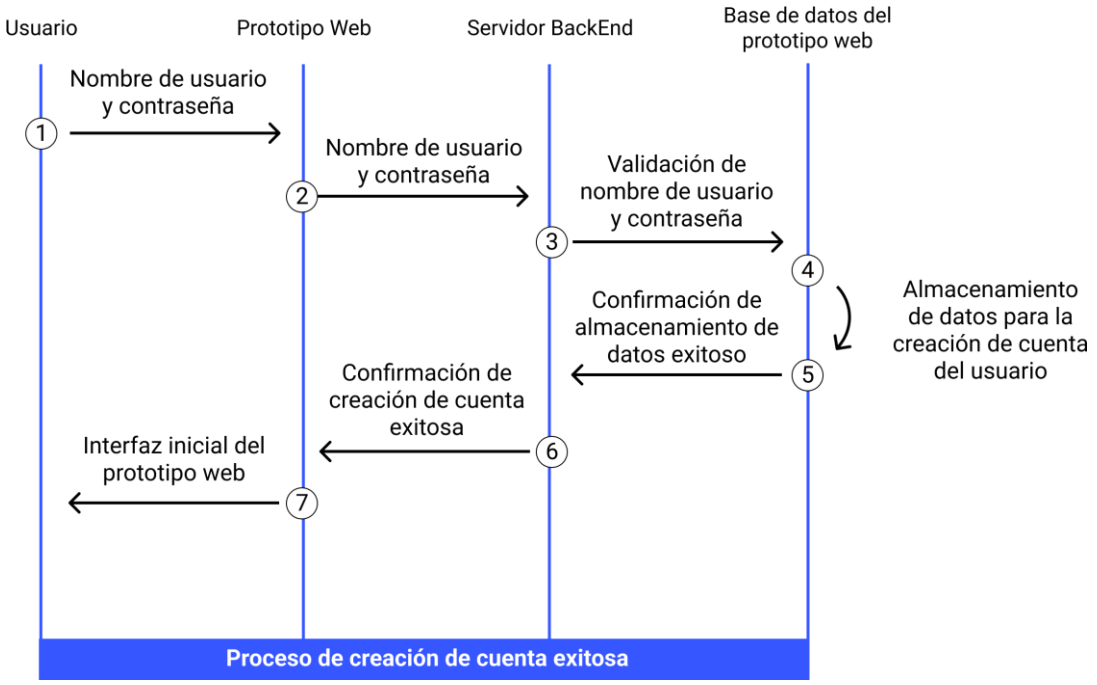


Figura 2. Proceso de creación de cuenta exitoso

- Posteriormente el usuario activará el doble factor de autenticación o por sus siglas en ingles Two-Factor Authentication (2FA) dentro del prototipo web. Para ello el usuario deberá completar los siguientes pasos: (1) el usuario realizará la solicitud de activación del doble factor de autenticación en el prototipo web. (2) el prototipo web enviará esta solicitud al servidor backend, (3) el servidor procesará la solicitud, (4) el servidor, además, indicará al prototipo web que se ha iniciado el proceso de activación del doble factor de autenticación, (5) el prototipo web presenta al usuario el formulario de activación del (2FA), (6) el usuario completará el formulario de activación del 2FA seleccionando el tipo de OTP que utilizará como segundo factor de autenticación y seleccionará el método de entrega por el cual desea recibir el OTP, habiendo completado este formulario, el usuario lo enviará al prototipo web, (7) el prototipo web enviará el formulario completo al backend, (8) el servidor backend validará la información proporcionada por el usuario y la enviará al servicio de base de datos, (9) el servicio de base de datos almacenará la nueva configuración de la cuenta del usuario, (10) la base de datos notificara al backend la actualización exitosa de la configuración de la cuenta del usuario, (11) el backend validará la activación del 2FA y notificará al prototipo web, (12) el prototipo web presentará al usuario un código QR que contendrá la información necesaria para poder registrar al prototipo web en el prototipo móvil.

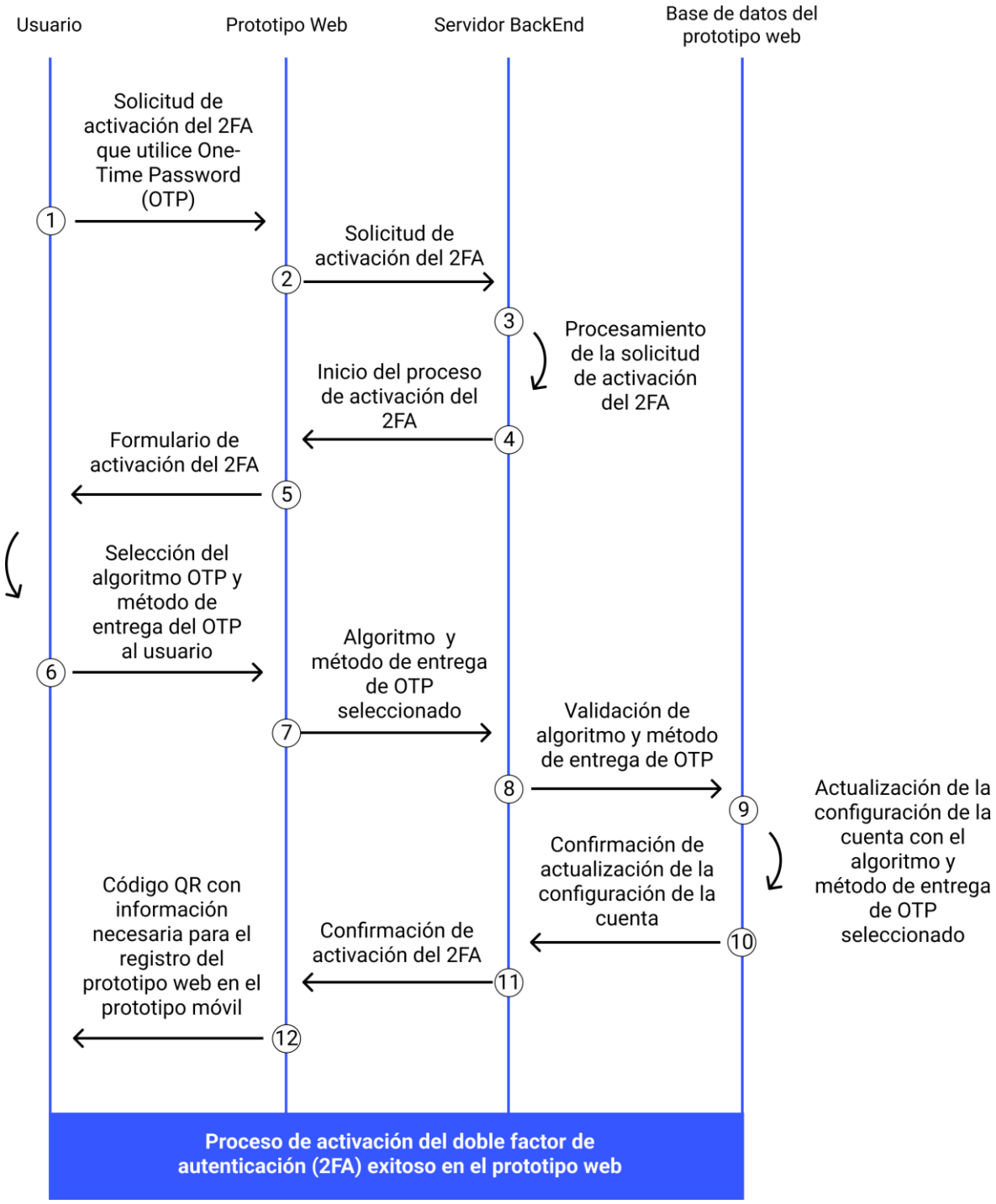


Figura 3. Proceso de activación exitoso del doble factor de autenticación (2FA) en el prototipo web

- En la siguiente fase, el prototipo móvil debe escanear el código QR generado en la fase anterior. Obteniendo así, la información que este contiene y realizando el proceso de registro de la aplicación web en el prototipo móvil, para lo cual se deben cumplir los siguientes pasos: (1) el código QR que contiene información acerca del prototipo web y del usuario es presentado a este como resultado de la finalización

del proceso de activación del 2FA, (2) el usuario escanea este código QR con el prototipo móvil, (3) el prototipo móvil envía esta información a su respectivo servicio de base de datos para ser almacenada, (4) la base de datos almacena el registro del prototipo web, (5) la base de datos además, notifica al prototipo móvil el registro exitoso del prototipo web, (6) el prototipo móvil muestra en su interfaz, en forma de lista, la información del prototipo web registrado.

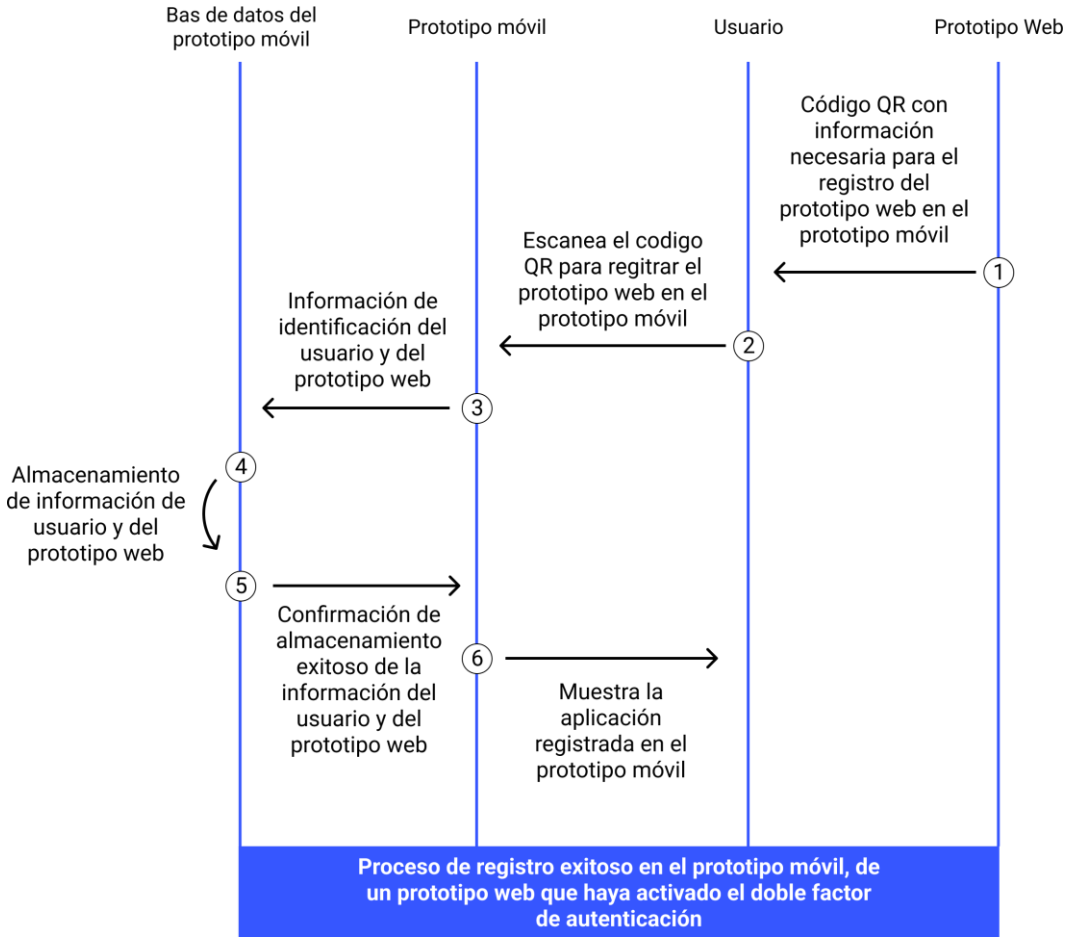


Figura 4. Proceso de registro exitoso en el prototipo móvil, de un prototipo web que ha activado el doble factor de autenticación (2FA)

- En la fase final, una vez se haya completado las fases anteriores. La siguiente vez que el usuario inicie sesión en el prototipo web, este enviará el OTP por el método de entrega seleccionado y el usuario deberá enviar el valor del OTP a través del prototipo móvil para poder autenticarse, para ello los siguientes pasos deben cumplirse: (1) el usuario intenta iniciar sesión en el prototipo web y envía su nombre de usuario y contraseña, (2) el prototipo web envía la información proporcionada por el usuario al servidor backend, (3) le servidor valida la información proporcionada por el usuario, (4) en el caso de que dichas credenciales sean auténticas el servidor backend genera un OTP, (5) el servidor backend se encarga

de enviar este OTP al usuario mediante el método de entrega previamente seleccionado por este, (6) el usuario ingresa el valor del OTP en el prototipo móvil, (7) el prototipo móvil, se encarga de enviar el OTP al servidor backend para su verificación, (8) el servidor comprueba que el valor del OTP sea el correcto, (9) en el caso de que el valor del OTP sea el correcto el servidor concede al usuario el acceso al prototipo web.

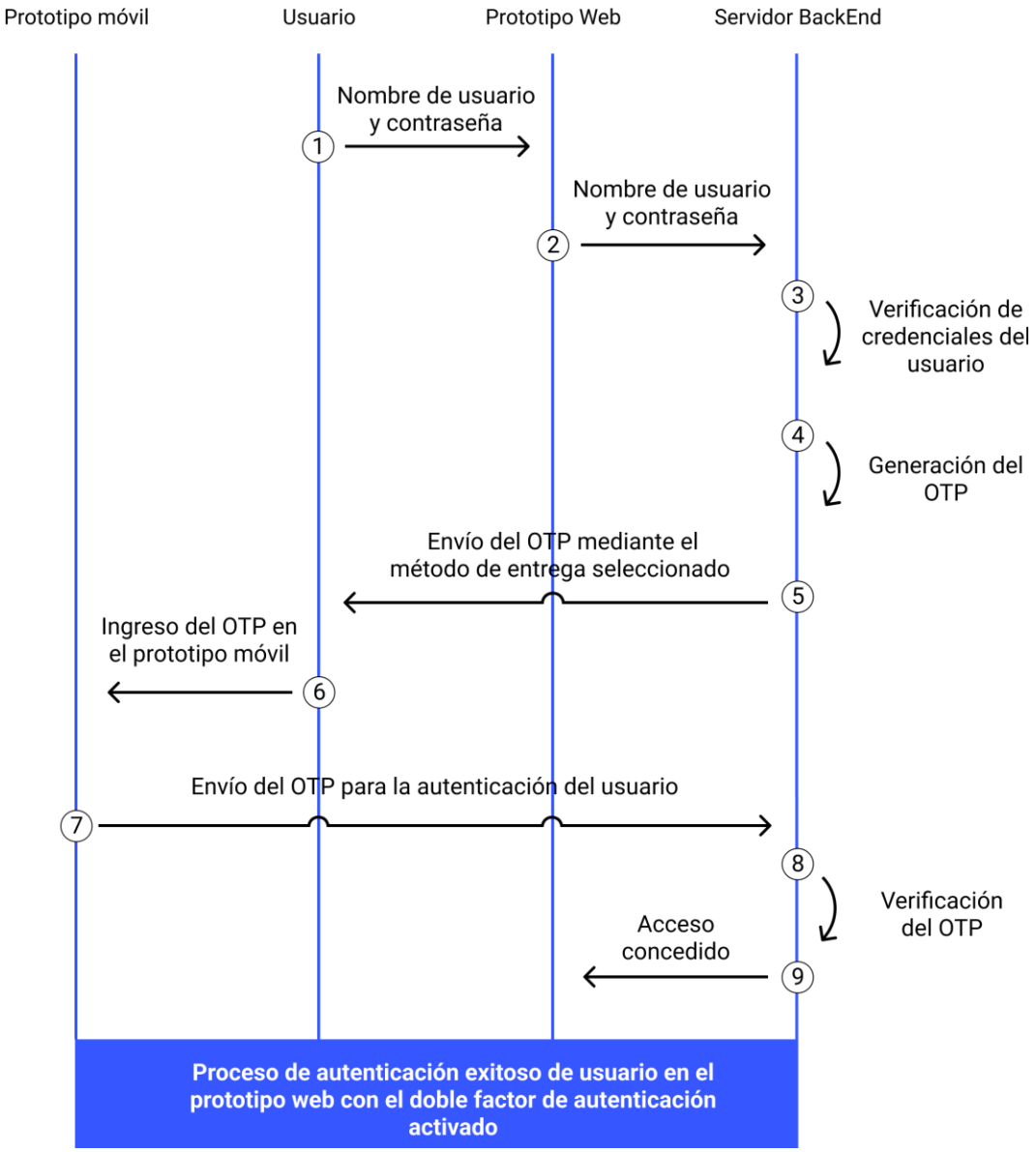


Figura 5. Proceso de autenticación exitoso de un usuario en el prototipo web con el doble factor de autenticación (2FA) activado

1.2 Descripción del componente

De la descripción completa del sistema, mencionada en la sección anterior. La parte que le compete al presente componente se muestra en la Figura 6.

