DESARROLLO DE UN MÓDULO DE REGISTRO DE USUARIO PARA LA APLICACIÓN CONECTA2

ANDRÉS FELIPE BARRAGÁN JAIMES

Directora de investigación:
MARIA DEL PILAR SALAMANCA AZULA

UNIVERSIDAD ANTONIO NARIÑO
FACULTAD DE INGENIERÍA DE SISTEMAS
PROGRAMA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
BOGOTÁ
2021

DESARROLLO DE UN MÓDULO DE REGISTRO DE USUARIO PARA LA APLICACIÓN CONECTA2

DEDICATORIA

Este proyecto de grado va dedicado a mis tías María Barragan y Yolanda Barragan quienes las considero mis segundas madres, mi padre Luis F. Barragán, mi hermano Luis G. Barragán, mi tío Enrique Barragán, y mi madre Lisbeth Jaimes, quienes me han dado el apoyo de todas las formas posibles para llevar a cabo mi proyecto personal y darme varios consejos para superar los obstáculos que se me presentaron en la carrera.

AGRADECIMIENTOS

Agradezco a las personas que han sido parte en mi proceso de aprendizaje, a mis amigos, en especial a Danilo Beleño y Sebastián Suarez quienes me han ayudado con sus conocimientos y han sido un apoyo en mi vida universitaria, a aquellos docentes que me enseñaron sobre la carrera y sus experiencias, a la institución por dejarme ser parte de una comunidad tan profesional y al semillero de investigación LACSER por permitirme ser parte de un proyecto tan prometedor como lo es Conecta2.

Finalmente, agradezco a mi directora de proyecto María del Pilar Salamanca por su acompañamiento, ayuda y dedicación constante en este proceso, quien junto a ella fue posible la culminación de este trabajo de grado.

CONTENIDO

Pág.

INDICE DE FIGURAS

Pag.

ÍNDICE DE TABLAS

Pag.

RESUMEN

Conecta2 es una aplicación prototipo para sistema operativo Android que permite el intercambio de mensajes de texto, audio y fotografías entre teléfonos inteligentes cercanos, inclusive cuando la red de telefonía celular no está disponible, ya que emplea las tecnologías de comunicación Wi-Fi Direct y Bluetooth. Esta aplicación fue diseñada con el propósito de facilitar la comunicación entre sobrevivientes después de un desastre, para permitir la colaboración y rescate de personas en caso de que las redes de comunicación queden fuera de servicio después de una catástrofe. Actualmente, la aplicación carece de un módulo de registro y únicamente le solicita al usuario escribir su nombre y el nombre que va a tener su celular, y con esta información identifica al usuario en la red, lo cual no da certeza de quien es en realidad. En este trabajo de grado se desarrolló un módulo de registro de usuario para Conecta2, cuyo objetivo es reducir la posibilidad de creación de perfiles falsos a partir de un registro más completo, que proporciona datos específicos de la persona que esté en la red. El módulo de registro solicita al usuario que ingrese sus datos de identificación manualmente. Luego, a partir de la lectura del código de barras de su documento de identidad, verifica que los datos diligenciados sean correctos y, finalmente, confirma el número del celular mediante el uso de mensajes SMS. Para el desarrollo de este proyecto se utilizó el entorno de desarrollo Android Studio y se usó la metodología Mobile-D.

INTRODUCCIÓN

Conecta2 es una aplicación prototipo para sistema operativo Android que permite el intercambio de mensajes de texto, audio y fotografías entre teléfonos inteligentes cercanos, inclusive cuando la red de telefonía celular está indisponible. Añadido a esto, facilita, además, que los usuarios de los teléfonos en los cuales se encuentra instalada la aplicación, puedan conocer la distancia que los separa entre sí, mediante el intercambio de las coordenadas obtenidas por el sensor de posicionamiento global (GPS). De esta manera, sirve como una alternativa de comunicación en situaciones de emergencia y facilita la colaboración entre sobrevivientes y el proceso de búsqueda de personas. Esta aplicación ofrece estas funcionalidades mediante el establecimiento de una red ad hoc entre dispositivos cercanos utilizando las tecnologías Wi-Fi Direct y Bluetooth (Castañeda, 2019).

Actualmente, Conecta2 no ofrece un registro seguro y verídico para sus usuarios. Por el momento solo se le pide al usuario que indique su nombre y el nombre que desea dar a su teléfono, haciendo que en el caso de que se presente un desastre natural, cualquier persona pueda entrar en la red y comunicar mensajes de solicitud de rescate, anunciando un nombre diferente a su nombre real. Esto sería un problema para las personas que estén vinculadas a la red, dado que cualquier usuario podría estar suplantando a otra persona. Adicionalmente, si después del desastre un usuario que no haya colocado información verídica en la aplicación tiene alguna dificultad de salud que le impida comunicarse, será difícil determinar su identidad real.

Con el fin de mejorar la veracidad de la información que Conecta2 muestra sobre los usuarios vinculados a la red, este trabajo de grado desarrolla un módulo de registro de usuarios para Conecta2. En el nuevo módulo se usa una API que permite el escaneo del código de barras 2D presente en los documentos de identidad, tales como tarjeta de identidad, cédula de ciudadanía y cédula de extranjería, los cuales

utilizan el formato de código de barras PDF417 que permite codificar gran cantidad de información (Cognex, s.f). El escaneo se realiza con la cámara del celular y permite, de una manera fácil y rápida, verificar que los datos que el usuario diligenció manualmente sean correctos. El código de barras, además del nombre y número de identificación, almacena información importante como el grupo sanguíneo del usuario, estos datos verificados podrían eventualmente facilitar el trabajo de los especialistas en rescates, al contar con información que permita atender con prontitud al usuario.

Esta implementación ayuda en gran medida a reducir la probabilidad de creación de perfiles falsos, pues solo podrá existir un registro por cada documento de identificación, y la información del registro únicamente puede corresponder con la que se encuentra en el documento de identificación del usuario. El proceso de registro es más riguroso, además, porque se efectúa el envío de un mensaje SMS que envía un PIN al número celular que el usuario proporcionó durante el registro, esto funciona como una forma de verificar que el número proporcionado es real. Sin embargo, por limitaciones de presupuesto no se puede comprobar si el registro se está realizando con el documento de identidad de una persona fallecida, y tampoco se agregó una autenticación biométrica, pues no todos los celulares poseen la tecnología para realizarla.

En cuanto a la metodología, se usó Mobile-D, que está centrada en el desarrollo de aplicaciones móviles, para equipos que no superen los 10 integrantes en un espacio físico. Es una combinación de varias metodologías incluyendo el modelo en cascada, pues al completar una de sus fases, no se debe devolver a una fase finalizada; sin embargo, sí existe la iteración de actividades dentro de una fase, pues se verifica que las actividades cubran los requerimientos planteados desde un inicio y, de no estarlo, se procede a volver a la primera actividad de la fase para poder solucionar y verificar qué se ejecutó mal. Se contemplan las siguientes fases,

exploración, iniciación, producción, estabilización, pruebas y reparación, las cuales se explican más adelante (Balaguera, 2015).

Para implementar este nuevo módulo se continuó usando Android Studio, que es el entorno en el que se desarrolló la primera versión de Conecta2, junto con los extras, ya sea para insertar nueva visual o funciones adicionales que ayuden a mejorar la usabilidad de este módulo. Por último, se actualizó la aplicación para que el nombre del usuario sea el mismo en todos los módulos de la aplicación.

Este documento está estructurado de la siguiente manera: el capítulo 1 presenta el planteamiento del problema, en el cual se describe el problema encontrado, su formulación y la justificación del proyecto. Se plantean el objetivo general y los específicos para finalmente describir el alcance y limitaciones que tendrá el desarrollo del nuevo módulo. El capítulo 2 presenta el marco de referencia, donde se comparan algunas aplicaciones que poseen funcionalidades semejantes; este capítulo también contiene el marco legal que se tendrá en cuenta en el desarrollo de software planteado. El capítulo 3 explica de manera detallada la metodología Mobile–D, la cual es la más indicada para el desarrollo de aplicaciones móviles. El capítulo 4 describe el desarrollo del proyecto y cómo se implementó la metodología Mobile-D. En el capítulo 5 se revisan los resultados, verificando el cumplimiento de los objetivos. Para terminar, el capítulo 6 presenta las conclusiones y recomendaciones del proyecto.

1. PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN DEL PROBLEMA

Conecta2 es una aplicación prototipo, que permite conectarse a una red ad hoc con otros dispositivos cercanos, utilizando las tecnologías Wi-Fi Direct y Bluetooth, las cuales permiten crear una red de alcance local cuando no hay una red de telefonía celular disponible. Esta aplicación da la posibilidad de establecer un chat con los dispositivos que estén conectados a la red mediante la aplicación, y permite saber la distancia entre los dispositivos gracias a que en la red se intercambian las coordenadas que se obtienen mediante el sensor de posicionamiento global (GPS). La funcionalidad de Conecta2 hace que sea una opción de comunicación en el caso de un desastre natural, ya que puede ayudar en la búsqueda de sobrevivientes y facilitar la colaboración entre los usuarios de la red (Castañeda, 2019).

Actualmente, el módulo de registro de la aplicación Conecta2 le pide al usuario que escriba su nombre y el nombre que recibirá su teléfono celular en la red, y los almacena localmente. Como el usuario es libre de escribir lo que desee y no hay ningún tipo de validación de los datos ingresados, las personas que tengan la aplicación instalada pueden llegar a crear un perfil *"falso"* donde, por ejemplo, pueden anunciar un nombre que no les corresponde, engañando de esta manera a los usuarios que estén vinculados a la red, incluyendo a personas que hayan asumido el rol de rescatistas. Una persona que se registra con información falsa podría tener malas intenciones como solicitar un rescate que no es requerido, llegando a retrasar o incluso sabotear una posible búsqueda en medio de un desastre o emergencia. Adicionalmente, podría generar falsas expectativas en los usuarios vinculados a la red, quienes eventualmente podrían conocer a la persona que se anuncia en el falso perfil.

Por otra parte, Conecta2 no tiene consistencia en el nombre con el que se anuncia al dispositivo en sus diferentes módulos: en algunos lo identifica con el nombre del usuario, en otros con el nombre del teléfono. Lo anterior dificulta la identificación del dispositivo dentro de la red y, consecuentemente, de la persona que lo está utilizando.

Por último, Conecta2 no facilita al rescatista información adicional del sobreviviente. Sería valioso conocer, por ejemplo, el grupo sanguíneo del usuario de la aplicación y su edad, en caso de que la persona no se pueda comunicar o que no pueda recordar quién es. Con esos datos, un rescatista tendría elementos suficientes para solicitar sangre, en caso de que se requiera, o podría realizar un chequeo rápido al paciente, teniendo en cuenta su edad.

1.2. FORMULACIÓN DEL PROBLEMA

Con el desarrollo de un nuevo módulo de registro y autenticación de usuarios para la aplicación móvil Conecta2, se disminuirá la posibilidad de creación de perfiles falsos en la red gracias a la verificación que se realiza escaneando el código de barras del documento con los datos registrados manualmente, para luego comprobar que el dispositivo sí posee el número celular del usuario mediante SMS.

1.3. JUSTIFICACIÓN

En caso de un desastre, los usuarios que tengan instalada la aplicación Conecta2 en su teléfono inteligente, tendrán a mano un buen recurso para colaborar y solicitar ayuda al resto de usuarios que estén conectados a la red. Sin embargo, hoy por hoy la aplicación solo tiene un registro simple, que consiste en escribir el nombre de usuario y el nombre que quiere que tenga el dispositivo. Para que la información que ofrece Conecta2 sobre sus usuarios sea veraz y más completa, es necesario tener un registro de usuarios más riguroso, que valide si el usuario ya estaba

registrado y que almacene, además del nombre y el número de identificación, otros datos que sean útiles en caso de que el usuario requiera atención médica. Por este motivo, el presente módulo evita la posibilidad de crear dos perfiles idénticos y permite identificar, con mayor certeza, quién es la persona que está en la red gracias al registro mediante su documento de identidad. De esta manera, este nuevo módulo evita la creación de dos perfiles idénticos y permite identificar quién es la persona que está en la red gracias al registro mediante su documento de identidad.

Finalmente se realiza una verificación del número de celular que indicó el usuario mediante el envío de un mensaje SMS con un código.

Actualmente, existen aplicaciones para escanear códigos de barras y otras para realizar consultas, sin embargo, algunas tienen limitaciones al capturar la información o son aplicaciones de pago, por lo que este nuevo módulo agrega valor a la aplicación Conecta2, sin costo adicional. Aunque para el desarrollo y pruebas iniciales de este trabajo de grado se usa SQLite para almacenar la información que se captura, para la implementación final se usó Firebase para el almacenamiento en la nube y validación de mensaje SMS.

Socialmente, el nuevo módulo captura la información del documento de identidad, que puede facilitar el proceso de atención de un usuario; por ejemplo, si es una persona mayor, en caso de que esté perdiendo sangre, los usuarios conectados a esa red sabrán a qué grupo sanguíneo pertenece esa persona y así poder darle una atención más rápida en el momento en el que los especialistas en rescate lleguen a encontrarlo.

Tecnológicamente, este módulo evita la duplicidad de registros, y reduce la posibilidad de crear falsos perfiles. Además, es un sistema de registro innovador para la aplicación Conecta2, ya que, de las indagaciones realizadas, no hay alguna aplicación de registro para implementarla directamente con Conecta2.

Profesionalmente, el aporte de este proyecto se enfoca en profundizar los conocimientos en programación móvil, ya que se implementa un módulo nuevo a una aplicación ya creada y se realiza la integración, manteniendo la compatibilidad de la aplicación. También permite profundizar los conocimientos en cuanto al procedimiento para conectarse a una base de datos en un desarrollo móvil, pues no se realiza de la misma manera que un desarrollo para ordenador.

1.4. OBJETIVOS

1.4.1. Objetivo general

Desarrollar un nuevo módulo de registro y autenticación de usuarios para la aplicación móvil Conecta2, mediante Android Studio, con el fin de disminuir la posibilidad de creación de perfiles falsos en la red con ayuda del escaneo de los documentos de identidad colombianos.

1.4.2. Objetivos específicos

1. Obtener la información del usuario a partir del escaneo del código de barras del documento de identificación y la captura de esa información, con el propósito de reducir la probabilidad de ingresar información falsa durante el registro.
2. Verificar el número de teléfono celular ingresado en el momento del registro del usuario por medio del envío de un mensaje SMS, con el fin de validar la información digitada por el usuario.
3. Integrar el módulo de registro y autenticación a la aplicación Conecta2, con el propósito de reducir la posibilidad de registro de falsos usuarios en la red.

4. Usar la información capturada durante el registro para identificar al usuario en los demás módulos de Conecta2, de manera que la identificación del usuario sea consistente en toda la aplicación.

1.5. ALCANCE Y LIMITACIONES DEL PROYECTO

1.5.1. Alcance

Los elementos tecnológicos que se usan en el desarrollo e implementación de este módulo son:

- **Back-end:** se usó Android Studio, pues la aplicación prototipo está desarrollado en este entorno de desarrollo. Se continuó con este entorno para garantizar la compatibilidad del nuevo módulo, la función de registro y captura de datos para los demás módulos.
- **Front-end:** el diseño del nuevo módulo se realizó con las librerías que proporciona el ambiente de desarrollo Android Studio, pues se efectuaron varias pruebas para acomodar el diseño y que se adaptara a la aplicación móvil Conecta2.
- **Base de datos:** se usó inicialmente SQLite, la base de datos básica para Android Studio, donde se realizaron las pruebas pertinentes de almacenado; posteriormente, se usa Firebase para verificar que se guarden correctamente los datos en la nube, junto con la autenticación SMS.
- **Captura de información de los documentos de identidad:** se utiliza una API que permite el escaneo de código de barras 2D en formato PDF417 y de manera aparte, se compara la con la información diligenciada por el usuario.

El alcance del módulo de registro y autenticación contempla:

- El registro funciona como un formulario que captura la información que el cliente aceptó proporcionar.
- Para el primer registro es necesario que el usuario se conecte a internet, pues se almacenarán los datos validados del documento de identificación, junto con el número de celular. Posteriormente se verifica dicho número mediante SMS.
- Es importante el haber agregado una autenticación de usuario que garantice en cierta medida que la cuenta creada le pertenece solamente a una persona mediante la validación en la base de datos en la nube.

1.5.2. Limitaciones

Al implementar esté nuevo módulo, las limitaciones serán las siguientes:

- Por limitaciones de presupuesto, se utiliza una base de datos gratuita que permite la creación de una cantidad reducida de registros.
- Solamente se captura la información de los documentos de identificación de Colombia para el registro de los usuarios.
- El módulo mejora en gran medida la seguridad del primer prototipo, pero no garantiza la posible suplantación de identidad que se pueda presentar si alguien se registra con el documento de identidad de otra persona, de una persona fallecida o un documento extraviado.
- Cuando el usuario desinstale la aplicación directamente, previamente debe borrar su perfil, siguiendo el procedimiento explicado en el Manual de Usuario. De otra manera, cuando reinstale la aplicación, no se podrá registrar de nuevo. Esta es la operación para este prototipo, posteriormente se diseñará un procedimiento más eficiente para recuperar un perfil previamente creado.

2. MARCO DE REFERENCIA

2.1. MARCO TEÓRICO

En esta sección se presentan algunas definiciones necesarias para comprender el desarrollo de este trabajo de grado y la metodología que se usó para su realización.

2.2. METODOLOGÍA MOBILE-D

La metodología Mobile-D es una metodología propuesta hacia 2004, resultado de la combinación de varias metodologías en la que se intentaba proponer un paso a paso de lo que se debe hacer para desarrollo en dispositivos móviles y para equipos pequeños. Esta metodología surge para crear una nueva manera de realizar actividades para equipos de trabajo que no pasaran de 10 miembros en un solo lugar físico, por lo que se convierte en un buen recurso para mantener un orden en el desarrollo de software para grupos pequeños (Balaguera, 2015).

Mobile-D propone un modelo lineal, lo que significa que, al terminar una etapa, continúa otra y no hay que volver atrás, pues en cada fase se deben dejar claros los requerimientos del sistema. Este modelo se caracteriza por poder entregarle al cliente en el último encuentro antes de comenzar el desarrollo, el costo y lo que se tendrá cuenta y lo que no en el producto final. Esto lo diferencia de, por ejemplo, los modelos de desarrollo ágil, cuya principal característica es reunirse con el cliente cada cierto tiempo, pues puede haber cambios de acuerdo a como lo vea el cliente y/o a las limitaciones que tenga el equipo de desarrollo. Mobile-D toma elementos del modelo en cascada, pues como se dijo anteriormente, cada fase posee sus entregables y no se debe volver a una fase anterior, ya que esto implica cambios que pueden tener costos que no fueron contemplados desde el comienzo (IONOS, 2019).