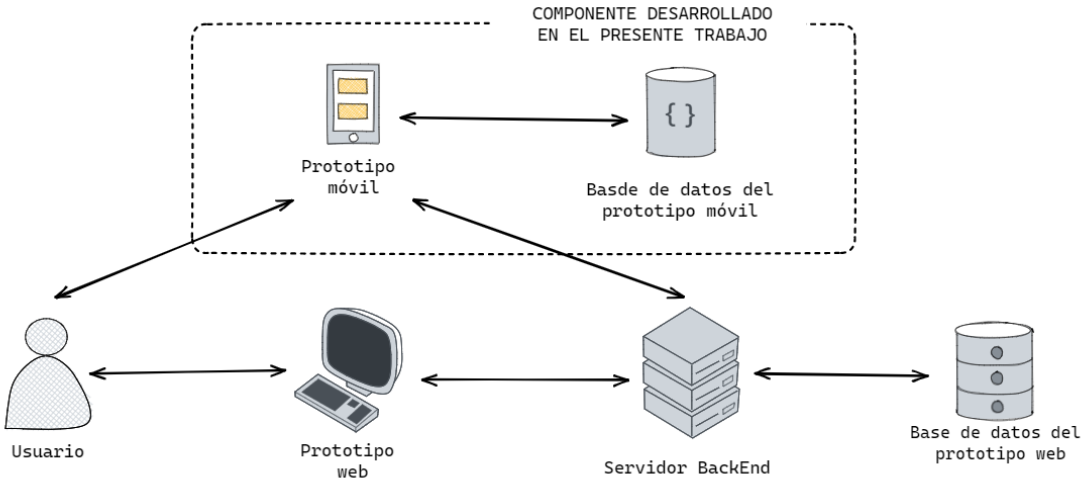


Figura 6. Parte del sistema de doble factor de autenticación que se desarrolló en el presente trabajo

Para el desarrollo de este componente se ejecutaron seis fases: (1) estudio de literatura para entender el estado del arte relacionado a las contraseñas de un solo uso o OTP (por sus siglas en ingles de One-Time Password), (2) definición de los métodos de entrega con los que el prototipo móvil debe ser compatible (3) análisis y diseño del prototipo de aplicación móvil, (4) implementación del prototipo móvil para dispositivos Android, (5) pruebas del prototipo y (6) documentación.

La primera fase se llevó a cabo con la definición de la pregunta de investigación: ¿Qué tipos de contraseñas de un solo uso (OTP) existen, y cuáles son los métodos de entrega que han surgido en los últimos años? Habiendo definido la pregunta de investigación, se procedió a realizar el estudio del arte, realizando una revisión literaria en bases de datos científicas como IEEE Xplore, Scopus, ACM Digital Library, entre otros. El resultado de esta investigación permitió conocer y comprender los protocolos de OTP existentes y algunas mejoras propuestas a los mismos. Adicionalmente, se encontró diferentes métodos de entrega de OTPs que han ido apareciendo como nuevas propuestas a lo largo de los años.

Habiendo terminado con la primera fase y haciendo uso del nuevo conocimiento adquirido, se analizó con los demás colaboradores, los diferentes métodos de entrega con los cuales el prototipo debía ser compatible. Estos métodos de entrega fueron seleccionados en base a su nivel de dificultad de implementación y su costo. Una vez definido lo anterior, se generaron los requerimientos necesarios para llevar a cabo la creación del prototipo.

En la etapa de análisis y diseño se definió la arquitectura general del sistema el cual no solo está conformado por el prototipo móvil desarrollado en el presente trabajo, sino que también están incluidos los prototipos web desarrollados por los colaboradores.

Adicionalmente, se realizaron mockups de alto nivel de las interfaces del prototipo móvil. Posteriormente, ya habiendo definido una arquitectura y un diseño se elaboró una lista de requerimientos funcionales que permitirán que el prototipo cumpla con el objetivo de este trabajo.

Para la etapa de implementación, se desarrolló un aplicativo móvil para dispositivos Android, donde el usuario pueda registrar las aplicaciones web, desarrolladas por los colaboradores, en las cual previamente se haya activado el doble factor de autenticación y posteriormente poder usar este mismo prototipo móvil para autenticarse en las aplicaciones anteriormente mencionadas. Además, el prototipo móvil fue desarrollado para ser compatible con los diferentes métodos de entrega pactados, los cuales fueron (SMS, correo electrónico, código QR, texto plano).

En la etapa de pruebas se desarrollaron pruebas tanto de rendimiento, como de usabilidad.

Por último, en la sexta fase se realizó el desarrollo de la Documentación, que incluye resultados y conclusiones.

1.3 Objetivo general

Crear un prototipo de aplicación móvil de un sistema de autenticación de dos factores utilizando One-Time Password, para dispositivos Android.

1.4 Objetivos específicos

1. Comprender el estado de arte de las OTP.
2. Realizar el diseño de un prototipo de aplicación móvil que utilice One-Time Passwords como segundo factor de autenticación.
3. Implementar el prototipo de aplicación móvil para dispositivos Android

1.5 Alcance

El presente trabajo consiste en la creación de un prototipo de aplicación el cual será utilizado por el usuario para poder autenticarse en un sistema, que utilice un esquema de doble factor de autenticación (i.e. contraseña más OTP). Este prototipo de aplicación móvil permitirá registrar los prototipos de aplicación web, desarrollados por 3 de los colaboradores del proyecto, en los cuales se haya activado el doble factor de autenticación. Cuando se active el doble factor de autenticación en los prototipos de aplicación web se deberá seleccionar una de las opciones de métodos de entrega de OTPs disponibles, los cuales son: (SMS, correo electrónico, código QR y texto plano). El prototipo de aplicación

móvil desarrollado en el presente trabajo deberá ser compatible con los métodos de entrega anteriormente mencionados.

El desarrollo de este prototipo está enfocado para dispositivos Android.

1.6 Marco teórico

Autenticación de usuario

Al proceso de autenticación se lo define como el proceso por el cual se establece confianza entre un usuario y un dispositivo o servicio, a través de una identificación provista, que compruebe que el usuario es quien dice ser [1]–[3]. Esta identificación provista, se la denomina método de autenticación, y dentro de la revisión de la literatura se han encontrado que trabajos como en [1], [3]–[6], en los cuales se listan tres principales métodos de autenticación.

- Algo que el usuario conoce: Se basa en el concepto de la existencia de un secreto que solo el usuario conoce. Este secreto puede ser: una contraseña, código, número de identificación personal o por sus siglas en inglés Personal Identification Number (PIN), entre otros [3], [4].
- Algo que el usuario posee: Para este método de autenticación es necesario que el usuario tenga posesión de un objeto en específico como: tarjetas inteligentes, teléfonos móviles, entre otros [3], [4]. A este tipo de objetos se los denomina tokens y pueden o no ser objetos físicos, puesto que existen tokens tanto de hardware como de software [3]
    - Token de hardware: Son dispositivos los cuales tienes como objetivo ser pequeños y portables, de modo que el usuario pueda llevarlo a todas partes. Usualmente almacenan en su interior algún tipo de llave criptográfica, un PIN que se muestra al usuario o incluso llegar a almacenar datos biométricos para posteriormente ser usados como llave de autenticación [2]. Además, tienen la propiedad de cambiar con el tiempo [2].
    - Token de software: Usualmente se trata de programas, que pueden ejecutarse en algún dispositivo inteligente como computadoras o en teléfonos móviles, los cuales tienen como función generar una contraseña que cambie cada vez que el usuario se haya autenticado. Por ejemplo, el algoritmo generador de un One-Time Password (OTP) [2].

- Algo que el usuario es: Este método está orientado a la autenticación biométrica, es decir, que sen miden de las características personales del usuario, por ejemplo: huella digital, reconocimiento facial, escaneo de iris, reconocimiento de voz [3]–[5], para verificar la identidad del usuario.

Cuando un proceso de autenticación cuenta con un solo método de los tres anteriormente mencionados (algo que el usuario conoce, algo que el usuario posee y algo que el usuario es), se lo denomina autenticación de un solo factor o por sus siglas en ingles Single Factor Authentication (SFA).

Cada uno de los métodos de autenticación presentados (algo que el usuario conoce, algo que el usuario posee y algo que el usuario es). Posee vulnerabilidades como, por ejemplo:

- En el caso de algo que el usuario conoce, las contraseñas, PINs, entre otros ejemplos, son susceptibles a ataques de diccionario, snooping, shoulder surfing, sniffing y ataques de fuerza bruta [1], [2], [5]. Existe también la posibilidad de que el usuario sea engañado para que ingrese sus credenciales en aplicaciones de phishing [2]

- En cuanto al método de algo que el usuario posee, cuando se trate de un token de hardware siempre existirá el riesgo de que este sea robado [3] se pierda o se dañe [2]. Además, en el caso de que el token deje de funcionar correctamente supone que el usuario o la organización que los use incurra en gastos adicionales para reparar o reemplazar el token [2].

- Finalmente, para el caso de algo que el usuario es, en [6] se menciona que es un método difícil de gestionar y de adoptar en la práctica con usuarios reales. En [2] también se hace referencia a que, a pesar de ser un método con un nivel considerable de seguridad, no es ampliamente implementado debido al alto costo de los dispositivos que tienen por objetivo registrar y autenticar a un usuario utilizando su información biométrica [2].

A pesar de las vulnerabilidades que posee cada método de autenticación. El paradigma que aún sigue dominando el campo de la autenticación y sigue siendo ampliamente implementado, es el uso de contraseñas [5], [6]. Entendiéndose por contraseña a una frase o una palabra que es usada para acceder a documentos, aplicaciones, sitios web, información o algún sistema computacional [7]. Una de las razones por las cuales las contraseñas siguen estando presentes en gran cantidad de sistemas de autenticación, se debe a que no se ha encontrado otro método que logre combinar seguridad, facilidad de

implementación y usabilidad de la misma forma en la que el uso de contraseñas lo ha hecho [5].

Actualmente se afirma que los métodos de autenticación de un solo factor basados en usuario y contraseña no son lo suficientemente seguros cuando de acceder a información sensible se refiere [3]. Del mismo modo en [6] a este método de autenticación se le considera inadecuado debido a que, además de las vulnerabilidades presentadas anteriormente, referentes a algo que el usuario conoce, las contraseñas presentan dos inconvenientes principales:

- El primer inconveniente se presente a nivel de transmisión y almacenamiento. A nivel de transmisión debido a la cantidad de servicios por los cuales pasa una contraseña antes de poder ser verificada, creando así una responsabilidad compartida entre estos servicios [5]. Estos servicios son: (aplicación en la cual el usuario ingreso su contraseña, canal de comunicación entre la aplicación y el servicio de verificación de credenciales y el servicio de verificación como tal) [5]. En cuanto al almacenamiento en [1] y [5] se menciona que las contraseñas pueden ser robadas desde su almacenamiento siendo susceptibles así al filtrado de contraseñas.

- El segundo inconveniente recae en el usuario, como se detalla en [5], es el usuario el encargado de la creación de su propia contraseña asi como de recordarla. Teniendo en cuenta la gran cantidad de aplicaciones y servicios que existen en la actualidad y sabiendo que cada uno de estos requieren de un usuario y contraseña diferentes [5]. Los usuarios tienden a usar contraseñas que son fáciles de adivinar [2] o a usar la misma contraseña o similares [6]. Las razones para que el usuario tienda a crear este tipo de contraseñas se debe a que la complejidad de la contraseña es inversamente proporcional a su usabilidad [6]. Finalmente, en [6], se menciona que el cerebro humano no tiene la capacidad de recordar muchas contraseñas que posean un alto nivel de complejidad.

Conociendo los principales inconvenientes con los que cuenta el uso de contraseñas ha habido intentos por mejorar este paradigma. Como se menciona en [5], se han creado políticas de creación de contraseñas, interfaces resistentes a phishing, entre otras medidas que buscan mejorar la seguridad del uso de contraseñas. A pesar de estos esfuerzos, en el mismo trabajo, se menciona que no se han logrado un cambio que represente una mejora tangible en este método de autenticación.

Considerando las vulnerabilidades presentes en el uso de contraseñas como método de autenticación, el “Reglamento general de protección de datos” de la unión europea ha declarado que el uso de un solo factor de autenticación no es suficiente para mantener la seguridad, y recomienda que estos sean combinados con un segundo o varios factores de autenticación [4].

Si se combinan dos factores de autenticación, por ejemplo, algo que usuario conoce con algo que el usuario es, esto ya supone una mejora a la seguridad. A esta combinación de dos factores se le conoce como doble factor de autenticación o por sus siglas en ingles Two-Factor Authentication (2FA) [1].

En cuanto a segundo factor de autenticación una de las alternativas más factibles en temas de costo es el uso de contraseñas de un solo uso (OTP). Cabe resaltar que se hace referencia a los tokens de software en específico. Los cuales toman como ventaja la gran proliferación de teléfonos inteligentes, que son los que alojan y ejecutan el token, sin necesidad de que el usuario deba preocuparse por llevar siempre un dispositivo adicional.

One-Time Passwords (OTPs)

Una contraseña de un solo uso o por sus siglas en ingles One-Time Password (OTP) son contraseñas que son válidas por una sola vez [3]. Esta característica representa una ventaja puesto que, si un OTP es comprometido, es decir, un atacante obtiene dicha contraseña. No representa un peligro para futuros inicios de sesión debido a los OTPs no son fáciles de predecir [3], [7]. En [7] se listan otras ventajas del uso de las OTP como, por ejemplo: son resistentes a replay attacks, reducen el daño causado por ataques de phishing o spyware.

La primera vez que se mencionó a las contraseñas de un solo uso fue en [8] por Leslie Lamport en 1998, dando como resultado la primera estandarización de las OTP [6]. Sin embargo, no se comercializo con este nombre sino con el nombre de S/KEY authentication [6].

A lo largo de los años han ido surgiendo diferentes algoritmos que buscan generar contraseñas de un solo uso. Es en base a estos algoritmos que en [4] y [6] las OTP se clasifican de la siguiente manera:

- One-Time Password (OTP): Este tipo de OTP corresponde al algoritmo original presentado por Leslie Lamport, en el cual el OTP es generado a partir de una semilla, en donde cada valor nuevo generado depende de su predecesor [4]. Tomando como referencia la representación matemática representada en [4], se

inicia con el valor de una semilla s_0 a la cual se le aplica una función unidireccional $F(x)$ dando como resultado el primer valor OTP, $otp_1 = F(s_0)$, el segundo valor vendría dado por la siguiente expresión $otp_2 = F(otp_1)$ y asi sucesivamente.

- HMAC-Based One-Time Password (HOTP): Este algoritmo a diferencia del OTP propuesto por Lamport, comparte un contador y un secreto compartido entre el servidor y el cliente [6]. De modo que para poder generar el mismo OTP y autenticar al usuario de forma correcta, tanto el servidor como el cliente deben mantener el contador en sincronía [6].

- Time-Base One-Time Password (TOTP): El algoritmo de TOTP basado en tiempo surgió como una mejora del algoritmo de (HOTP) [6]. La mejora con respecto al algoritmo de (HOTP) viene dada por intercambiar el contador, por el tiempo de UNIX, el cual se utiliza para mantener tanto al cliente como al servidor en sincronía [6]. Adicionalmente, este algoritmo añade una capa extra de seguridad debido a que existe un rango de tiempo dentro del cual el OTP es válido y fuera de este periodo de tiempo, no lo es más, puesto que un nuevo valor ha de ser generado [4].

- Challenge-Based OTP: También denominados Challenge-Response, este método de autenticación hace uso de un token de hardware, por ejemplo, una tarjeta o una llave inteligentes [4], [7]. Para poder obtener el valor del OTP el usuario deberá ingresar una contraseña o un PIN (el reto) que, en el caso de ser correcto, el token generará el OTP [7]. Este tipo de autenticación ha sido usando principalmente como una forma de autenticación en tarjetas de crédito o débito en Europa [7].

Método de entrega de OTP

En trabajos como [7] existe una sección en específico dedicada a describir la forma en la que los OTPs son enviados a los usuarios. Adicionalmente a lo largo de la revisión literaria también se han encontrado algunas formas inusuales en las que se entrega el OTP.

- Mensaje de texto o SMS: Teniendo en cuenta que en la actualidad la mayoría de las personas en el mundo lleva consigo un teléfono inteligente por motivos de comunicación [2]. El envío de OTPs a través de mensajes de texto se ha convertido en uno de los métodos de entrega más comunes, debido a la omnipresencia de teléfonos móviles y el bajo costo que implica usar el servicio de SMS [7]. No obstante, este método de entrega tiene algunas vulnerabilidades como que generalmente el OTP que se envía por este medio no se cifra y esta vulnerable a un ataque man-in-the-middle [7].

- Teléfonos móviles: Considerando la proliferación de teléfonos móviles, el uso de un token de software que se ejecute dentro de estos dispositivos, supone una gran ventaja teniendo en cuenta que este tipo de tokens no consumen gran cantidad de recursos del dispositivo asi como almacenamiento [7]. Además, esto supone una ventaja para el usuario dado que podrá autenticarse en múltiples servicios en varias ocasiones con la ayuda de un mismo dispositivo [7]. Sin embargo, este tipo de dispositivos están sujetos a algunos riesgos como que este sea robado, se dañe o se pierda [7].

- Tokens propietarios: Este método de entrega está relacionado con los tokens de hardware, los cuales son dispositivos que en su interior guardan alguna llave secreta que les permitirá generar los diferentes OTPs cada ocasión en la que el usuario desee autenticarse [2], [7].

- Basados en la web: Para este método de entrega se basa completamente en la capacidad del usuario de reconocer categorías que hayan sido seleccionadas previamente [7]. En [7] se presenta el siguiente ejemplo, a un usuario que desea autenticarse en una aplicación web, se le muestra una serie de imágenes las cuales pertenecen a ciertas categorías como: (perros, gatos, vehículos, entre otros). El usuario debe seleccionar las imágenes relacionadas a una categoría específica que el mismo haya establecido anteriormente. Cada una de estas imágenes tienen caracteres alfanuméricos asociadas, de modo que, una vez se hayan seleccionado todas las imágenes relacionadas a la categoría preestablecida el usuario obtendrá el valor del OTP. A diferencia de los métodos de entrega anteriormente presentados, este no necesita un token ya que es presentado en el propio servicio al que se quiere acceder [7].

- Basados en papel: En [7] se menciona que algunos bancos enviaban una lista impresa con los OTPs a los usuarios. De esta forma cada vez que el usuario deseará realizar una transacción, se vería obligado a agregar, en orden secuencial, el valor del OTP de la lista, para poder efectuar dicha transacción.

- Código QR: En trabajos como en [9] se propone un método de entrega que combina el concepto de teléfonos móviles y basados en la web. En [9] se describe que la aplicación en la cual el usuario quiere autenticarse será la que muestre el código QR, el cual tendrá encriptado el valor del OTP. Por otra parte, el usuario tendrá un token de software que se ejecutará en su dispositivo móvil y utilizará la dirección MAC como identificador único. De esta forma cuando el usuario escanee el código

QR con su teléfono móvil. El token de software enviará tanto el valor del OTP, así como su identificador único (dirección MAC) al servicio verificador de la aplicación para de esta manera autenticar al usuario.

- Canal Piezo-Gyro: En [10] se describe como se utiliza un token de hardware el cual enviará el OTP a una aplicación móvil a través de una simulación acústica. Esta simulación estimula el giroscopio del dispositivo móvil, mismo que decodificará el valor del OTP y lo ingresará en la aplicación móvil sin necesidad de que el usuario conozca el valor del OTP. Para que el proceso anteriormente mencionado sea exitoso en [10] se menciona que el usuario deberá poner en contacto al token de hardware con dispositivo móvil y presionar un botón en el token, dando inicio así al proceso descrito anteriormente.

2 METODOLOGÍA

El proyecto ha sido dividido en seis etapas, las cuales se listan a continuación: (1) Estudio sistemático de la literatura, (2) Análisis y selección de los métodos de entrega de OTP, (3) Análisis y diseño del prototipo, (4) Desarrollo del prototipo, (5) Desarrollo de las pruebas del prototipo y (6) Documentación.

2.1 Metodología iterativa e incremental

A lo largo de todo el proyecto se utilizó la Metodología de Desarrollo Iterativo e Incremental, la cual está enfocada en la gestión de proyectos de moto tal que su desarrollo es progresivo e iterativo con el objetivo alcanzar el resultado esperado [11]. En el caso de la tercera, cuarta y quinta etapa referentes al desarrollo, se utilizó una metodología de desarrollo de software ágil como lo es Scrum [11].

Figura 7. Etapas del proyecto y metodologías utilizadas

2.2 Scrum

Scrum es un framework que tiene como objetivo entregar soluciones en cortos periodos de tiempo de una mejor manera y a menor costo [12]. Este framework se enfoca en la gestión de proyectos, los cuales tiene problemas de planificación o tienen cierto grado de

incertidumbre [12], [13]. Scrum está basado en un modelo iterativo e incremental [12], [13]. Estos incrementos, se denominan “sprints” y tienen una duración de entre 2 y 4 semanas [12], [13]. Cada sprint inicia con una reunión denominada “Sprint Planning”, la cual tiene por objetivo detallar las tareas que se deberán cumplir a lo largo del “sprint” y tiene duración de máximo hasta 4 horas [13]. Así como existe una reunión de apertura del “sprint” existe una reunión de cierre denominada “Sprint Review” [13], en esta reunión se encuentran presentes las partes interesadas del proyecto para evaluar el progreso de este [13]. Al igual que el “Sprint Planning”, tiene una duración de máximo 4 horas [13]. Existen reuniones adicionales como lo son las “Daily Meetings”. Como su nombre lo sugiere, son reuniones que se llevan a cabo de forma diaria en donde se mantiene al equipo actualizado sobre la información del progreso de las tareas establecidas en ese “sprint” realizándose preguntas como: “¿Qué es lo que voy a hacer hoy?, ¿Qué fue lo que hice ayer?, ¿Existe algún bloqueo que impida el avance de las tareas?” [13], [14]. Para esta reunión se encuentran presentes todos los miembros, incluyendo a aquellos que realicen su trabajo de forma remota [15]. Estas reuniones tienen una duración de entre 10 y 35 minutos [14]. Otra reunión que se lleva a cabo es la denominada “Sprint Retrospective”, en la cual se identifica los problemas que se suscitaron durante el “sprint” y las oportunidades de mejora que puedan aplicarse a los siguientes sprints [14].

Otro aspecto esencial de Scrum se menciona en [16], en donde se sugiere que se deben llevar a cabo pruebas de aceptación de la usabilidad durante cada sprint para asegurarse que el objetivo de dicho sprint se haya cumplido.

Artefactos presentes en Scrum

En [17] se define a los artefactos de Scrum como un método de comunicación opuesto a la comunicación cara a cara. Los principales artefactos presentes en esta metodología son:

- Product Backlog: En este artefacto, se enumeran todas los requisitos, características, funciones, mejoras y correcciones que ayudan a definir el futuro del producto de software [17].
- Sprint Backlog: Toma los elementos del Product Backlog seleccionados para un sprint en específico y los contiene en subconjuntos [17].
- Product Increment: Es una lista de todos los elementos del Product Backlog que se han completado durante cada sprint [17].

Roles que existen en Scrum

El framework de Scrum a parte de las reuniones posee roles definidos como los que se listan a continuación.

- Producto Owner: representa a las partes interesadas externas y sus interesa. Es el puente por el cual se establece una conexión entre las partes interesadas y el equipo de desarrollo de software [18]. Adicionalmente, en versiones actuales de scrum, se menciona que el “Product Owner”, es el encargado de establecer el calendario de lanzamiento del producto final, además de gestionar la evolución del producto a medida que el proyecto avance y se susciten cambios en el mismo [18]. Se ocupa además del product backlog, el riesgo y el contenido se va a mostrar como resultado [18].
- Scrum Master: Además de ser la persona a cargo del “Scrum Team”, en [18] se listan seis actividades principales que son realizadas por este rol, las cuales son
    - Soporte del proceso, se le denomina de esta forma debido a que es el encargado de fomentar la adopción los métodos ágiles [18].
    - El organizador de las “Daily meetings”, porque es la persona que se encarga de garantizar que todos y cada uno de los miembros del equipo compartan información sobre el estado del cumplimiento de sus tareas, asi como los bloqueos que han ocurrido durante cada sprint [18].
    - El eliminador de bloqueos, puesto que es el “Scrum Master” quien se encarga de resolver los bloqueos que se les presente a los miembros del Scrum Team [18].
    - El planificador de sprints, se debe a que el “Scrum Master” es la persona que clasifica las historias de usuario y coordina las actividades que se les asignara a cada miembro del equipo en cada sprint [18].
    - El organizador de scrums, este nombre hace referencia al caso en donde existan varios equipos de desarrollo y cada equipo cuente con su propio “Scrum Master”. Este se encarga de coordinar el trabajo con los demás “Scrum Masters” [18].
    - El encargado de integración, se refiere a que es el encargado de realizar la unión de bases de código que han sido desarrolladas por otros equipos de desarrollo que trabajan en paralelo [18].
- Scrum Team: Miembros responsables de desarrollo de software [18].

Para el presente proyecto se definieron de la siguiente manera cada uno de los roles establecidos.

Tabla 1. Definición de roles para el proyecto tras aplicar Scrum

Rol	Desempeñado por:
Product Owner	PhD. Sang Guun Yoo
Scrum Master	Anthony Almachi
Scrum Team	Anthony Almachi

Diseño de la arquitectura

Para el desarrollo del prototipo móvil se utilizó React Native como lenguaje de programación. React Native es una librería open source diseñada por Facebook en marzo del 2015 [19]. Una de las ventajas que tiene el uso de esta librería se menciona en [20], donde se destaca su flexibilidad y mutabilidad. Permitiéndole a React Native poder adaptarse a cualquier ambiente operativo sin ningún inconveniente. React Native, además, posee una similitud de sintaxis del 80% en comparación con la base de código con ReactJS de modo que, si se tiene conocimiento en esta librería, React Native no supone un gran cambio de paradigma [21]. Finalmente, como se menciona en [22] React Native tiene un buen desempeño y brinda una buena experiencia de usuario.

Para la base de datos se utilizó Firestore. Firestore es una base de datos No-SQL alojada en la nube y proporcionada por Firebase [23]. Casi cualquier plataforma puede acceder a este servicio a través de una interfaz de programación de aplicaciones o por sus siglas en inglés Application Programming Interface (API) [23].

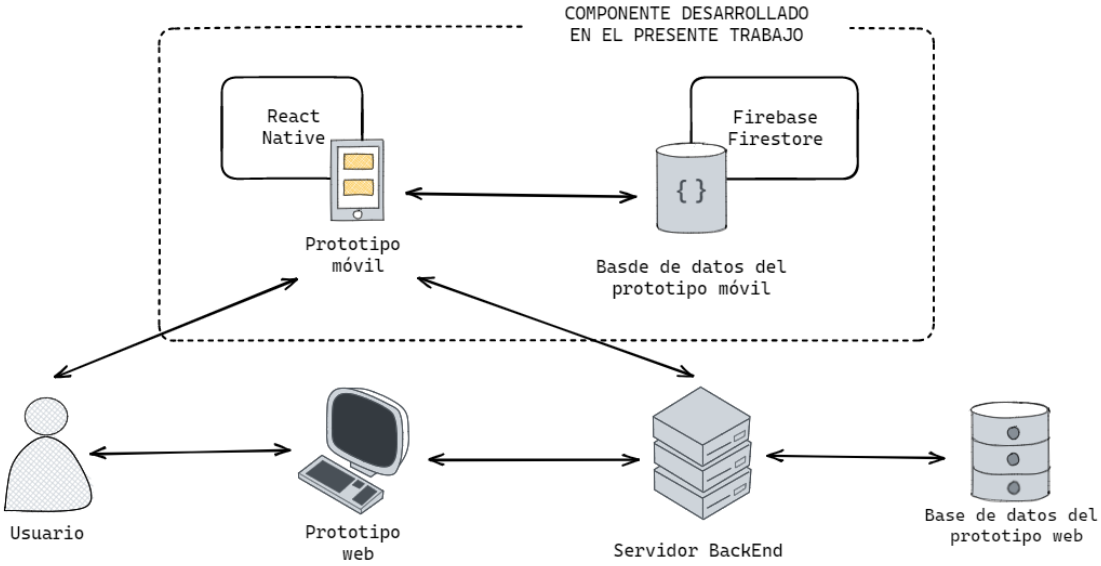


Figura 8. Arquitectura del sistema de doble factor de autenticación

Aplicación de Scrum

Sprint 0

- **Product Backlog**

Tabla 2. Product Backlog

Código	Título	Prioridad	Esfuerzo (/20)
EP01US01	Inicio de la aplicación	Baja	5
EP01US02	Introducción al funcionamiento de la aplicación	Baja	5
EP02US01	Lista de aplicaciones registradas	Media	10
EP02US02	Registro de aplicaciones	Alta	15
EP02US03	Información adicional acerca del funcionamiento del prototipo móvil	Baja	7
EP03US01	Ingreso del OTP manualmente	Media	5
EP03US02	Ingreso del OTP mediante el escaneo de un código QR	Media	5
EP03US03	Envió del OTP	Alta	7

- **Historias de usuario**

Tabla 3. Historias de usuario

Código	Título	Descripción

EP01US01	Inicio de la aplicación	Yo como desarrollador del prototipo móvil deseo que se muestre el logo y nombre de la aplicación para crear una experiencia de marca para el usuario
EP01US02	Introducción al funcionamiento de la aplicación	Yo como desarrollador del prototipo móvil deseo mostrar una breve introducción a la funcionalidad del prototipo para que el usuario final pueda utilizarla de manera efectiva
EP02US01	Lista de aplicaciones registradas	Yo como usuario final deseo que se muestren las aplicaciones registradas en donde he activado el doble factor de autenticación para poder autenticarme en las mismas.
EP02US02	Registro de aplicaciones	Yo como usuario final deseo registrar una aplicación en la que he activado el doble factor de autenticación para poder autenticarme en esta.
EP02US03	Información adicional acerca del funcionamiento del prototipo móvil	Yo como desarrollador del prototipo móvil deseo que exista más información acerca del funcionamiento del prototipo móvil para poder solventar las dudas adicionales de los usuarios finales
EP03US01	Ingreso del OTP manualmente	Yo como usuario final deseo poder ingresar manualmente el valor del OTP que se me ha enviado a través de los métodos de entrega, (SMS, correo electrónico, texto plano) para autenticarme en la aplicación web
EP03US02	Ingreso del OTP mediante el escaneo de un código QR	Yo como usuario final deseo poder escanear el código QR que se me ha enviado, el cual contiene el valor del OTP para poder autenticarme.
EP03US03	Envió del OTP	Yo como desarrollador del prototipo móvil deseo poder enviar el valor del OTP ingresado por el usuario para poder completar el proceso de autenticación.

- **Mockup del prototipo**

Para realizar el diseño de interfaces se utilizó la aplicación Figma. A continuación, se muestras las pantallas principales, pero si se desea tener acceso a todo el diseño de interfaces, el enlace a esta se encuentra en el Anexo I.