A continuación, se describen las fases que posee esta metodología y las etapas que la componen.

2.2.1. Exploración

En esta fase se llevan a cabo reuniones en las que se determina el alcance y limitaciones del proyecto. También se aclara qué funcionalidades tendrá, qué se recomienda agregar, se propone un diseño de la interfaz y las herramientas que se usarán para poder realizar el software que se solicitó. Posee las siguientes etapas:

- Establecimiento de actores: se identifican los grupos de interés necesarios para cumplir las diferentes tareas que se plantean. Además de esto, se identifican los tipos de usuarios finales que usarán la aplicación (Gómez & Hernández, 2016).
- Definición del alcance: se definen los objetivos dentro del proyecto, el tiempo que durará cada etapa futura y los requisitos que se deberán cumplir al final del proyecto (Gómez & Hernández, 2016).
- Establecimiento de proyectos: se explica qué recursos se necesitan para dar inicio al desarrollo del proyecto (Gómez & Hernández, 2016).

2.2.2. Iniciación

En esta fase, se planifican los procesos que se requieren para el desarrollo, y se elaboran ejemplos de interfaces que se pueden usar, esto para darle al usuario final una vista agradable y fácil de entender. Se incluyen también los recursos tanto tecnológicos como físicos y se documentan los avances de la fase. Las etapas que conforman esta fase son las siguientes:

- Puesta en marcha del proyecto: en esta etapa se determinan los recursos disponibles, tanto humanos como tecnológicos, el nivel de conocimientos del

equipo de desarrollo y el lugar de trabajo en el que se encontrarán las personas que participarán en el proyecto (Gómez & Hernández, 2016).

- Planificación inicial: en esta etapa, se trabaja en la comprensión del producto que se desarrollará, y se realiza una planificación de todo lo que se tendrá en cuenta en las siguientes etapas y fases (Gómez & Hernández, 2016).
- Día de la prueba: en esta etapa se realizan pruebas para la implementación de algunas funciones, estas no deben producir ningún código de trabajo, más bien hace alusión a posibles servicios que se vayan a utilizar (Gómez & Hernández, 2016).
- Día de salida: se refiere al momento en el que todo debe estar listo para poder empezar con la fase de producción (Gómez & Hernández, 2016).

Finalmente se verifica que todos los requerimientos estén bien especificados para asegurar que no habrán cambios drásticos en alguna de las siguientes fases (Balaguera, 2015).

2.2.3. Producción

En esta fase se realizan iterativamente, hasta cumplir con los requerimientos, las siguientes etapas en el tiempo establecido. Estas son:

- Planificación: luego de haber dejado claros los requerimientos, se procede a planificar las actividades a realizar en el desarrollo (Gómez & Hernández, 2016).
- Trabajo: en esta etapa se desarrolla el código fuente, teniendo en cuenta la planificación realizada con anterioridad, implementando las funcionalidades de alta prioridad definidas en los requisitos (Gómez & Hernández, 2016).
- Liberación: se lanza una versión totalmente funcional del desarrollo realizado en la anterior etapa, integrando subsistemas creados, pruebas de prelanzamiento, pruebas de aceptación y una ceremonia de lanzamiento

para confirmar que se completó satisfactoriamente la iteración (Gómez & Hernández, 2016).

La repetición de estas etapas se lleva a cabo hasta implementar todas las funcionalidades. En otras palabras, esta fase es donde se realiza la codificación del módulo, añadiendo cambios a un repositorio que se genera con anterioridad. Junto con esto, se añaden las pruebas de aceptación, que sirven para saber si se terminó con la fase o no (Balaguera, 2015).

2.2.4. Estabilización

Luego de haber terminado con la fase de implementación, se procede a la fase de estabilización, donde se realiza la integración final de las diferentes partes que conforman el proyecto, verificando que el desarrollo realizado cumpla con el objetivo general y los objetivos específicos. Por último, se realiza la documentación necesaria para los entregables al cliente (Balaguera, 2015).

2.2.5. Prueba y reparación

La última fase del proyecto es la de prueba y reparación del sistema, en la cual se evalúa la versión final y estable de la aplicación. Con esto se busca que los requisitos planteados desde el principio se cumplan correctamente y, de ser necesario, eliminar o controlar errores que se encontraron a la hora de probar el producto de software (Balaguera, 2015).

La ventaja que posee esta metodología frente a las demás, es su implementación fácil y flexible, añadiendo que fue creada para grupos de trabajo pequeños y para no extenderse más allá de lo que pide un desarrollo móvil. Para este caso, se enfoca en el desarrollo de un módulo que se implementa en la aplicación Conecta2.

2.2.6. Redes ad hoc

Las redes ad hoc son un tipo de redes que no necesitan infraestructura, como torres de comunicación, para poder comunicar a los dispositivos conectados. En una red ad hoc, todos los nodos tienen la misma jerarquía, por lo tanto, cualquiera de los nodos participantes puede ejercer la función de emisor de información, enrutador o receptor de información.

Las redes ad hoc son bastante dinámicas, pues pueden crearse espontáneamente en el momento que se requieran, y son muy económicas, dado que no requieren la instalación de torres o grandes antenas. Sin embargo, tienen limitaciones cuando están conformadas por teléfonos inteligentes, dado que la activación del modo ad hoc en estos dispositivos no es trivial, pues se requiere ingresar como usuario *root*, lo cual no es viable para un usuario regular. Por esa razón, cuando se desea generar redes de teléfonos móviles de alcance local, las tecnologías de comunicación más adecuadas son Bluetooth y Wi-Fi Direct (Basagni et al., 2013).

2.2.7. Registro

El registro es un proceso que implica proporcionar un nombre usuario o correo, junto con una contraseña que servirá para agregarse a una lista dentro de un servicio. Luego, el usuario deberá aportar algunos datos personales si el servicio al que quiere entrar lo requiere; esta información se guardará en una base de datos que, dependiendo de los términos y condiciones que el usuario aceptó, tendrá confidencialidad o algunos datos serán recolectados para estudios de algún tipo (CommonSpaces, 2015).

2.2.8. Autenticación

Se refiere al proceso mediante el cual es posible demostrar que un usuario dentro de una página web o servicio es realmente quien dice o asegura ser (IBM, s.f).

Existen 3 diferentes tipos de autenticación, estos son:

- Autenticación utilizando algo conocido por el usuario (contraseña): es el más usado, consiste en utilizar un recurso secreto que solo sabrá la persona que lo haya creado. No es de alta seguridad, pero proporciona cierto grado de protección y es de bajo costo (RedIRIS, 2008).
- Autenticación mediante algo que posee el usuario (tarjetas inteligentes): en este caso, la autenticación se realiza con un dispositivo de seguridad que puede almacenar información de manera segura. Esta técnica es más resistente a la adulteración, ya que el dispositivo posee un chip en el cual la información está cifrada en ficheros y acompañada de funciones criptográficas. Cuando el usuario usa una tarjeta inteligente, deberá saber la clave para poder autenticarse y tener acceso a la información, esto hace que un tercero no pueda usar una tarjeta que no le pertenezca (RedIRIS, 2008).
- Autenticación por una característica física que posee el usuario (biométrica): se basa en usar un aspecto físico del usuario para poder acceder a la información guardada o generada en un servicio. Existen múltiples opciones, entre otras, verificación por voz, por escritura, mediante huellas dactilares, o a partir del reconocimiento de iris (RedIRIS, 2008).

2.2.9. SMS (Servicios de Mensajes Cortos)

Son mensajes de texto a celular disponibles desde los celulares más sencillos a los más actuales. Fue una de las primeras aplicaciones para móviles, creada mucho antes que las aplicaciones actuales que permiten comunicar por medio de mensajes en internet. Estos mensajes pueden tener entre 70 a 160 caracteres (Auronix, 2020).

Ahora bien, el añadir la autenticación mediante SMS es una manera de fortalecer la seguridad al registro de nuevos usuarios a una plataforma web o de servicio, donde puede ser solamente de registro inicial o para acceso continuo. Funciona enviando

un código PIN a través de mensaje de texto, en un lapso de tiempo muy corto, mediante un API que detecte la creación de un nuevo usuario y luego envíe el mensaje de texto al número de celular que proporcionó en el registro (MDIRECTOR, 2018).

2.2.10. Seguridad Informática

La seguridad informática es el proceso de proteger la información contenida en un sistema informático, desde las perspectivas de integridad, confidencialidad y disponibilidad de la información, con el fin de prevenir y localizar el uso inapropiado y no autorizado de la información (VIU, 2018).

2.2.11. Seguridad en aplicaciones móviles

Teniendo en cuenta la definición de seguridad informática, la seguridad en aplicaciones móviles tiene varias aristas. Por una parte, tiene como propósito mantener las propiedades de la información (integridad, confidencialidad y disponibilidad) de acuerdo con los privilegios del usuario registrado. Por otra parte, es el conocimiento por parte del usuario de las posibles implicaciones de dar permisos de acceso a una aplicación descargada, teniendo en cuenta las posibles ventajas y desventajas al proporcionar vía libre al acceso de datos que necesitará en algunos casos para su funcionamiento (Generalitat Valenciana, 2011).

2.2.12. Zxing

Es una librería que permite procesar diferentes tipos de imágenes multiformato en una dimensión, dos dimensiones y código abierto. También permite generar códigos QR personalizados y guardar la información que se quiera hasta lo que se permita en el formato (Zomwi, 2012).