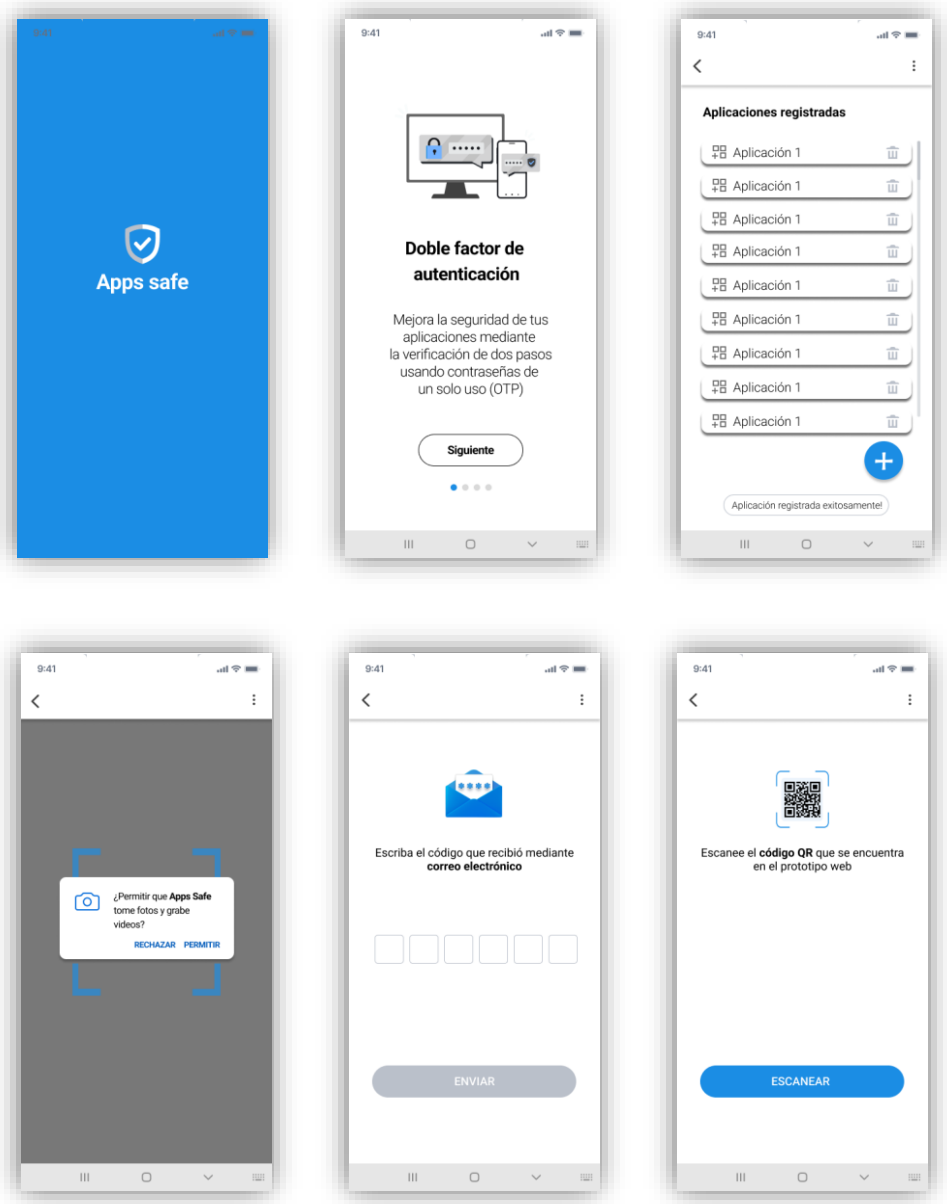


Figura 9. Mockup de las pantallas principales del prototipo móvil

Sprint 1

- **Release plan**

Tabla 4. Estimación del sprint 1

Duración del sprint	**1 semana**
Días de trabajo durante el sprint	5 días

Tabla 5. Estimación de horas de trabajo para el sprint 1

Miembros del equipo	Días disponibles durante el sprint	Horas disponibles por día	Total, de horas disponibles por sprint
Anthony Almachi	5 días	4 horas	20 horas

Tabla 6. Tabla de pasos

Sprint 0	Sprint 1	Esfuerzo	Sprint 2	Esfuerzo	Sprint 3	Esfuerzo
	EP01US01	5	EP02US01	10	EP03US01	5
	EP01US02	5	EP02US02	15	EP03US02	5
	EP02US03	7			EP03US03	7
Total		17		25		17

- **Sprint planning**
  - **Objetivo**

Implementar las siguientes interfaces: interfaz que se mostrará al usuario final todas las veces que este inicie la aplicación, interfaces que contendrán una breve introducción sobre el funcionamiento del prototipo y finalmente la implementación de un menú que permita al usuario conocer más sobre el funcionamiento del prototipo.

  - **Resultado del sprint planning**

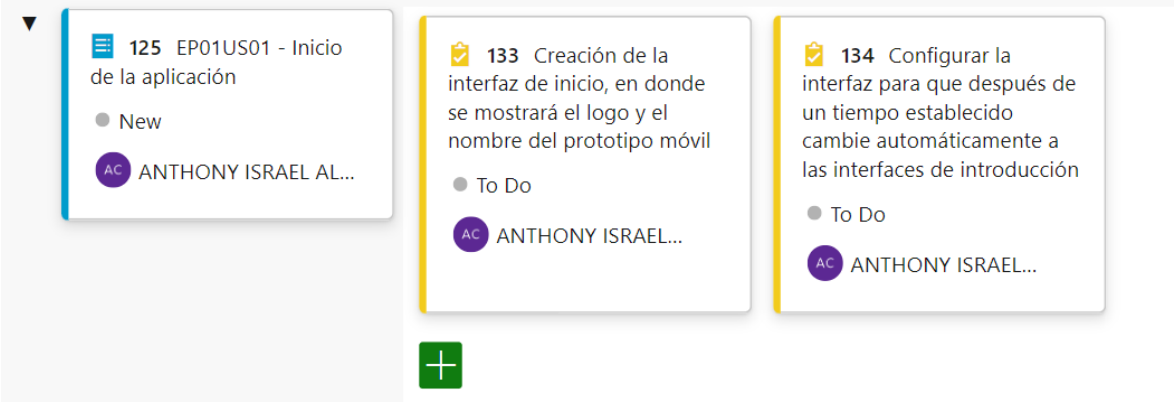


Figura 10. Lista de tareas para la historia de usuario EP01US01

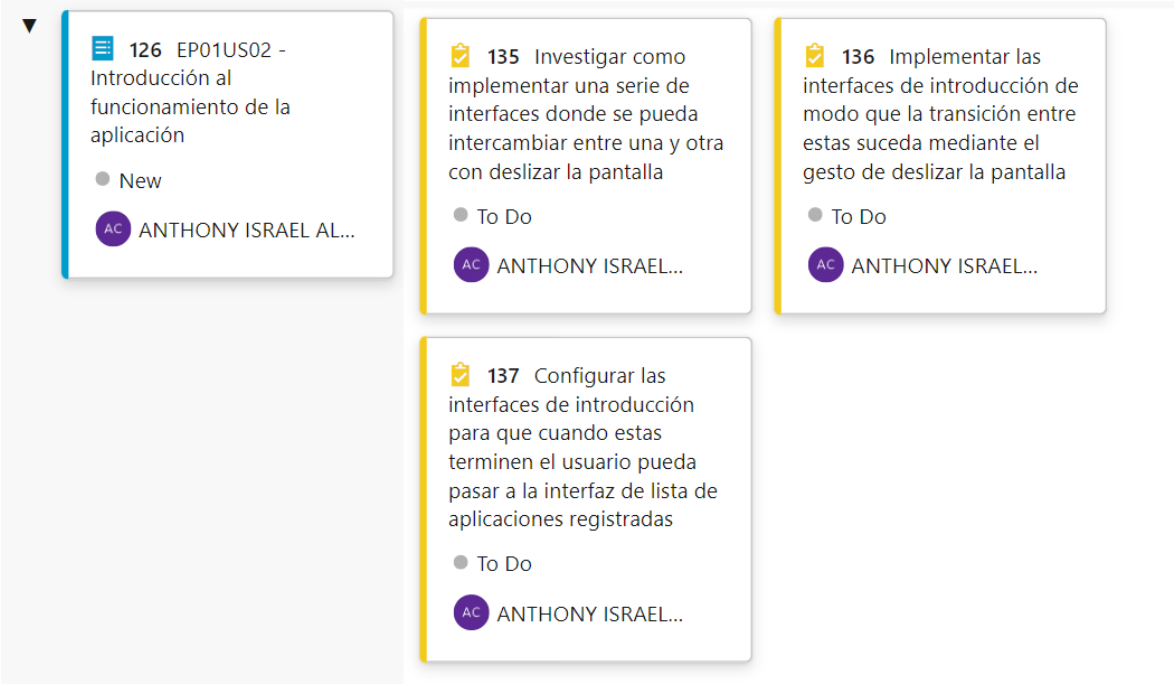


Figura 11. Lista de tareas para la historia de usuario EP01US02

Figura 12. Lista de tareas para la historia de usuario EP02US03

- **Sprint review**

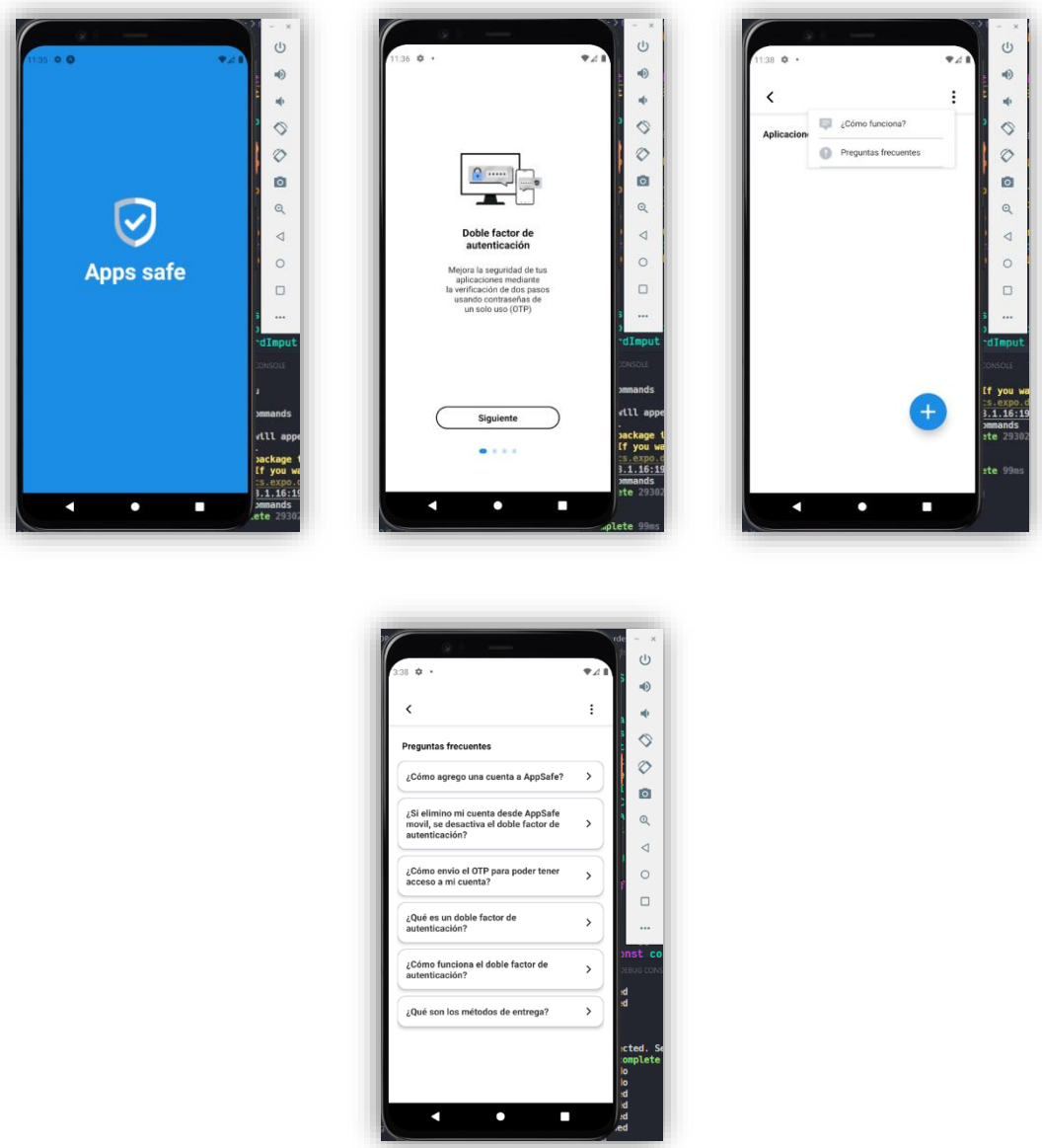


Figura 13. Resultados del sprint 1

Para cerciorarse que el sprint 1 se haya llevado a cabo de forma satisfactoria, se verificó que se hayan cumplido con los siguientes criterios de aceptación. En la siguiente tabla se presenta un ejemplo de cómo se formularon los criterios de aceptación para el sprint mencionado anteriormente. Para observar todos los criterios de aceptación propuestos se debe revisar el Anexo II.

Tabla 7. Ejemplo de los criterios de aceptación para el sprint 1

Criterios de aceptación					
Escenario	**Título**	**Contexto**	**Evento**	**Acción**	**Cumplido**

1	Primer Inicio prototipo	El usuario final acaba instalar el prototipo	El usuario final ejecuta el prototipo por primera vez	Se presenta el logo de la aplicación y automáticamente se redirige al usuario a la primera interfaz de introducción	Si

- **Sprint retrospective**

Existieron inconvenientes con la configuración del ambiente de desarrollo por lo que hubo retrasos que se solventaron con horas extra dedicadas al presente sprint. Para mejorar este aspecto en los siguientes sprints, se dedicaron horas específicas a capacitaciones en tecnologías desconocidas.

Sprint 2

- **Release plan**

Tabla 8. Estimación del sprint 2

Duración del sprint	**2 semana**
Días de trabajo durante el sprint	10 días

Tabla 9. Estimación de horas de trabajo para el sprint 2

Miembros del equipo	Días disponibles durante el sprint	Horas disponibles por día	Total, de horas disponibles por sprint
Anthony Almachi	10 días	4 horas	40 horas

Tabla 10. Tabla de pasos

Sprint 0	Sprint 1	Esfuerzo	Sprint 2	Esfuerzo	Sprint 3	Esfuerzo
	EP01US01	5	EP02US01	10	EP03US01	5
	EP01US02	5	EP02US02	15	EP03US02	5
	EP02US03	7			EP03US03	7
Total		17		25		17

- **Sprint planning**

- **Objetivo**

Llevar a cabo el proceso completo de registro de una aplicación web al prototipo móvil y mostrarla en la lista de aplicaciones registradas.