2.2.13. Toast

Se trata de un mensaje que se muestra en la pantalla durante un tiempo para que el usuario lo vea, después de terminar el tiempo, desaparecerá, se pueden personalizar, sin embargo, ya existe un formato estándar al mostrarse en un rectángulo de un color gris translucido. Son usados principalmente para mostrar mensajes cortos de notificación si se quiere que el usuario lo lea luego de realizar alguna acción dentro de la aplicación (Sgoliver, 2011).

2.2.14. Bots

Es una aplicación de software programada para realizar diversas tareas, dependiendo de lo que se requiera hacer, son automatizados, lo que significa que se llegan a ejecutar con ciertas instrucciones sin que el usuario humano deba iniciarlos de manera manual. Normalmente se usan para imitar el comportamiento de un humano y realizan tareas de manera repetitiva (Cloudflare, s.f). Los bots pueden ser de diversos tipos como:

- Chatbots, que simulan la conversación humana cuando se les inicia con una frase.
- Rastreadores web (GoogleBot), escanean contenido en páginas web de todo internet.
- Bots sociales, operan en plataformas de redes sociales.
- Bots maliciosos, realizan raspado de contenido, difunden spam o llevan a cabo ataques de relleno de credenciales.

2.2.15. Suplantación de identidad

Consiste en un tercero que se hace pasar por otra persona para tratar de obtener información que está restringida o para desviar la atención de las autoridades hacia

otra persona cuando se comete un ilícito. Esto trae muchos inconvenientes en cualquier ámbito que incluya el procesamiento de datos personales, pues puede perjudicar de manera significativa la integridad de una persona (Grupo Ático34, 2019). Existen varios métodos de suplantación de identidad, entre estos están:

- Sustracción o pérdida del documento de identidad: es la pérdida o robo del documento de identificación de una persona, que puede llegar a ser usada para que una persona mal intencionada se haga pasar por aquel que perdió el documento (Ayudaley, s.f).
- Falsificación de firma: se presenta cuando una persona firma un documento con una firma que le corresponde a otra persona (Ayudaley, s.f).
- Perfiles falsos en internet y redes sociales: corresponde al registro falso en un servicio, donde el principal objetivo puede ser engañar a terceros o hacerse pasar por alguien ya activo en la red (Ayudaley, s.f).
- Phishing: se trata de enviar correos electrónicos que aparentan provenir de fuentes verídicas, en los que se incluyen enlaces web que direccionan a una página web falsa. La página falsa puede llegar a tener la misma interfaz gráfica real para engañar al usuario, y al momento de iniciar sesión, se extraen los datos digitados para así robar su identidad con los datos proporcionados sin intención por la víctima (Ayudaley, s.f).

Con el nuevo módulo de Conecta2 se reduce la probabilidad de suplantación, pues al momento del registro se verifica que no existan 2 usuarios con el mismo número de documento.

2.2.16. Código de barras 2D en PDF417

El código PDF417 consiste en 4 barras y 4 espacios, donde cada patrón en medio de estas barras tiene 17 unidades de longitud, esto permite codificar hasta 1800 caracteres ASCII o 1100 caracteres binarios, por lo cual permite almacenar una

buena cantidad de información (Cognex, s.f). La Figura 1-1 muestra un ejemplo del código de barras 2D con formato PDF417 presente en la cédula de ciudadanía. El nuevo módulo de Conecta2 le permite al usuario, con la ayuda de la cámara de su celular, realizar el escaneo de este código de barras y, a partir de la información capturada, se verifica si ese documento de identidad ya se había registrado. Si se confirma que el documento no había sido registrado previamente en la base de datos, creará un nuevo usuario con la información capturada del documento.

Figura 1-1. Ejemplo del código PDF417 presente en un documento de identidad

Fuente: registraduría nacional del estado civil

La Figura 1-1 muestra la estructura visual trasera de una cédula de ciudadanía colombiana junto con el código de barras en formato PDF417.

La información que contienen los documentos de identificación utilizados en Colombia es la siguiente:

a) Cédula de ciudadanía:

- Cara frontal: presenta el número único de identificación, apellidos, nombres, espacio para firma del ciudadano y foto a color del ciudadano (Registraduría Nacional del Estado Civil, s.f).

- Cara posterior: validación de huella dactilar, código de barras en PDF417, datos de nacimiento y expedición, estatura, grupo sanguíneo y sexo (Registraduría Nacional del Estado Civil, s.f).

b) Tarjeta de identidad:

- Cara frontal: presenta el número único de identificación, apellidos, nombres, espacio para firma del menor de edad, foto a color del menor de edad, impresión TOV (tinta ópticamente variable) y fondo de seguridad con líneas finas, anti fotográfico (Registraduría Nacional del Estado Civil, s.f).
- Cara posterior: validación de huella dactilar del menor, código de barras en PDF417, datos de nacimiento y expedición, fecha de vencimiento del documento, grupo sanguíneo y sexo (Registraduría Nacional del Estado Civil, s.f).

c) Cédula de extranjería:

- Cara frontal: presenta los apellidos, nombres, nacionalidad, fecha de nacimiento, sexo, fecha de expedición, grupo sanguíneo, fecha de vencimiento del documento (si es temporal), firma del extranjero y foto del extranjero (Ministerio de Relaciones Extreriores, s.f).
- Cara posterior: código de barras PDF417, espacio para imprimir una lectura mecánica de tres líneas de 30 caracteres y nombre y firma del Director de Migración de Colombia (Ministerio de Relaciones Extreriores, s.f).

2.3. ANTECEDENTES O ESTADO DEL ARTE

Para la realización de este nuevo módulo es necesario saber qué herramientas eran semejantes o cuáles podían tener la funcionalidad de lector de código de barras en 2D.

Entre las aplicaciones móviles que están disponibles de forma gratuita y que realizan la función de escanear el código de barras presente en los documentos de identidad, se identificaron tres:

- Aplicación *"Verifíquese Cédula"* nos permite por medio de la cámara del celular, escanear el código de barras y mostrar los datos que se encuentran codificados presentes en el propio documento. El mayor inconveniente con esta aplicación, es que, para la realización de varias consultas, el usuario deberá pagar la versión premium (Verifíquese Cédula, s.f).
- Aplicación *"PDF417 barcode scanner"*: funciona de manera similar a la aplicación anterior, sin embargo, la mayoría de los datos se presentan cifrados y solo mostrará el nombre de la persona a quien pertenece el documento de identidad.
- Aplicación *"PDF417 Barcode Scanner – Qr Generator & reader 2 in 1"*, al igual que la aplicación anterior, presenta la mayoría de los datos cifrados y solo mostrará en texto descifrado el nombre de la persona a quien pertenece del documento.

Muchas de las aplicaciones presentes en línea que se dedican a leer tanto códigos de barras 1D como 2D, que almacenan diferente cantidad de información, tienen una gran limitante, donde lo único que se puede leer del documento será el nombre y lo demás estará cifrado. En la Tabla 1-1 se pueden ver las ventajas y desventajas de las aplicaciones encontradas.

Tabla 1-1. Ventajas y desventajas de aplicaciones de lectura de códigos de barras.

Aplicación	Ventajas	Desventajas
Verifíquese Cédula	• Decodificación de la información presente en el código de barras. • Búsqueda en bases de datos, información extra que esté en alguna institución pública. • Captura la información y permite compartirla.	• La multiconsulta de información tiene un costo. • No captura los datos para generar un registro en una base de datos.
PDF417 barcode scanner	• Multi-lectura de códigos de barras. • Captura la poca información y permite compartirla.	• Solamente muestra el nombre de la persona. El resto de la información mostrada luego de la lectura, está cifrada.
PDF417 Barcode Scanner – Qr Generator & reader 2in 1	• Generador de QR y multi lector de códigos de barras. • Captura la poca información y permite compartirla.	• Solamente muestra el nombre de la persona. El resto de la información mostrada luego de la lectura, está cifrada.

Fuente: elaboración propia.

De acuerdo al objetivo de presentar un módulo de registro y autenticación de usuario capturando y comparando la información contenida en el código de barras de los documentos de identidad, las aplicaciones comparadas anteriormente poseen algunas características necesarias, sin embargo, ninguna crea un registro de usuario mediante los datos recolectados al hacer el escaneo. Por lo tanto, este nuevo desarrollo implementa esta función mediante la lectura del documento de identidad que el usuario posea y finalmente, se integra con la aplicación Conecta2.

2.4. MARCO LEGAL

Para el desarrollo de este módulo, se tuvieron en cuenta las siguientes leyes regidas en la sociedad colombiana:

Ley de derechos de autor, ley 23 de 1982 junto con la decisión andina 351 de 1993. Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta ley a los

intérpretes o ejecutantes, a los productores de fonogramas y a los organismos de radiodifusión, en sus derechos conexos a los del autor.(Dirección nacional de derecho de autor, 1982)

Las disposiciones de la presente Decisión tienen por finalidad reconocer una adecuada y efectiva protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino. Asimismo, se protegen los Derechos Conexos a que hace referencia el Capítulo X de la presente Decisión.(Alcaldía mayor de Bogotá, 1982).

Ley de habeas data bajo la ley estatutaria 1581 de 2012. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.(Función Pública, 2012).