- **Resultado del sprint planning**

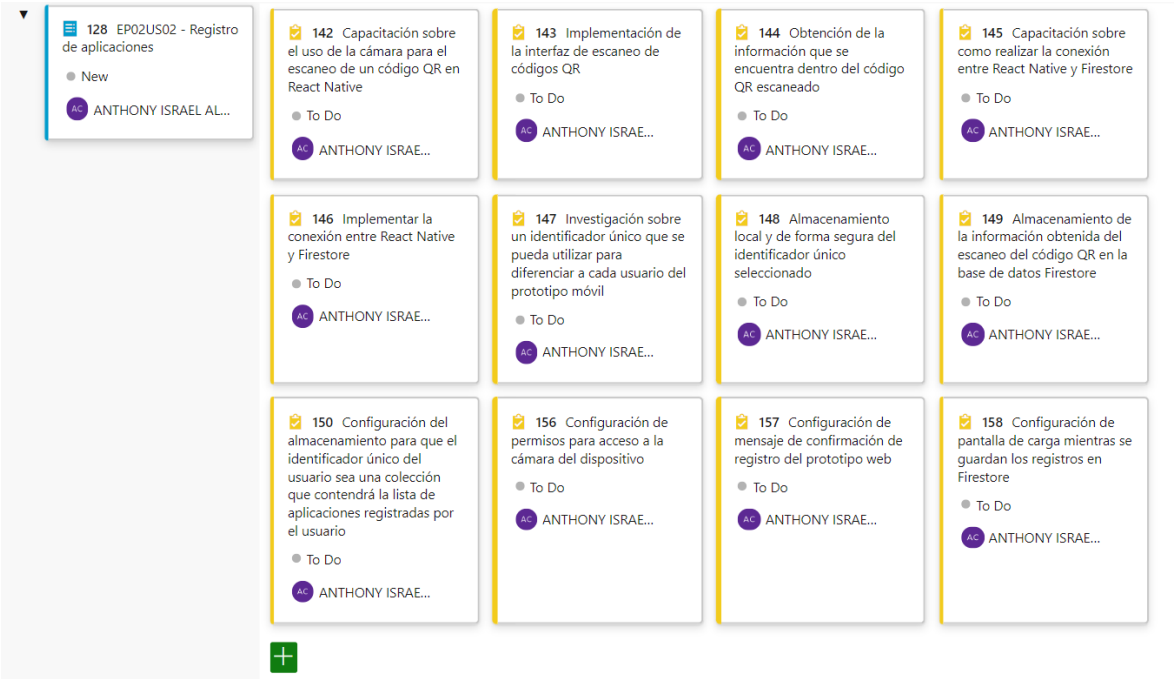


Figura 14. Lista de tareas para la historia de usuario EP02US02

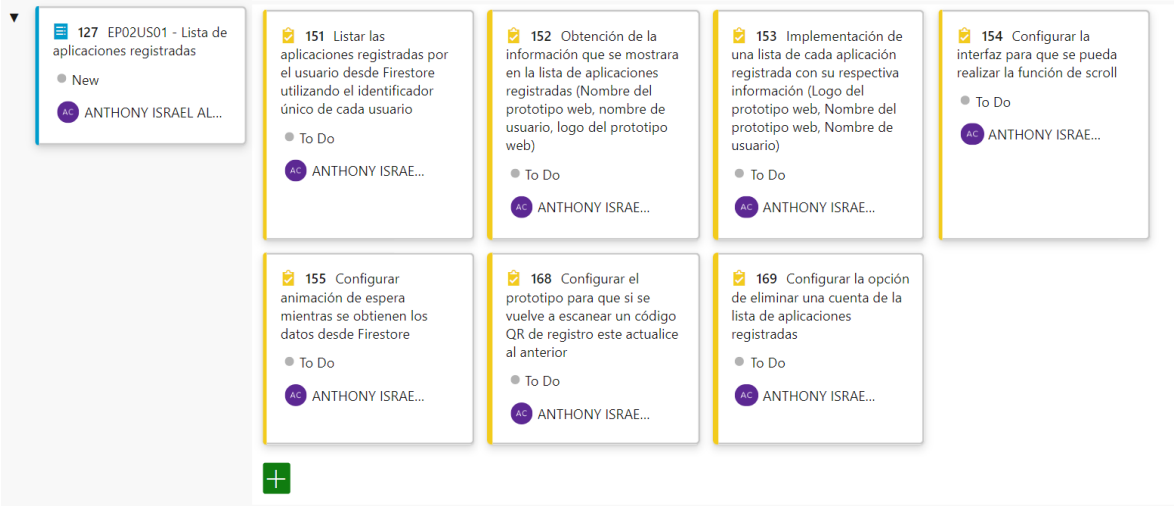


Figura 15. Lista de tareas para la historia de usuario EP02US01

- **Sprint review**

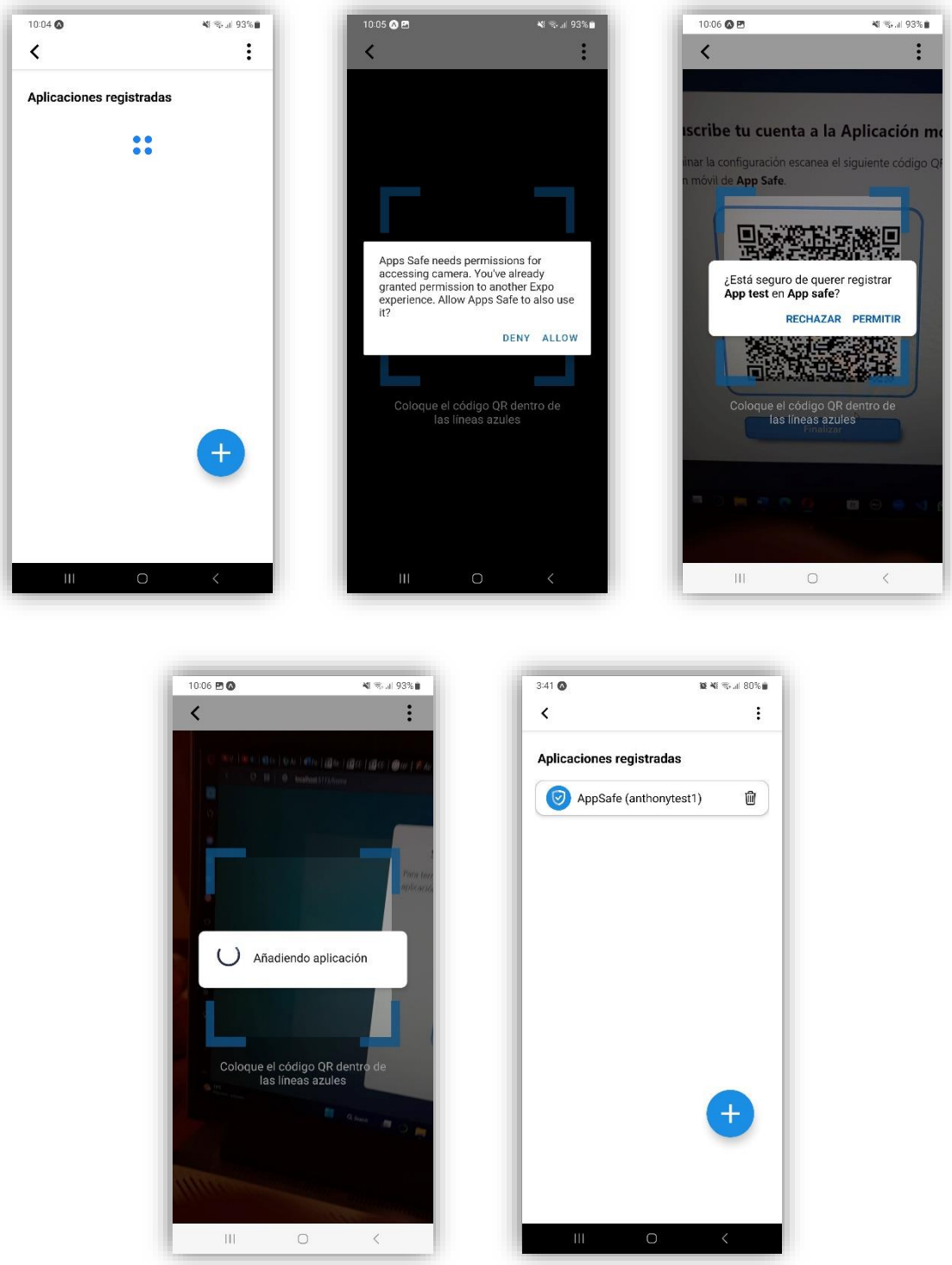


Figura 16. Resultados del sprint 2

Para cerciorarse que el resultado del sprint 2 cumplió con los objetivos propuestos, se verificó que se hayan cumplido con los siguientes criterios de aceptación. En la siguiente tabla se presenta un ejemplo de cómo se formularon los criterios de aceptación para el

sprint 2. Para observar todos los criterios de aceptación propuestos se debe revisar el Anexo III.

Tabla 11. Ejemplo de los criterios de aceptación para el sprint 2

Criterios de aceptación					
Escenario	**Título**	**Contexto**	**Evento**	**Acción**	**Cumplido**
1	Primer registro de aplicación	El usuario final acaba finalizar la introducción al funcionamiento del prototipo y se encuentra en la interfaz de registro de una aplicación.	El usuario final selecciona la opción de registro de una aplicación mediante un código QR	Se muestra una interfaz en donde se le preguntara al usuario si desea dar acceso a la cámara del dispositivo para poder escanear el código QR	Si

- **Sprint retrospective**

Existieron inconvenientes con los tiempos establecidos puesto que durante el sprint fueron surgiendo nuevas interrogantes en cuanto al funcionamiento del prototipo. En otras palabras, a lo largo de este sprint aparecieron nuevas tareas como: el hecho de que se necesitara un identificador único para cada usuario del prototipo móvil.

Sprint 3

- **Release plan**

Tabla 12. Estimación del sprint

Duración del sprint	**1 semana**
Días de trabajo durante el sprint	5 días

Tabla 13. Estimación de horas de trabajo

Miembros del equipo	Días disponibles durante el sprint	Horas disponibles por día	Total, de horas disponibles por sprint
Anthony Almachi	5 días	4 horas	20 horas

Tabla 14. Tabla de pasos

Sprint 0	Sprint 1	Esfuerzo	Sprint 2	Esfuerzo	Sprint 3	Esfuerzo
	EP01US01	5	EP02US01	10	EP03US01	5
	EP01US02	5	EP02US02	15	EP03US02	5
	EP02US03	7			EP03US03	7
Total		17		25		17

- **Sprint planning**
    - **Objetivo**

Crear las interfaces de ingreso de OTP compatibles con los métodos de entrega disponibles (SMS, correo electrónico, texto plano, código QR) y gestionar el envío del OTP para completar el proceso de autenticación del usuario.