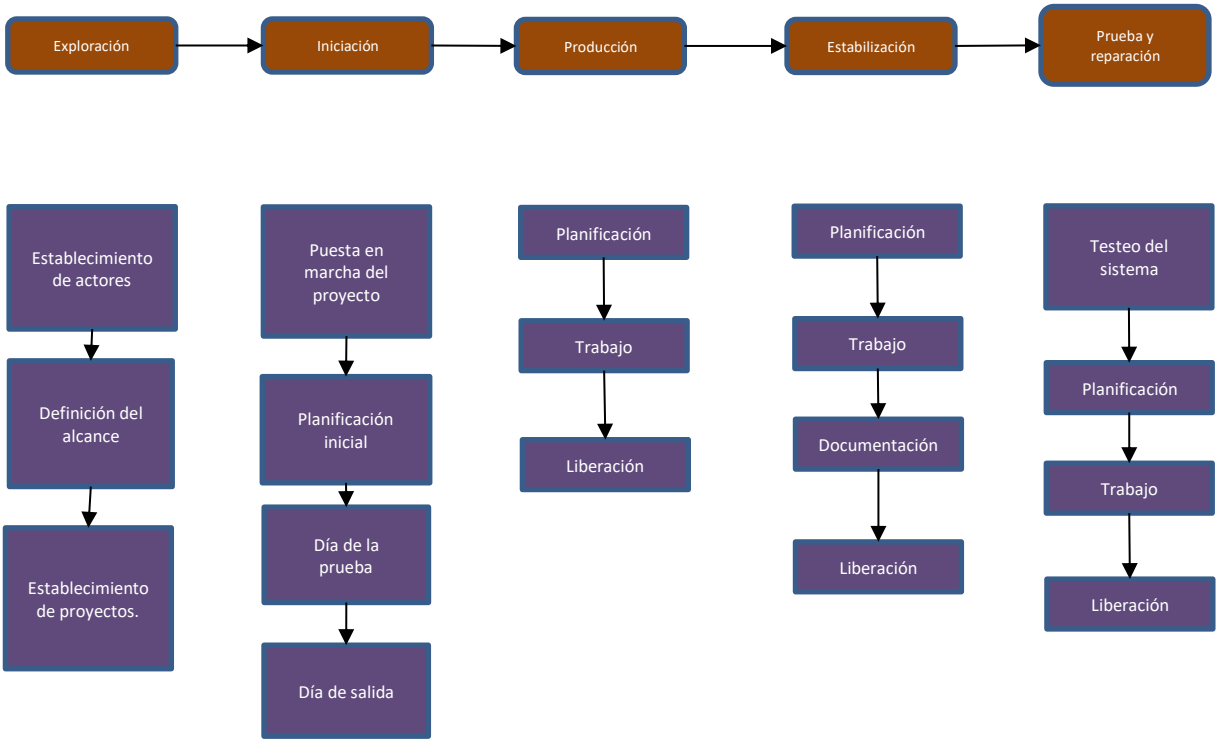
El desarrollo de este módulo también se mantendrá bajo las normativas solicitadas por el líder de investigación de la aplicación Conecta2.

3. ASPECTOS METODOLÓGICOS

En este capítulo se describe la aplicación de la metodología Mobile-D para el desarrollo del módulo de autenticación para la aplicación Conecta2

En la Figura 3-1, se presenta un diagrama que representa cómo se usó la metodología dentro del proyecto de desarrollo, planteando las etapas que tiene cada fase principal:

Figura 3-1. Ciclo de la metodología Mobile – D (Balaguera, 2015)**.**



Fuente: tomado de Amaya Balaguera, 2015

3.1. EXPLORACIÓN

Se tuvieron 2 reuniones para esta fase: en la primera se exploró con la líder del proyecto Conecta2 la propuesta en términos técnicos, herramientas que se usarían y los posibles prototipos para la interfaz que se necesitarían para la vista de registro de los usuarios. En el segundo encuentro, se entregó a la líder, de manera más depurada, una vista de los requerimientos estructurados y organizados en donde se realizaron las últimas correcciones y cambios para el proyecto. De esta manera, se abarcaron las 3 etapas correspondientes a esta fase.

Para cada etapa, la directora de proyecto estuvo presente, pues ella fue quien decidió que los requerimientos propuestos por el desarrollador fueran aceptados o no. Cuando no estuvo de acuerdo, se hicieron los cambios necesarios para poder llegar a un nivel de aceptación.

En cuanto a diagramas, se realizaron diagramas de casos de uso y de secuencia, esto para tener una estructura base y no tener problemas cuando se comenzara con la generación de código, evitando cambios luego de dejar claro los diseños que se utilizarían.

En esta fase se contemplaron y realizaron las siguientes tareas:

- Se realizó el primer encuentro con la directora de proyecto, se levantaron los requerimientos y planteó el alcance y limitaciones.
- Se acoplaron las sugerencias por parte del desarrollador y de la directora de proyecto.
- Se mostraron los posibles prototipos visuales para implementar en el módulo.
- Se realizó el segundo encuentro con la directora de proyecto.
- Se entregó la documentación, diseños y explicación de los casos de uso para las soluciones en el desarrollo del nuevo módulo.
- Se exploraron las herramientas tecnológicas que se usarían en el desarrollo.

Esta fase tuvo como resultado los siguientes productos:

- Formato extendido de casos de uso.
- Diagramas pertinentes que se tuvieron como base para el desarrollo.
- Prototipos visuales que se adaptaron e implementaron al final del desarrollo.

3.2. INICIACIÓN

Luego de que se dejó claro con la líder de proyecto todos los requerimientos y posibles vistas de interfaz, se procedió a agregarlos como elementos base para tenerlos en cuenta durante todo el proceso de diseño. Adicionalmente, se instaló el ambiente de trabajo y aquellos programas que se usaron para desarrollar tanto los diagramas como el nuevo módulo. Finalmente, se identificaron aquellas cosas que se necesitarían primero y cuáles se podían dejar para la última parte del desarrollo.

En esta fase se contemplaron las siguientes tareas:

- Se planearon las actividades a realizar en el desarrollo.
- Se verificó cuántas funcionalidades se tendrían al final de la fase de producción.
- Se implementaron las herramientas tecnológicas que se usaron en el desarrollo.

Esta fase tuvo como resultado los siguientes productos:

- Ambiente de programación instalado (en este caso, Android Studio).
- Herramientas instaladas con las que se realizó la parte visual del programa.

3.3. PRODUCCIÓN

Para el desarrollo de este módulo, se tuvieron en cuenta los diseños que se realizaron y que la líder de proyecto aceptó. Todo este proceso se realizó evitando cambios en esos diseños originales, siempre que fuera posible.

En esta fase se contemplaron las siguientes tareas:

- Se inició y realizó la codificación del módulo de registro.
- Se realizaron las interfaces acoplando la codificación realizada.
- Se verificó la funcionalidad de cada parte del desarrollo.
- Se realizó la conexión a la base de datos local y el almacenamiento de datos.
- Se realizó la conexión a la base de datos en la nube comprobando que los datos se guardaran correctamente.

Esta fase tuvo como resultado los siguientes productos:

- Código fuente del módulo.
- Verificación de la consistencia de los diagramas con el código realizado.

3.4. ESTABILIZACIÓN

Luego de observar y evidenciar que el módulo funciona, se procedió a integrarlo a la aplicación Conecta2, verificando que no hubiera problemas al realizar una acción dentro del módulo y que repercutiera negativamente en la aplicación.

Se hicieron diferentes pruebas, por ejemplo, para que los datos del documento de identificación del usuario se guardaran correctamente en el formulario de registro, así como también la verificación de 2 pasos con la herramienta Firebase. Se le entregaron a la directora de proyecto los documentos pertinentes del uso del módulo.

En esta fase se contemplaron las siguientes tareas:

- Se integraron todas las funcionalidades de registro a la aplicación Conecta2.
- Se agregó el perfil de usuario en los demás módulos disponibles en Conecta2.
- Se realizó la documentación para los futuros desarrolladores y directora de proyecto, para poder entender cómo funciona el código fuente generado.
- Se estabilizaron las funcionalidades creadas en la fase de producción.

Esta fase tuvo como resultado los siguientes productos:

- Documentación de funcionalidades e integración las mismas en el código fuente.
- Código fuente compilado con las funcionalidades propuestas desde la primera fase.

3.5. PRUEBA Y REPARACIÓN

Al haber verificado de manera interna que las funcionalidades fueran correctas, se implementó la versión en la que se pudieron eliminar los errores críticos que no dejaban ejecutar la aplicación Conecta2. Finalmente, la directora de proyecto dio la aceptación del nuevo módulo y se demostró que funcionan de manera correcta a como se planeó desde un principio.

En esta fase se contemplaron las siguientes tareas:

- Se probó y verificó que las funcionalidades no ocasionaran errores en Conecta2 y en los módulos disponibles.
- Se corrigieron los errores al integrar las funcionalidades.
- Se realizaron los manuales, la documentación para la directora de proyecto y desarrolladores que deseen agregar funcionalidades o integrar un nuevo módulo con el de registro.
- Se preparó y entregó el módulo de autenticación a la directora de proyecto.

Esta fase tuvo como resultado los siguientes productos:

- Entrega de producto final a la directora de proyecto.
- Entrega de manual técnico y de manual de usuario.

4. DESARROLLO DEL PROYECTO

Para el desarrollo de este módulo se utilizó la metodología Mobile-D, llevando a cabo cada una de las fases anteriormente explicadas. En este capítulo se explica cómo se aplicó la metodología para obtener la versión de la aplicación Conecta2 con el nuevo módulo de registro.

4.1. DESCRIPCIÓN DEL MÓDULO

El registro que se desarrolló en la primera versión de la aplicación Conecta2 permitía al usuario cambiar su nombre y el nombre del dispositivo, las veces que lo deseara. Como los datos ingresados por el usuario no se validaban, el usuario podía elegir una identidad diferente a la suya.