- **Resultado del sprint planning**

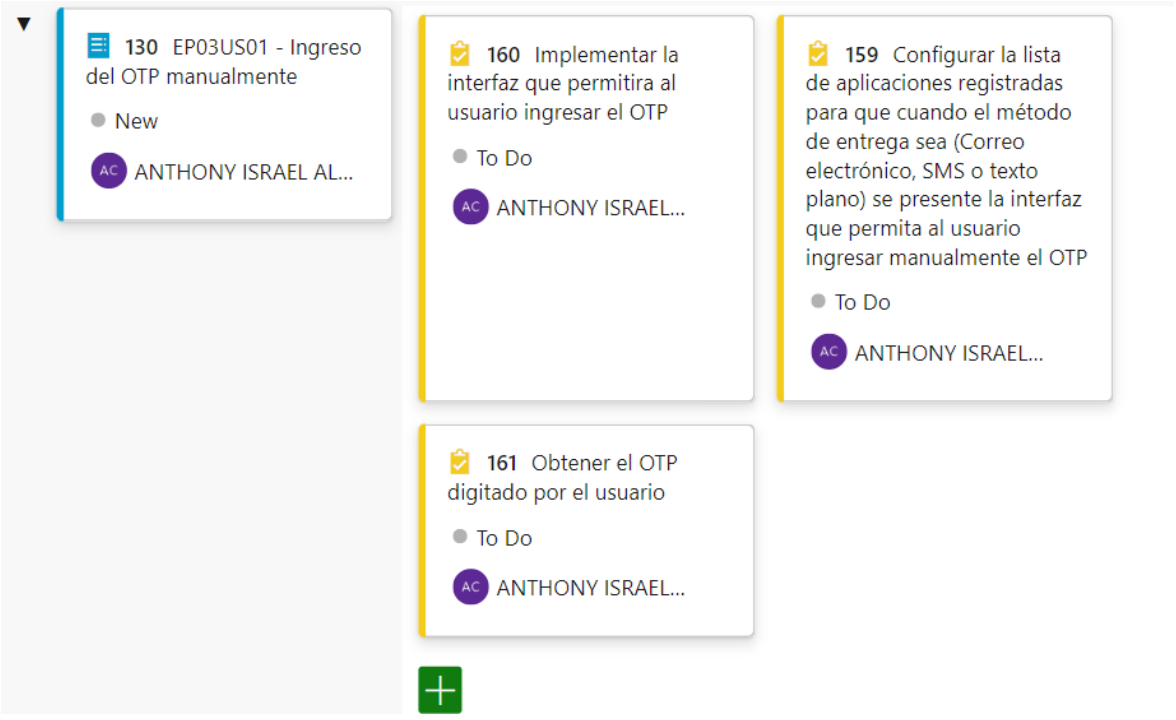


Figura 17. Lista de tareas para la historia de usuario EP03US01

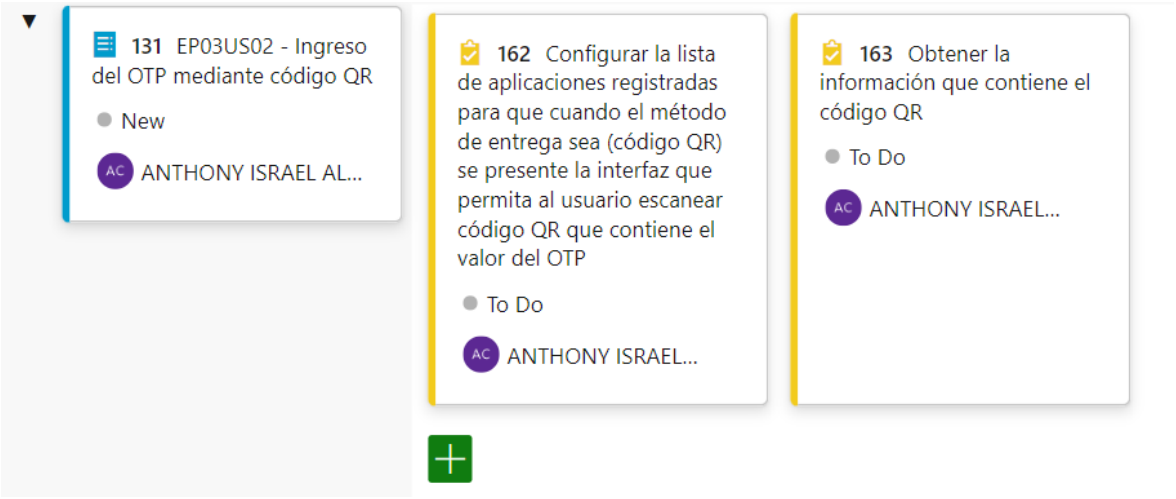


Figura 18. Lista de tareas para la historia de usuario EP03US02

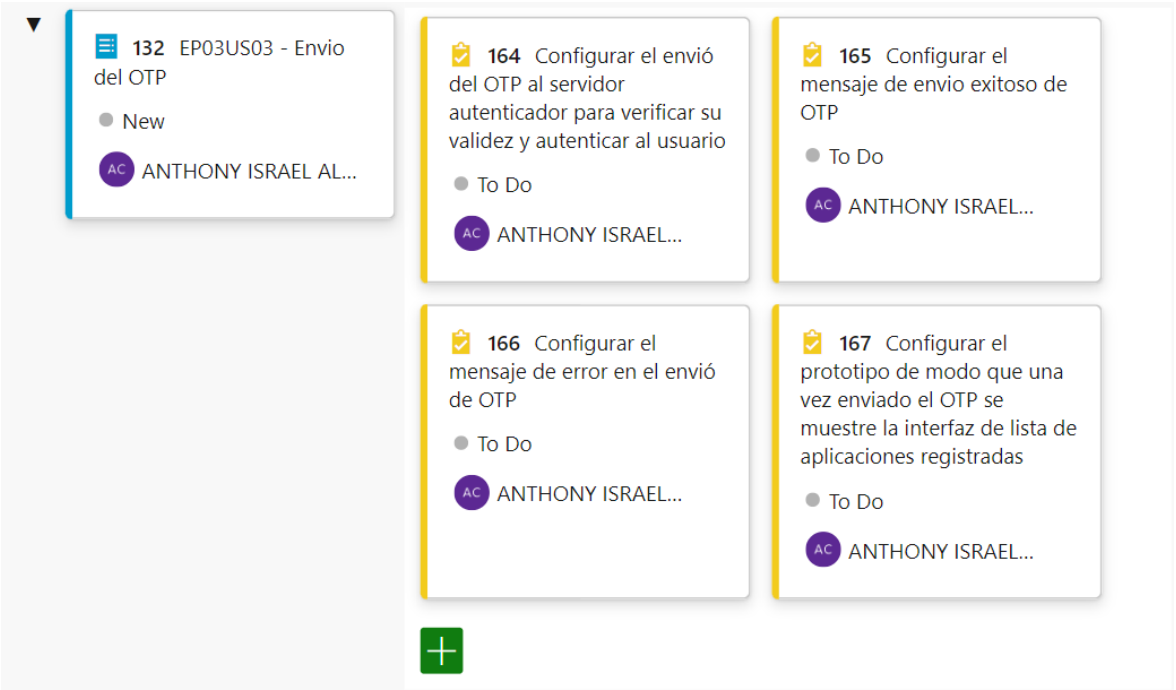


Figura 19. Lista de tareas para la historia de usuario EP03US03

- **Sprint review**

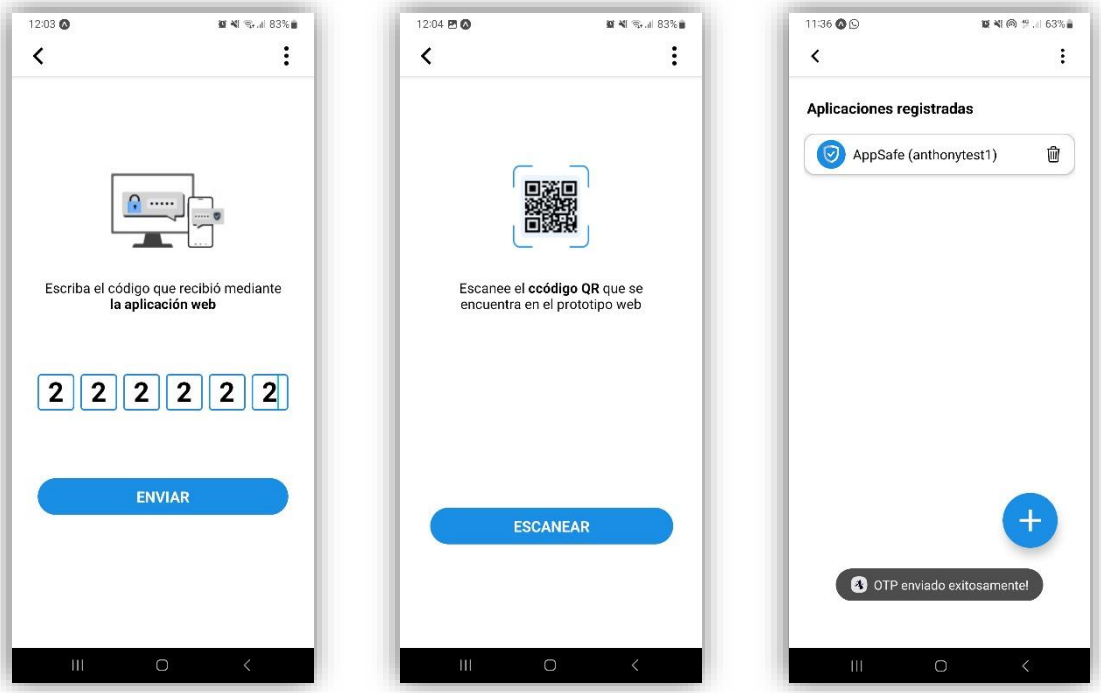


Figura 20. Resultados del sprint 3

Para verificar que el resultado del sprint 3 haya sido el esperado, se verificó que se hayan cumplido con los siguientes criterios de aceptación. En la siguiente tabla se presenta un ejemplo de cómo se formularon los criterios de aceptación para el sprint 3. Para observar todos los criterios de aceptación propuestos se debe revisar el Anexo IV.

Tabla 15. Ejemplo de los criterios de aceptación para el sprint 3

Criterios de aceptación					
Escenario	**Título**	**Contexto**	**Evento**	**Acción**	**Cumplido**
1	ingreso mediante código QR (escaneo del OTP mediante el prototipo)	El usuario final habiendo activado el 2FA en el prototipo web, habiendo seleccionado el método de entrega por código QR y habiendo registrado la aplicación en el prototipo móvil, desea ingresar a la aplicación web y se le	El usuario final dentro de la lista de aplicaciones registradas selecciona la aplicación en la que desea autenticarse	Se muestra la interfaz que permitirá escanear cualquier código QR	Si

		solicita que ingrese el OTP en el prototipo.			

- **Sprint retrospective**

Una vez cumplido los sprints anteriores, hubo un tiempo prudencial para familiarizarse con el entorno de desarrollo de modo que el cumplimiento de este sprint no supuso un mayor inconveniente.

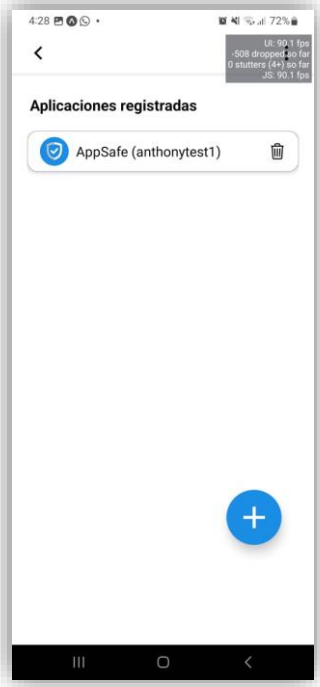
2.3 Producto final terminado

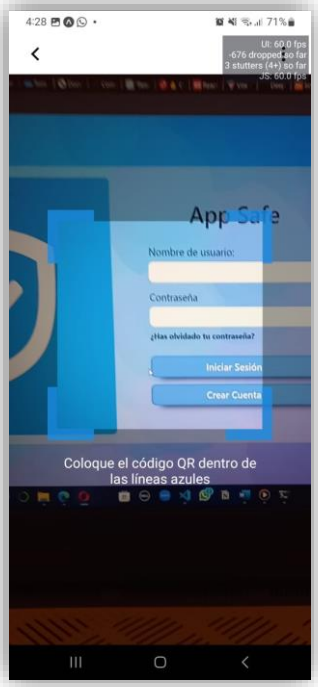
El resultado de la fase de desarrollo se la puede encontrar en el repositorio cuyo enlace se encuentra en el Anexo V.

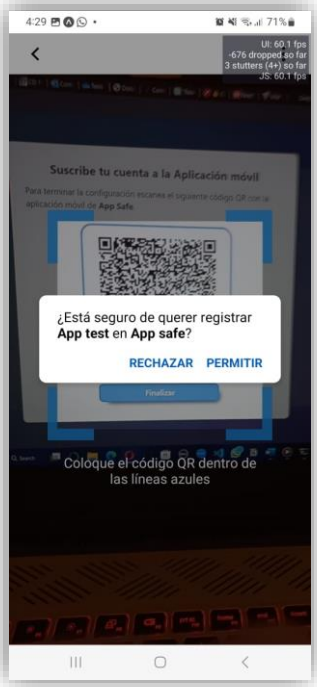
A continuación, se muestra las interfaces principales del prototipo final ejecutándose en un dispositivo de marca Samsung Galaxy A32.

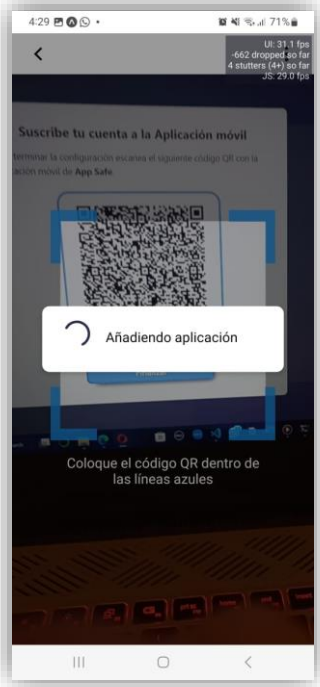

Apps safe


Doble factor de autenticación
Mejora la seguridad de tus aplicaciones mediante la verificación de dos pasos usando contraseñas de un solo uso (OTP)
Siguiente


Aplicaciones registradas
AppSafe (anthonytest1)


Nombre de usuario:
Contraseña
¿Has olvidado tu contraseña?
Iniciar Sesión
Crear Cuenta
Coloque el código QR dentro de las líneas azules


Suscribe tu cuenta a la Aplicación móvil
¿Está seguro de querer registrar App test en App safe?
RECHAZAR
PERMITIR
Coloque el código QR dentro de las líneas azules


Suscribe tu cuenta a la Aplicación móvil
Añadiendo aplicación
Coloque el código QR dentro de las líneas azules

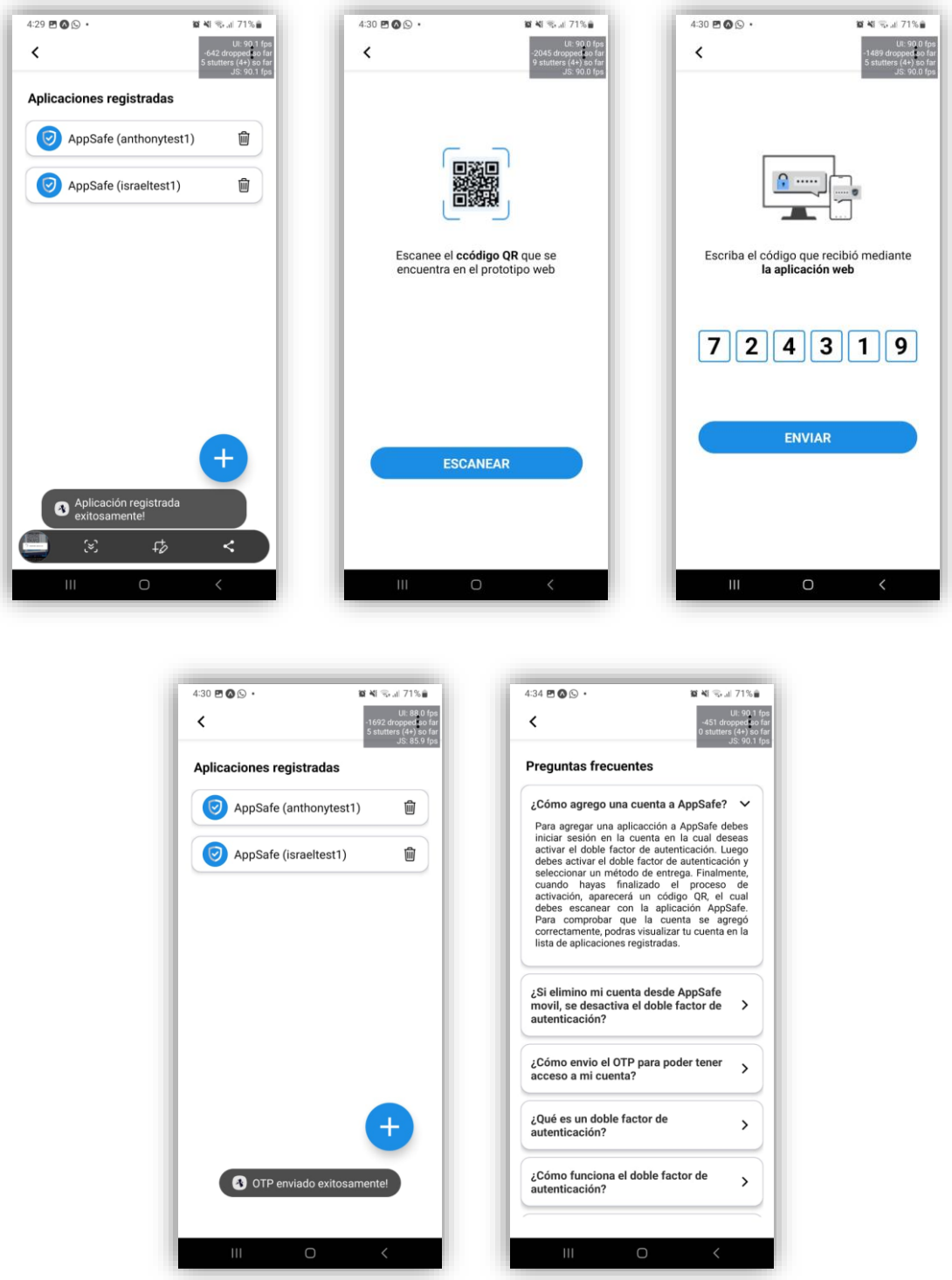


Figura 21. Capturas de pantalla del prototipo móvil funcionando sobre un dispositivo Samsung Galaxy A32

2.4 Pruebas de usabilidad

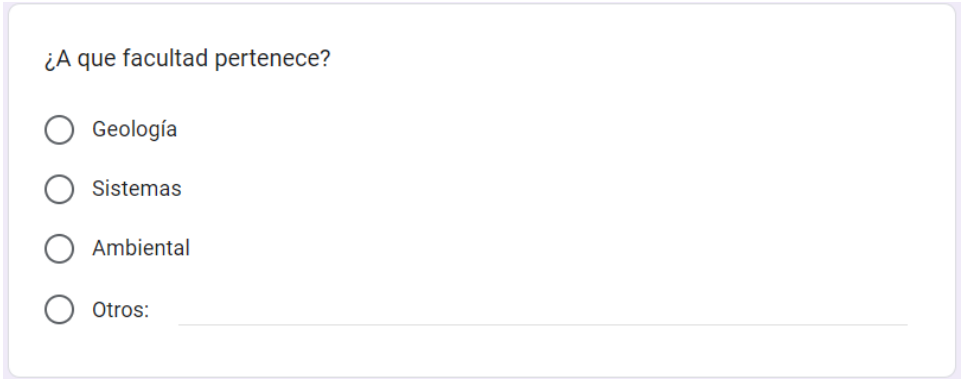
Como se menciona en [16] además de las pruebas y revisiones que se realizan dentro del desarrollo de cada sprint, tambien es necesario realizar pruebas en posibles usuarios finales con la finalidad de conocer algunos aspectos sobre el prototipo móvil como: la facilidad de uso, la aceptabilidad y la accesibilidad del sistema.

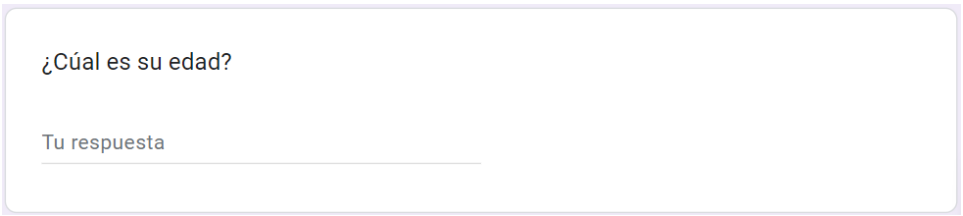
Objetivos de las pruebas

- Encontrar el método de entrega preferido por el usuario de entre las opciones de: correo electrónico, SMS, código QR, texto plano.
- Conocer cuántos usuarios habían usado con anterioridad la autenticación de dos factores.
- Identificar cuantos usuarios estarían dispuestos a usar el doble factor de autenticación luego de haber probado el prototipo móvil.

Definición del cuestionario

Con la finalidad de cumplir con los objetivos anteriormente mencionados, se propuso el siguiente cuestionario a ser llenado por los sujetos que probaron el prototipo móvil.