Con el nuevo módulo, el registro de usuarios dentro de la aplicación se hace más robusto, dado que la información personal que el usuario digita para su registro, se compara contra los datos almacenados en el código de barras de la parte trasera de su documento de identificación. Lo anterior trae como consecuencia que la identidad del usuario en la aplicación coincida con la información de su documento de identidad. Si los datos digitados por el usuario y los escaneados coinciden, el registro pasa a una etapa en la que se verifica el número de teléfono del usuario mediante un mensaje SMS. Si esta verificación es exitosa, en seguida el usuario procede a tomarse una foto y presiona un botón para completar el registro, para lo cual la aplicación valida en la nube que ese documento de identificación no hubiera sido registrado previamente y guarda una copia local de la información.

Si el documento se está registrando por primera vez, la aplicación se redireccionará a la pantalla principal de Conecta2, de lo contrario se le avisará al usuario que ya existe un registro con ese mismo número de documento y no podrá avanzar. El proceso de registro se realiza una sola vez y requiere que el celular esté conectado

a internet. Después de que el proceso de registro es exitoso, siempre que el usuario abra la aplicación Conecta2 será direccionado a la pantalla principal de la misma y su identidad ya estará almacenada localmente en el dispositivo.

4.2. FASE DE EXPLORACIÓN

Dentro de esta fase se realizaron 2 reuniones con la directora, en las cuales se acordó cómo se desarrollarían las siguientes etapas.

4.2.1. Establecimiento de actores

Se establecieron los siguientes actores para tener claridad de quien recibirá el producto y quienes hacen parte del equipo que realizará del módulo.

- **Cliente:** Maria del Pilar Salamanca Azula.
- **Equipo de desarrollo:** Andrés Felipe Barragán Jaimes.
- **Tester:** Andrés Felipe Barragán Jaimes – María del Pilar Salamanca Azula.

4.2.2. Definición de alcance

Se revisó el alcance que tendría el módulo en cuanto a funcionalidades, y en la primera reunión se establecieron las cosas que se tendrán en cuenta y los preparativos base para el desarrollo. Para la segunda reunión se obtuvieron distintos entregables, empezando con los casos de uso extendidos, para los cuales se planteó el uso de la plantilla mostrada en la Tabla 4-1. Esta plantilla posee varios aspectos que permiten describir de una manera más completa los casos de uso. Se detacan los diferentes tipos de caminos, además del curso básico junto con un resumen, las entradas y salidas que se generarán para explicar que tendrá cada función.

Tabla 4-1. Plantilla caso de uso extendido.

Identificador		
Nombre de caso de uso		
Actor(es)		
Indispensable / deseable		
Prioridad		
Visible / no visible		
Autor		
Fecha de elaboración		
Revisión		
Última fecha de revisión		
Resumen		
Entradas		
Salidas		
Curso básico de uso	Usuario	Sistema
Caminos alternativos	Usuario	Sistema
Caminos de excepción	Usuario	Sistema

Fuente: elaboración propia

Junto con la directora se elaboró la Tabla 4-2 que contiene los casos de uso que se tendrían en cuenta para el desarrollo, con su correspondiente identificador.

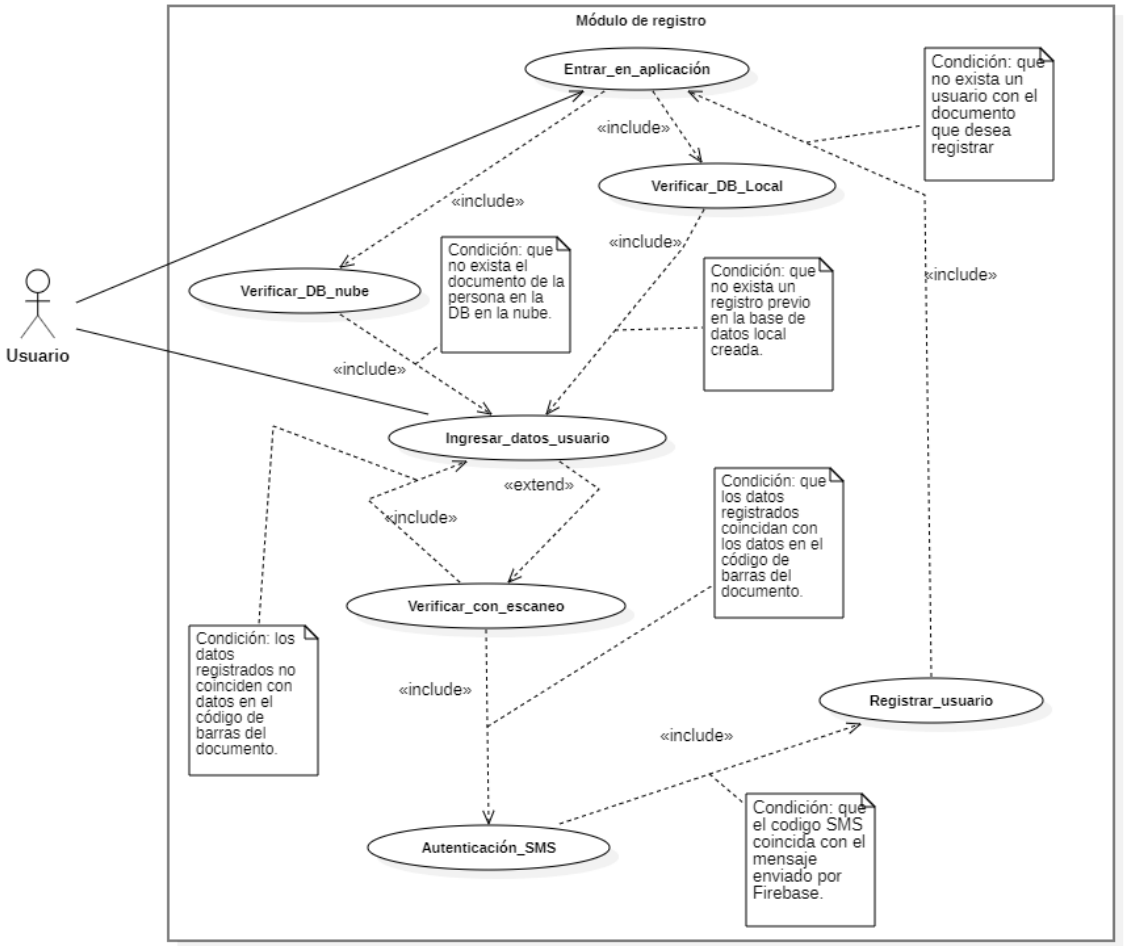
Tabla 4-2. Casos de uso identificados.

Caso de uso	Identificador
VARIFICAR BASE DE DATOS LOCAL	Md_Rg_001
VERIFICA REGISTRO DE DOCUMENTO EN LA NUBE	Md_Rg_002
INGRESAR LOS DATOS DEL USUARIO	Md_Rg_003
VERIFICAR CON ESCANEO	Md_Rg_004
AUTENTICACIÓN SMS	Md_Rg_005
REGISTRAR USUARIO	Md_Rg_006

Fuente: elaboración propia.

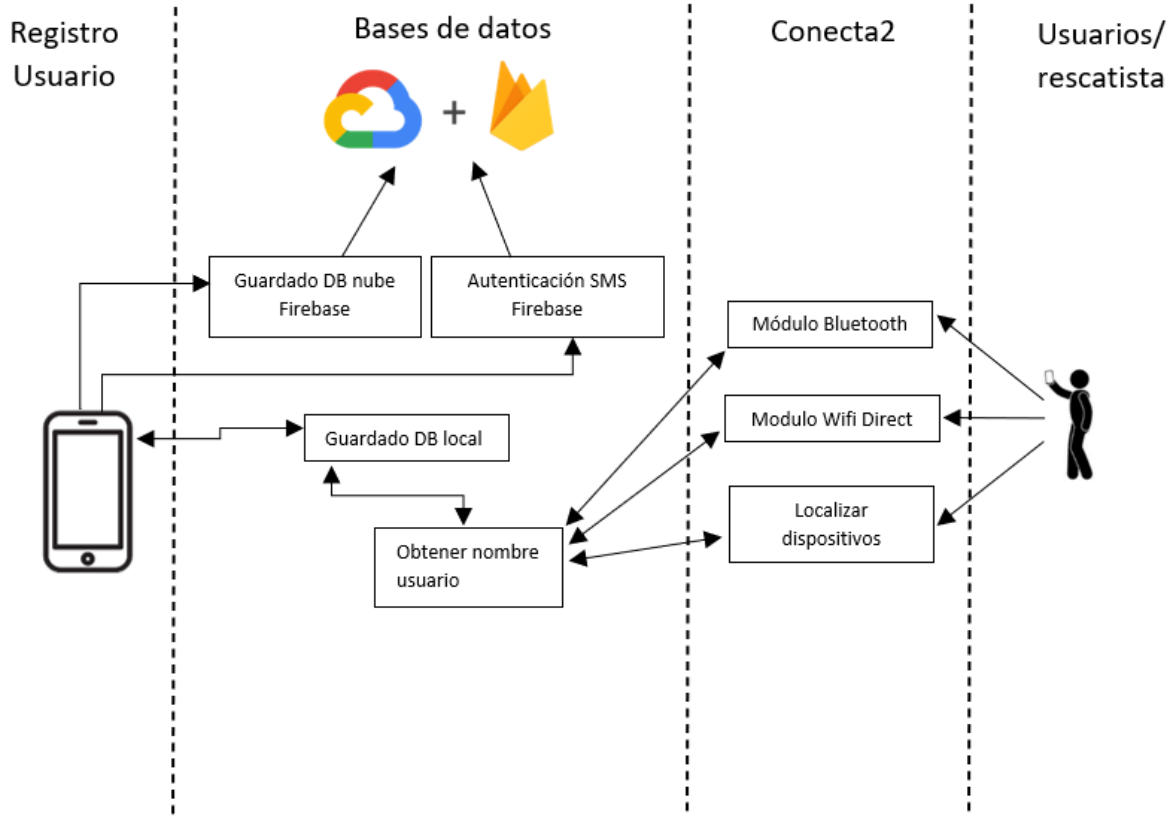
A continuación en la Figura 4-1, se presenta el diagrama que se generó a partir de los requerimientos de los casos de uso, estos se tomaron como base para el desarrollo y se realizaron los cambios necesarios para que se acomodaran al desarrollo final. Es importante destacar que en este desarrollo, el único actor es el usuario final.

Figura 4-1. Diagrama caso de uso módulo de registro



Fuente: elaboración propia

Figura 4-1.1. Estructura del registro en Conecta2

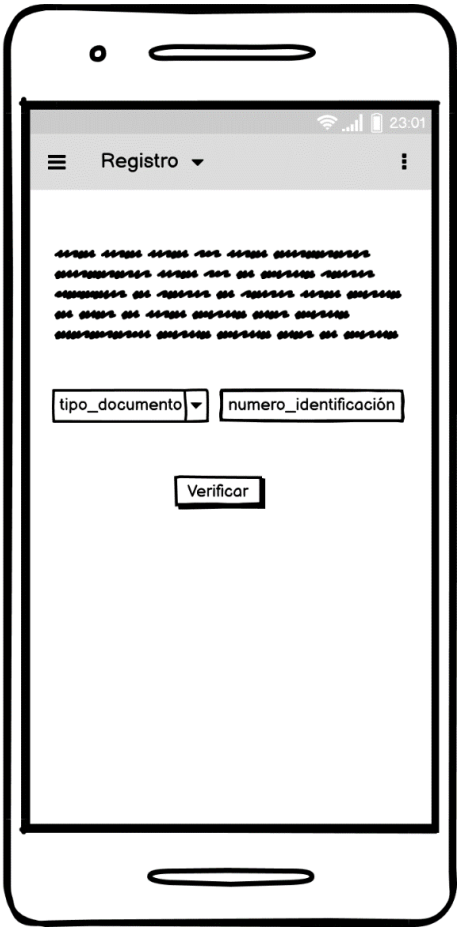


Fuente: elaboración propia

En la Figura 4-1.1 se puede observar de una manera sencilla cómo al realizar el registro, la información se guarda tanto localmente como en la nube. Luego, la aplicación usa el nombre que se guarda en la base de datos local y los usuarios que la usan, pueden observarlo en los módulos disponibles al conectarse en la red.

Para el diseño de las actividades con las funcionalidades requeridas, se elaboraron mockups con la herramienta Balsamiq Wireframes, con las que se crearon prototipos que ayudarían al diseño final:

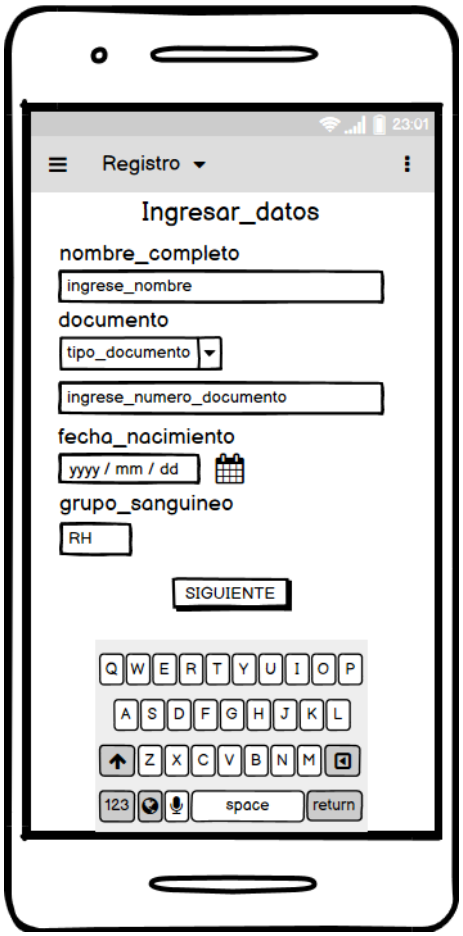
Figura 4-2. Mockup de la pantalla verificar documento.



Fuente: elaboración propia.

La Figura 4-2 muestra un prototipo visual para la pantalla de verificar documento, donde el usuario ingresaría el tipo de documento junto con el número para verificar en la base de datos en la nube si ya existe un registro con el documento digitado.

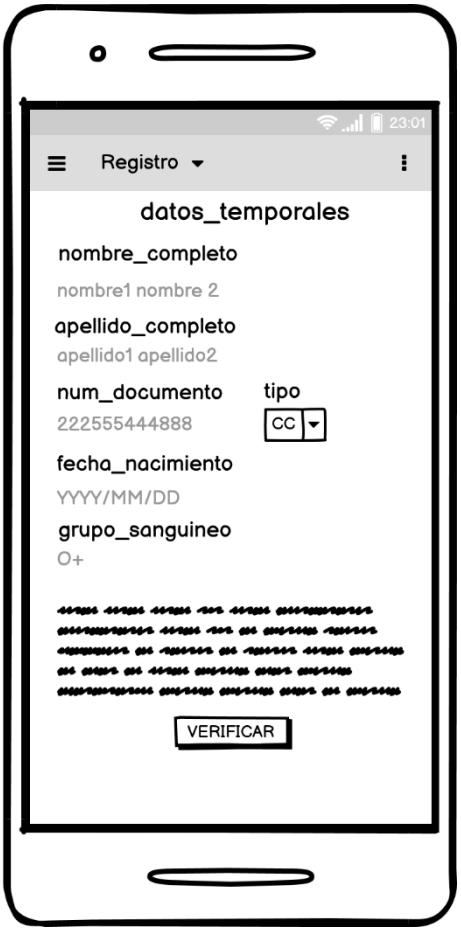
Figura 4-3. Mockup de la pantalla ingresar datos.



Fuente: elaboración propia.

La Figura 4-3 muestra un prototipo visual de la pantalla para ingresar datos, en donde el usuario deberá poner sus datos para poder registrarse y luego continuar si la información es correcta.

Figura 4-4. Mockup de la pantalla datos para verificar.



Fuente: elaboración propia.

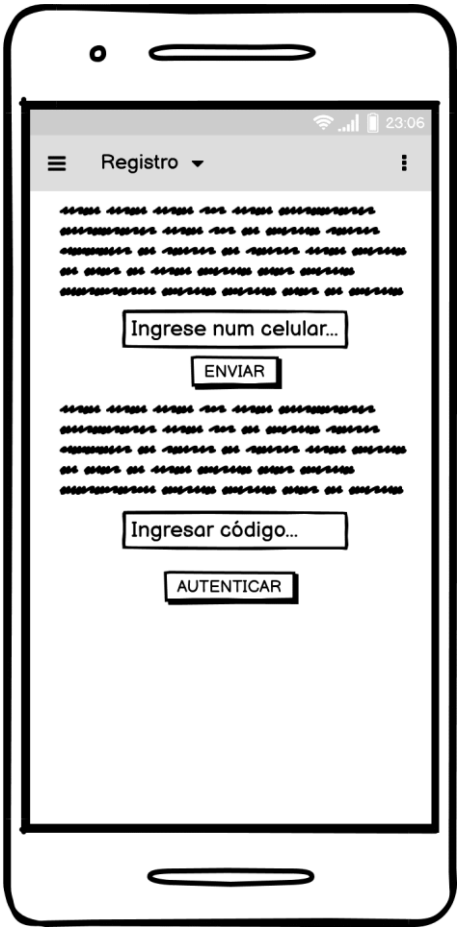
La Figura 4-4 muestra el prototipo de la pantalla datos para verificar, aquí el usuario puede tener una previsualización de los datos escritos en la pantalla de ingresar datos, para que verifique que todo esté correcto y proceda a escanear su documento.

Figura 4-5. Mockup de la pantalla escaneo documento

Fuente: elaboración propia.

La Figura 4-5 muestra cómo se ve en la pantalla la librería de escaneo de Zxing y cómo el usuario debe poner el documento antes de escanearlo.

Figura 4-6. Mockup de la pantalla Autenticar SMS



Fuente: elaboración propia.

La Figura 4-6 muestra la pantalla prototipo de autenticación SMS, donde el usuario deberá digitar su número de celular, enviar una solicitud de un código a Firebase y por último autenticar el código recibido escribiéndolo en “ingresar código”.