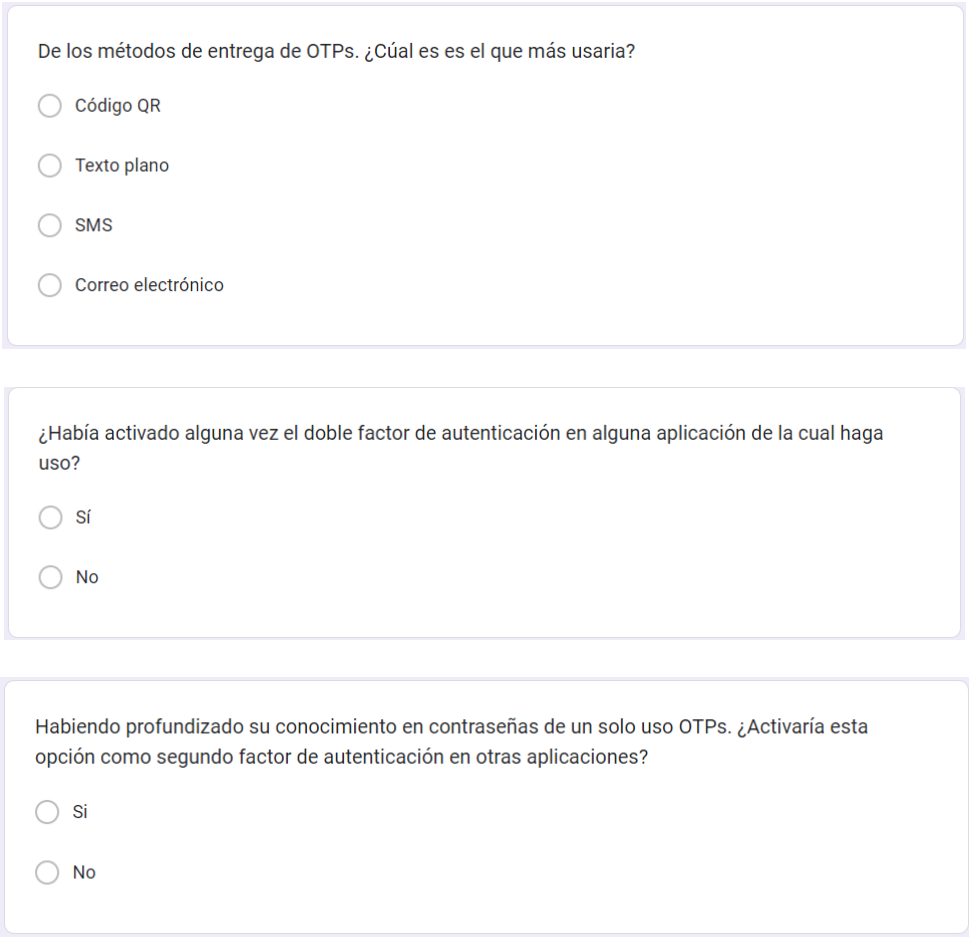


Figura 22. Preguntas correspondientes al cuestionario realizado

Criterio de selección de la muestra

Para llevar a cabo estas pruebas se tomó como muestra a los estudiantes de diferentes facultades de la Escuela Politécnica Nacional. Habiendo obtenido la participación de facultades como: Sistemas, Geología, Ambiental, Mecánica, Ciencias, Telecomunicaciones, Electrónica y Agroindustrial. Se seleccionó a esta población en específico debido a que representan al usuario final, ya que es la población joven la más susceptible al uso de redes sociales, servicios web entre otros [25]. Esto significa que deben gestionar la seguridad de todas sus cuentas.

Planificación

Para realizar las pruebas a los sujetos de pruebas mencionados anteriormente se realizó los siguientes pasos:

- Creación de una cuenta en el prototipo web de prueba.

- Activación del doble factor de autenticación, y selección de uno de los métodos de entrega disponibles.
- Registro del prototipo web en el prototipo móvil.
- Inicio de sesión en el prototipo web con el doble factor de autenticación activado.
- Ingreso del OTP en el prototipo móvil, mismo que fue entregado al usuario por método de entrega previamente seleccionado. Dando como resultado, el acceso a la cuenta del usuario, en el caso de haber ingresado correctamente el OTP.

2.5 Pruebas de rendimiento

En [24] ,se habla sobre algunas formas en las cuales se puede medir el rendimiento de un producto software. Una de estas métricas mencionadas en [24], y la cual se aplicó al presente trabajo fue, el índice de cumplimiento de la tarea para la cual fue diseñada el producto software. Este tipo de métrica tiene un formato binario, debido a que la tarea se llevó a cabo de forma exitosa o no, no existen puntos intermedios.

En el caso del prototipo de aplicación móvil desarrollado en el presente trabajo existen dos tareas principales para las cuales fue diseñado.

- Registro del prototipo web: El usuario debe poder registrar en el prototipo móvil un prototipo web en el cual se ha activado el doble factor de autenticación.
- Envío del OTP: Una vez el usuario haya activado el doble factor de autenticación en el prototipo web y lo haya registrado con éxito en el prototipo móvil. El usuario debe ser capaz de enviar el OTP provisto por el prototipo web a través del prototipo móvil.

Al llevar a cabo las pruebas de usabilidad paralelamente se contabilizó el número de usuarios que no tuvieron problemas en realizar las actividades principales mencionadas anteriormente y cuales tuvieron problemas y no pudieron completar dichas tareas.

3 ANÁLISIS DE RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

3.1 Análisis de resultados de las pruebas de usabilidad

A continuación, se presenta un breve análisis de los resultados obtenidos en cada una de las preguntas realizadas en la encuesta:

Como resultado de la primera pregunta, se muestra la lista de facultades que participaron en las pruebas realizadas al prototipo de aplicación móvil. Teniendo a la facultad de Ingeniería en Sistemas como la facultad con mayor participación en estas pruebas con un 48,8%.

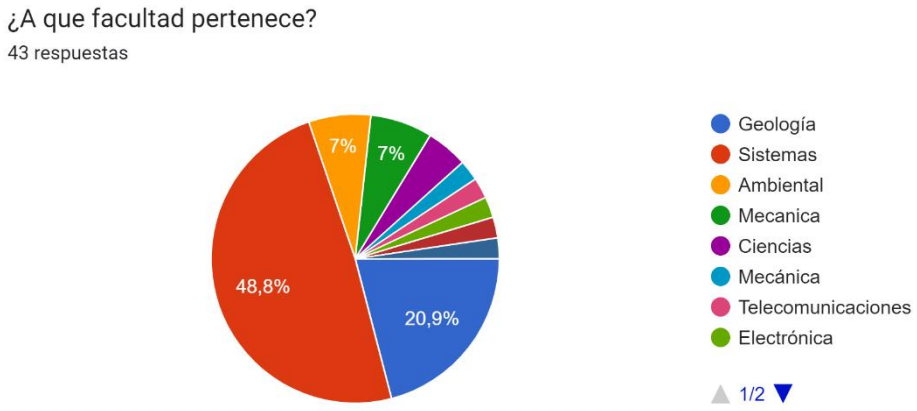


Figura 23. Facultadas que participaron en las pruebas del prototipo

En el caso de la segunda pregunta, se observó que la población se encuentra en un rango de entre 18 y 27 años con un sesgo de una persona de 35 años.

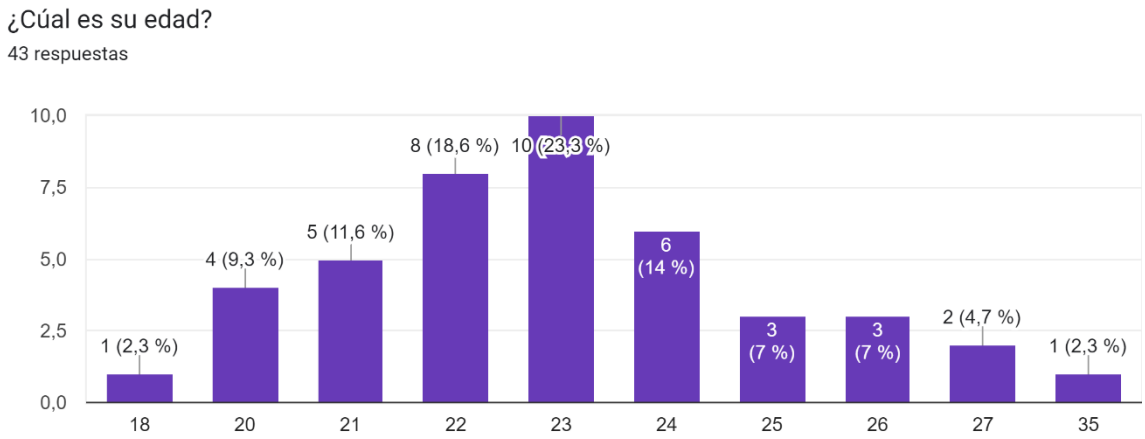


Figura 24. Rango de edades de las personas que realizaron la encuesta

Para la tercera pregunta se puede observar que el método de entrega que más acogida tuvo fue el escaneo de un código QR que contenía la información del OTP con un 65,1%. Según los comentarios hechos por los participantes esto se debe a la rapidez con la que podían acceder a sus cuentas. En según lugar se tiene el método de entrega vía SMS con

un 20,9 %. Algunos usuarios aseguraban estar familiarizados con este método de entrega alegando que era el método utilizado por la entidad bancaria que utilizaban. En el tercer lugar se encuentra el método de entrega en texto plano con un 14%, cabe resaltar que este método de entrega a diferencia de los demás era presentado directamente en el prototipo web. Finalmente, ningún usuario seleccionó el método de entrega por correo electrónico. Según algunos comentarios realizados por los participantes este método de entrega es poco eficiente debido a que implica tener que ingresar a sus cuentas de correo electrónico cada vez que estos quieren acceder a las aplicaciones en las que quieren autenticarse.

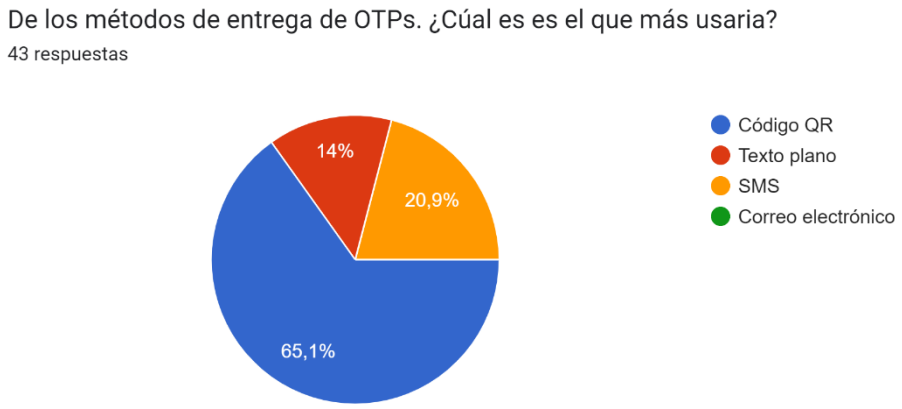


Figura 25. Resultado de los métodos de entrega preferido por los usuarios

Como resultado de la cuarta pregunta, se observó que el 70.7% de los sujetos de prueba habían utilizado alguna vez la autenticación de dos factores en algún servicio web o sistema computacional.

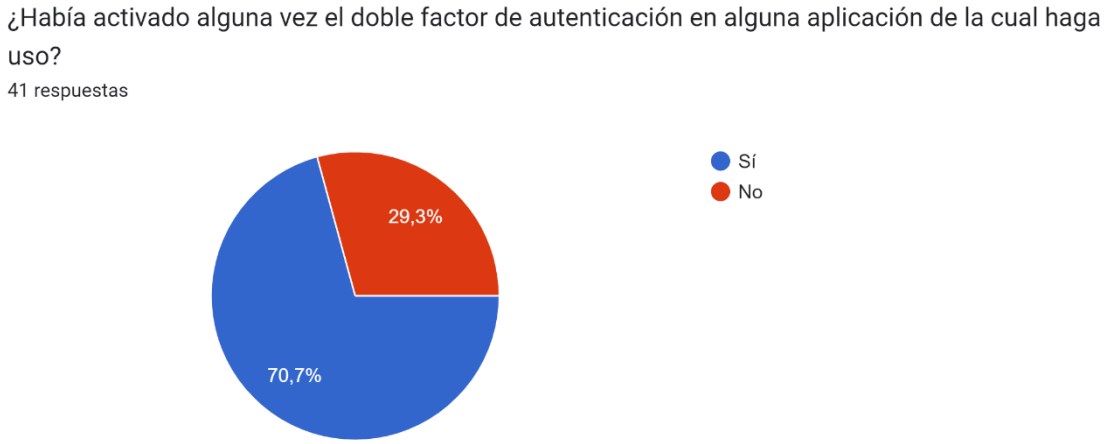


Figura 26. Porcentaje de usuarios que han usado previamente el doble factor de autenticación.

Finalmente, para la pregunta final se puede observar que un 86% de los usuarios están dispuestos a activar el doble factor de autenticación en alguna de sus cuentas. Cabe mencionar que las personas que no lo estaban, aseguraba que el proceso del doble factor de autenticación es un proceso muy tedioso de realizar cada vez que intentan acceder a sus cuentas.

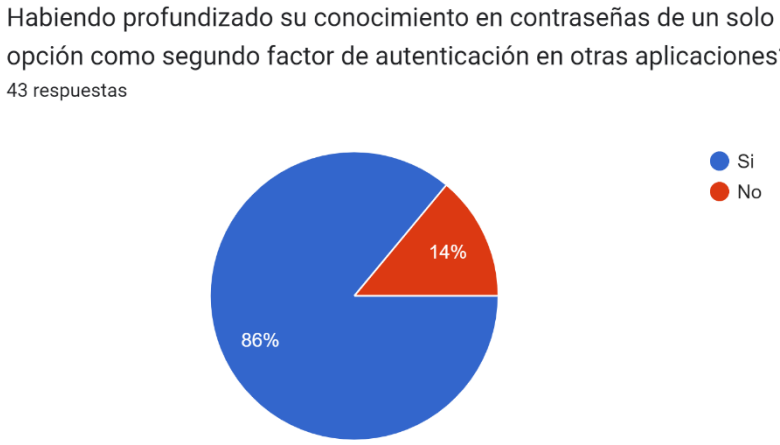


Figura 27. Porcentaje de usuarios que afirma estar dispuesto a activar el doble factor de autenticación en sus aplicaciones

3.2 Análisis de resultados de las pruebas de rendimiento

Como resultado de esta prueba se obtuvo que de los 43 sujetos de prueba 4 no pudieron llevar a cabo las actividades principales de (registro del prototipo web y envío del OTP). Obteniendo un porcentaje de éxito del 91% y una taza de error del 9%.

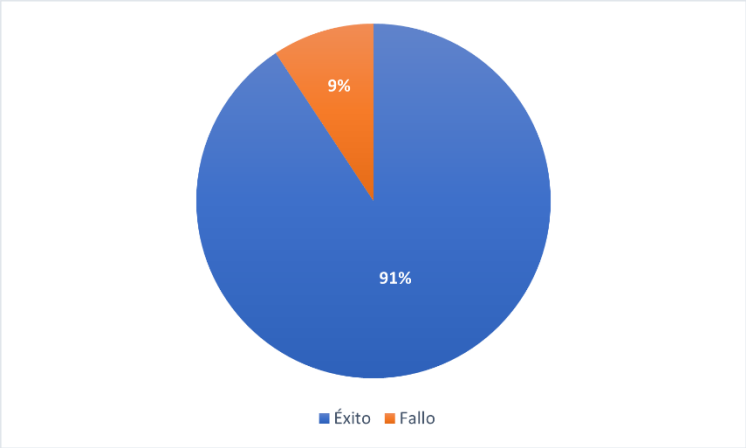


Figura 27. Porcentaje de error y éxito al momento de usar el prototipo de aplicación móvil con los usuarios de prueba

El error por el cual los sujetos de prueba no pudieron cumplir con las tareas principales fue que al momento de que el prototipo móvil debía presentar un cuadro de texto solicitando los permisos de accesos a la cámara del dispositivo, este no aparecía. Este inconveniente se presentó en dispositivos de marca Huawei.

3.3 Conclusiones

Se cumplió el objetivo de crear un prototipo de aplicación móvil de un sistema de autenticación de dos factores, en el cual el primer factor de autenticación es el uso de nombre de usuario y contraseñas mientras que el segundo factor de autenticación está basado en contraseñas de un solo uso. Este prototipo no tiene capacidad de integración con aplicaciones reales como FaceBook, Twitter, Instagram, entre otras.

Como se pudo observar en la revisión de la literatura realizada en el marco teórico, se pudo observar que existen 4 algoritmos de generación de OTPs, los cuales son: OTP, HOTP, TOTP, OTP basado en retos. En la misma sección se observó que existen diferentes formas en los que el valor del OTP es entregado al usuario, por ejemplo: mediante códigos QR, texto plano, SMS, correo electrónico, teléfonos móviles, tokens propietarios e incluso mediante simulaciones acústicas en donde el usuario nunca conoce el valor del OTP.

Este prototipo fue diseñado como parte de un sistema más grande. Las actividades principales que se buscaba realizar con el desarrollo del prototipo fueron:

- Registrar en el prototipo móvil al prototipo web desarrollado por los colaboradores en el cual se haya activado el doble factor de autenticación utilizando One-Time Passwords como segundo factor de autenticación.

- Enviar el OTP generado por el prototipo web a través del prototipo móvil para completar el proceso de autenticación de un usuario.

En cuanto a la implementación del prototipo para dispositivos Android, se observó que se suscitaron errores únicamente con teléfonos de marcas chinas como Huawei y Xiaomi.

3.4 Recomendaciones

Se sugiere implementar un procedimiento de desactivación del doble factor de autenticación, sin que el usuario corra el peligro de perder el acceso a su cuenta en el caso de que el dispositivo en donde se aloja el prototipo de aplicación móvil sufra algún desperfecto, sea robado o se pierda.

En el caso de que se desee probar el prototipo móvil desarrollado en el presente trabajo se recomienda ejecutarlo en dispositivos que utilicen el sistema operativo Android debido a que el desarrollo de este prototipo estuvo enfocado en este sistema operativo en específico.

Teniendo en cuenta que tanto el prototipo móvil como el prototipo web fue probado localmente, es decir, en dispositivos diferentes, pero dentro de la misma red. Se deben configurar las direcciones IP de las APIs a las cuales se le realizan las peticiones.

4 REFERENCIAS BIBLIOGRÁFICAS

[1] J. Zhang, X. Tan, X. Wang, A. Yan, y Z. Qin, “T2FA: Transparent Two-Factor Authentication”, *IEEE Access*, vol. 6, pp. 32677–32686, jun. 2018, doi: 10.1109/ACCESS.2018.2844548.

[2] F. Aloul, S. Zahidi, y W. El-Hajj, “Two factor authentication using mobile phones”, en *2009 IEEE/ACS International Conference on Computer Systems and Applications*, 2009, pp. 641–644. doi: 10.1109/AICCSA.2009.5069395.

[3] D. de Borde, “Selecting a two-factor authentication system”, *Network Security*, vol. 2007, núm. 7, pp. 17–20, jul. 2007, doi: 10.1016/S1353-4858(07)70066-1.

[4] G. Sciarretta, R. Carbone, S. Ranise, y L. Viganò, “Formal Analysis of Mobile Multi-Factor Authentication with Single Sign-On Login”, *ACM Transactions on Privacy and Security*, vol. 23, núm. 3. Association for Computing Machinery, el 1 de julio de 2020. doi: 10.1145/3386685.

[5] S. Ruoti y K. Seamons, “End-to-End Passwords”, 2017, doi: 10.1145/3171533.

[6] E. Erdem y M. T. Sandikkaya, “OTPaaS-One time password as a service”, *IEEE Transactions on Information Forensics and Security*, vol. 14, núm. 3, pp. 743–756, mar. 2018, doi: 10.1109/TIFS.2018.2866025.

[7] K. Aravindhan, “One-time Password: A Survey”, *International Journal of Emerging Trends in Engineering and Development Issue 3*, vol. 1, núm. 3, 2013.

[8] L. Lamport, “Password authentication with insecure communication”, *Commun ACM*, vol. 24, núm. 11, pp. 770–772, nov. 1981, doi: 10.1145/358790.358797.

[9] M. Imanullah y Y. Reswan, “Randomized QR-code scanning for a low-cost secured attendance system”, *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, núm. 4, p. 3762, ago. 2022, doi: 10.11591/ijece.v12i4.pp3762-3769.

[10] Y. Oren y D. Arad, “Toward Usable and Accessible Two-Factor Authentication Based on the Piezo-Gyro Channel”, *IEEE Access*, vol. 10, pp. 19551–19557, 2022, doi: 10.1109/ACCESS.2022.3150519.

[11] S. M. Mitchell y C. B. Seaman, “A comparison of software cost, duration, and quality for waterfall vs. iterative and incremental development: A systematic review”, en *2009 3rd International Symposium on Empirical Software Engineering and Measurement*, oct. 2009, pp. 511–515. doi: 10.1109/ESEM.2009.5314228.

[12] T. Dybå y T. Dingsøyr, “Empirical studies of agile software development: A systematic review”, *Information and Software Technology*, vol. 50, núm. 9–10. pp. 833–859, agosto de 2008. doi: 10.1016/j.infsof.2008.01.006.

[13] E. Hossain, M. Ali Babar, y H. Y. Paik, “Using scrum in global software development: A systematic literature review”, en *Proceedings - 2009 4th IEEE International Conference on Global Software Engineering, ICGSE 2009*, 2009, pp. 175–184. doi: 10.1109/ICGSE.2009.25.

[14] N. B. Moe, T. Dingsøyr, y T. Dybå, “A teamwork model for understanding an agile team: A case study of a Scrum project”, *Inf Softw Technol*, vol. 52, núm. 5, pp. 480–491, may 2010, doi: 10.1016/j.infsof.2009.11.004.

[15] L. Rising y N. S. Janoff, “The Scrum software development process for small teams”, *IEEE Softw*, vol. 17, núm. 4, pp. 26–32, 2000, doi: 10.1109/52.854065.

[16] R. Gershon, N. E. Rothrock, R. T. Hanrahan, L. J. Jansky, M. Harniss, y W. Riley, “The development of a clinical outcomes survey research application: Assessment centerSM”, *Quality of Life Research*, vol. 19, núm. 5, pp. 677–685, jun. 2010, doi: 10.1007/s11136-010-9634-4.

[17] G. Wagenaar, R. Helms, D. Damian, y S. Brinkkemper, “Artefacts in agile software development”, en *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015, vol. 9459, pp. 133–148. doi: 10.1007/978-3-319-26844-6_10.

[18] J. Noll, M. A. Razzak, J. M. Bass, y S. Beecham, “A study of the scrum master’s role”, en *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10611 LNCS, pp. 307–323. doi: 10.1007/978-3-319-69926-4_22.

[19] K. Shah, H. Sinha, y P. Mishra, “Analysis of Cross-Platform Mobile App Development Tools”, en *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, mar. 2019, pp. 1–7. doi: 10.1109/I2CT45611.2019.9033872.

[20] D. Mena y M. Santorum, “Maintainability and Portability Evaluation of the React Native Framework Applying the ISO/IEC 25010”, en *Advances in Intelligent Systems and Computing*, 2021, vol. 1273 AISC, pp. 429–439. doi: 10.1007/978-3-030-59194-6_35.

[21] N. A. Shevtsiv y A. M. Striuk, “Cross platform development vs native development”, 2020. [En línea]. Disponible en: http://mpz.knu.edu.ua/pro-kafedru/vikladachi/224-andrii-striuk

[22] X. Zhou, W. Hu, y G.-P. Liu, “React-Native Based Mobile App for Online Experimentation”, 2020. doi: 10.23919/CCC50068.2020.9189636.

[23] A. Al-Kababji *et al.*, “Energy Data Visualizations on Smartphones for Triggering Behavioral Change: Novel Vs. Conventional”, en *Proceedings - 2020 IEEE 2nd Global Power, Energy and Communication Conference, GPECOM 2020*, oct. 2020, pp. 312–317. doi: 10.1109/GPECOM49333.2020.9247901.

[24] A. Suzianti y A. Belahakki, “Redesigning User Interface of MRT Jakarta’s Mobile Application using Usability Testing Approach”, en *ACM International Conference Proceeding Series*, sep. 2020, pp. 73–78. doi: 10.1145/3429551.3429587.

[25] T. A. Pempek, Y. A. Yermolayeva, y S. L. Calvert, “College students’ social networking experiences on Facebook”, *J Appl Dev Psychol*, vol. 30, núm. 3, pp. 227–238, may 2009, doi: 10.1016/j.appdev.2008.12.010.

5 ANEXOS

5.1 Anexo I. Diseño de interfaces en Figma

Enlace al diseño de interfaces en Figma: https://www.figma.com/file/EoZ6Mj6v6OTTiH27BUfe9L/High-Fidelity-Android?node-id=1%3A935&t=RRgFOI3baasB2Roo-1

5.2 Anexo II. Criterios de aceptación para el Sprint 1

Criterios de aceptación					
Escenario	**Título**	**Contexto**	**Evento**	**Acción**	**Cumplido**
1	Primer Inicio prototipo	El usuario final acaba instalar el prototipo	El usuario final ejecuta el prototipo por primera vez	Se presenta el logo de la aplicación y automáticamente se redirige al usuario a la primera interfaz de introducción	Si
2	Bienvenida pág. 1	El usuario final se encuentra en la primera interfaz de introducción	El usuario final se desliza hacia la izquierda	Se muestra la segunda interfaz de introducción	Si
			El usuario final se desliza hacia la derecha	Se mantendrá en la misma interfaz	Si
			El usuario final da click en el botón siguiente	Se muestra la segunda interfaz de introducción	Si
3	Bienvenida pág. 2	El usuario final se encuentra en la segunda interfaz de introducción	El usuario final se desliza hacia la izquierda	Se muestra la tercera interfaz de introducción	Si
			El usuario final se desliza hacia la derecha	Se muestra la primera interfaz de introducción	Si
			El usuario final da click en el botón siguiente	Se muestra la tercera interfaz de introducción	Si
4	Bienvenida pág. 3	El usuario final se encuentra en la tercera	El usuario final se desliza hacia la izquierda	Se mantendrá en la misma interfaz	Si

		interfaz de introducción	El usuario final se desliza hacia la derecha	Se muestra la segunda interfaz de introducción	Si
			El usuario final da click en el botón comenzar	Se muestra la interfaz de registro de la primera aplicación.	Si
5	Segundo y siguientes inicios del prototipo	El usuario final ya ha ejecutado el prototipo anteriormente	El usuario final ejecuta el prototipo por segunda o más veces sin haber registrado ninguna aplicación	Se muestra la interfaz que lista las aplicaciones registradas	Si
			El usuario final ejecuta el prototipo por segunda o más veces ya habiendo registrado aplicaciones anteriormente	Se muestra la interfaz que lista las aplicaciones registradas	Si
6	Menú Bar	El usuario final se encuentra en la interfaz que lista las aplicaciones registradas y ha seleccionado la opción del Menú Bar	El usuario final ha seleccionado la opción de "Como funciona"	Se redirige al usuario a la primera interfaz de introducción	Si
			El usuario final ha seleccionado la opción de "Preguntas frecuentes"	Se muestra la interfaz que contiene una lista con las preguntas frecuentes referentes al funcionamiento del prototipo	Si

5.3 Anexo III. Criterios de aceptación para el Sprint 2

Criterios de aceptación					
Escenario	**Título**	**Contexto**	**Evento**	**Acción**	**Realizado**
1	Primer registro de aplicación	El usuario final acaba finalizar la introducción al funcionamiento del prototipo y se encuentra en la interfaz de registro de una aplicación.	El usuario final selecciona la opción de registro de una aplicación mediante un código QR	Se muestra una interfaz en donde se le preguntara al usuario si desea dar acceso a la cámara del dispositivo para poder escanear el código QR	Si
2	Permiso de accesos a la cámara del dispositivo	El usuario final ha seleccionado la opción de registrar una aplicación mediante un código QR y se le ha preguntado si desea dar permiso a la cámara del dispositivo	El usuario final da click en la opción de aceptar para así permitir el acceso a la cámara del dispositivo	Se muestra una interfaz que permita al usuario escanear cualquier código QR	Si
			El usuario final da click en la opción de cancelar para así negar el acceso a la cámara del dispositivo	Se emite un mensaje que indica al usuario que se necesitan los permisos a la cámara del dispositivo para poder registrar una aplicación y se vuelve a solicitar el permiso	Si
3	Escaneo del código QR para activar el 2FA	El usuario final acaba de otorgar los permisos a la cámara del dispositivo	El usuario final escanea un código QR válido para registrar una aplicación en la que desea activar el 2FA	Se verifica que el código QR sea válido y se muestra un mensaje de confirmación	Si

			El usuario final escanea un código QR no válido para registrar una aplicación en la que desea activar el 2FA	Se emite un mensaje que indica al usuario que el código QR escaneado no pertenece a ninguna aplicación que esté tratando de activar el 2FA	Si
4	Adición de una nueva aplicación	EL usuario ha escaneado un código QR válido y se le ha mostrado un mensaje de confirmación para agregar o no la aplicación	El usuario final selección la opción aceptar	Se muestra la interfaz que listará todas las aplicaciones registradas	Si
			El usuario final selecciona la opción cancelar	Se quita el mensaje de confirmación y se muestra la interfaz que permite al usuario escanear cualquier código QR	Si
5	Actualización del método de entrega una aplicación previamente registrada	El usuario ya ha registrado una aplicación web, pero genera un nuevo código QR de registro con un método de entrega diferente. Lo escanea, y se muestra el mensaje de confirmación de registro de aplicación	El usuario selecciona la opción de aceptar	Se muestra un mensaje de confirmación de actualización de registro de aplicación y se pasa a la interfaz de lista de aplicaciones registradas	Si
			El usuario selecciona la opción de cancelar	Se realiza una transición a la pantalla de lista de aplicaciones registradas	Si

6	Eliminar una cuenta del prototipo móvil	El usuario se encuentra en la interfaz de lista de aplicaciones	El usuario presiona el ícono de eliminar de una aplicación de la lista	Se muestra un mensaje que le pide la verificación al usuario si desea proceder con el proceso de eliminación de la cuenta seleccionada	Si
7	Confirmación de eliminación de una cuenta	El usuario ha presionado el ícono de eliminar cuenta, y se le ha mostrado un mensaje de pidiendo al usuario que confirme su acción	El usuario selecciona la opción aceptar	El prototipo elimina el registro correspondiente a esa aplicación en la base de datos y actualiza la lista de aplicaciones registradas	Si
			El usuario selecciona la opción de cancelar	El prototipo quita el mensaje de confirmación y sin realizar ninguna acción adicional muestra la interfaz de lista de aplicaciones registradas	Si

5.4 Anexo IV. Criterios de aceptación para el Sprint 3

Criterios de aceptación					
Escenario	**Título**	**Contexto**	**Evento**	**Acción**	**Cumplido**
1	ingreso mediante código QR (escaneo del OTP mediante el prototipo)	El usuario final habiendo activado el 2FA en el prototipo web, habiendo seleccionado el método de entrega por código QR y habiendo registrado la aplicación en el prototipo	El usuario final dentro de la lista de aplicaciones registradas selecciona la aplicación en la que desea autenticarse	Se muestra la interfaz que permitirá escanear cualquier código QR	Si

		móvil, desea ingresar a la aplicación web y se le solicita que ingrese el OTP en el prototipo.			
2	Ingreso del OTP manualmente (digitado por el usuario final)	El usuario final habiendo activado el 2FA en el prototipo web, habiendo seleccionado el método de entrega por código SMS, correo electrónico o texto plano y habiendo registrado la aplicación en el prototipo móvil, desea ingresar a la aplicación web y se le solicita que ingrese el OTP en el prototipo	El usuario final dentro de la lista de aplicaciones registradas selecciona la aplicación en la que desea autenticarse	Se muestra una interfaz que permitirá al usuario digitar el valor del OTP enviado por SMS, correo electrónico o mostrado en texto plano	Si
3	Envío del OTP	El usuario ya ha ingresado o escaneado el OTP	El valor del OTP se ha enviado exitosamente	Se muestra un mensaje que indique al usuario que el OTP se ha enviado exitosamente	Si
			El valor del OTP no ha podido enviarse	Se muestra un mensaje que indique al usuario final que ha ocurrido un	Si

				error al enviar el OTP	

5.5 Anexo V. Enlace al repositorio donde se encuentra el código fuente del prototipo de aplicación móvil

Enlace al repositorio del código del prototipo móvil: https://github.com/Isr43l86/OTP-Client