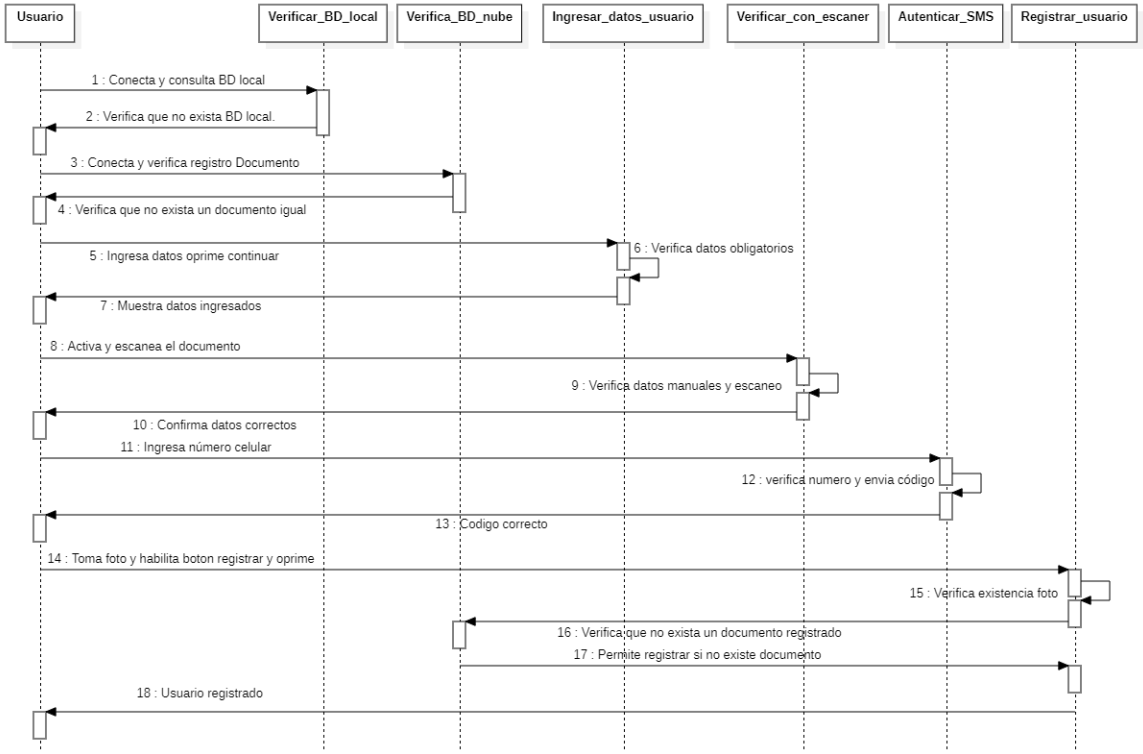
Figura 4-7. Mockup de la pantalla foto y registro.

Fuente: elaboración propia.

Por ultimo, la Figura 4-7 muestra la pantalla de foto y registro, en donde el usuario deberá tomarse una foto para continuar el proceso, no sin antes comprobar que no exista un documento del mismo tipo con el mismo número registrado en la base de datos de la nube.

A continuación en la Figura 4-8, se presenta el diagrama de secuencia, el cual ayuda a comprender el flujo que llevan las actividades del módulo para luego incluirlo en Conecta2.

Figura 4-8. Diagrama de secuencia módulo de registro.



Fuente: elaboración propia.

4.2.3. Establecimiento de proyectos

Con los recursos del punto anterior, se procedió a realizar las tareas para preparar y elaborar los distintos entregables que se tendrían para las siguientes fases.

4.3. FASE DE INICIACIÓN

Dentro de esta fase, se mantendría el cronograma de actividades presentado en el anteproyecto en el cual se daba un estimado para la realización del módulo de registro, esto con el objetivo de tener un flujo de trabajo constante y en la medida de lo posible no sobrepasar el tiempo esperado para la terminación de las siguientes fases. A continuación se explica lo que se hizo de manera específica en cada etapa.

4.3.1. Puesta en marcha del proyecto

Luego de obtener varios recursos base tales como los diagramas, prototipos visuales para el módulo y la identificación de los casos de uso, se prosiguió a poner en marcha el proyecto.

4.3.2. Planificación inicial

En el inicio del proyecto, la agenda que se utilizó fue la misma que se propuso en el anteproyecto. Sin embargo, posteriormente se fue ajustando debido a que algunas actividades se realizaron más rápidamente de lo previsto y otras, en cambio, se extendieron más de lo estimado. Por ejemplo, la codificación requirió tres semanas más, en tanto que la fase de exploración se hizo en la mitad del tiempo previsto inicialmente. En la Tabla 4-3 se muestra el cronograma final del desarrollo del trabajo de grado.

Tabla 4-3. Cronograma de actividades

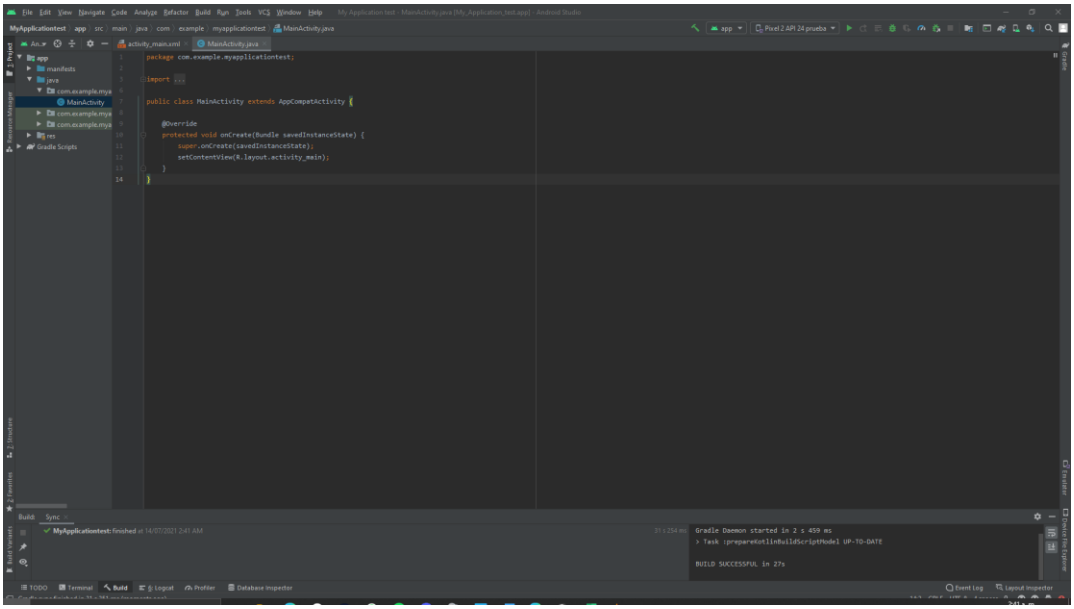
Fase	Tarea	Semanas														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Exploración	Se realizó el primer encuentro con la directora de proyecto, se plantearon los casos de uso, alcance y limitaciones.															
	Se acoplaron las sugerencias por parte del desarrollador y de la directora de proyecto.															
	Se crearon los prototipos visuales que se pueden implementar para el módulo.															
	Se realizó el segundo encuentro con la directora de proyecto y se realizaron los cambios pertinentes.															
	Se entrego documentación, diseños y explicación los casos de uso para las soluciones en el desarrollo del nuevo módulo.															
	Se exploraron e instalaron las herramientas para el desarrollo del módulo.															
Iniciación	Se agendo las actividades de las demás fases.															
	Se verificaron las funcionalidades se iban a generar al final de la fase de producción.															
	Implementación de herramientas tecnológicas finales a usar.															

Producción	Se adaptaron los diagramas generados para codificar.			■												
	Se inicio de la codificación.			■	■	■	■	■	■	■	■					
	Se realizaron las interfaces acoplando los prototipos propuestos.			■	■	■	■	■	■	■	■					
	Verificar de funcionalidad de cada parte del desarrollo.			■	■	■	■	■	■	■	■					
	Se realizó la conexión a la base de datos local y guardado de datos.										■					
	Se realizó la conexión a la base de datos en la nube comprobando que los datos se guarden correctamente.										■					
	Se realizó la conexión para la autenticación por SMS.										■					
Estabilización	Se realizaron pruebas de usuario para verificar las funcionalidades.											■				
	Integrar todas las funcionalidades en el mismo módulo.											■				
	Implementar el módulo de registro en la aplicación Conecta2.											■				
	Se realizó documentación para los futuros desarrolladores y directora de proyecto, para poder entender cómo funciona el módulo de registro.											■	■			
	Se estabilizaron las funcionalidades creadas en la fase de producción.												■			
Prueba y reparación	Se probo y verificó que las funcionalidades no repercutan con errores en Conecta2 y en los módulos disponibles.												■			
	Se corrigieron varios errores en la codificación que se presentaron en Conecta2 luego de implementar el nuevo módulo.												■	■		
	Se termino y se entregaron los manuales y documentación para la directora de proyecto y desarrolladores que deseen agregar funcionalidades o integrar un nuevo módulo con el de autenticación.													■		
	Se implemento la versión final y más estable en Conecta2.														■	
	Se entrego el producto dentro de Conecta2 junto con la documentación necesaria para entender el uso en la aplicación.															■

Fuente: elaboración propia

Como siguiente paso, se procede a instalar el ambiente de trabajo Android Studio y se crea una aplicación aparte que luego se integraría al código de Conecta2.

Figura 4-9. Ambiente de trabajo Android Studio



Fuente: elaboración propia

En la Figura 4-9 se púede ver un aplicación totalmente nueva, para realizar el desarrollo del módulo y posteriormente implementarlo en la aplicación Conecta2.

Por otra parte, tal como se hizo en la versión original de Conecta2, para el desarrollo del módulo de registro se usaron los recursos de creación visual que proporciona Android Studio, esto con el fin de no comprometer a futuro la posible compatibilidad de recursos visuales de la aplicación Conecta2 cuando se hiciera la integración con el módulo de registro.

4.3.3. Día de la prueba

Para esta fase, se hizo un recuento de todos los recursos disponibles, verificando que no haga falta nada y poder llegar al día de salida.

4.3.4. Día de salida

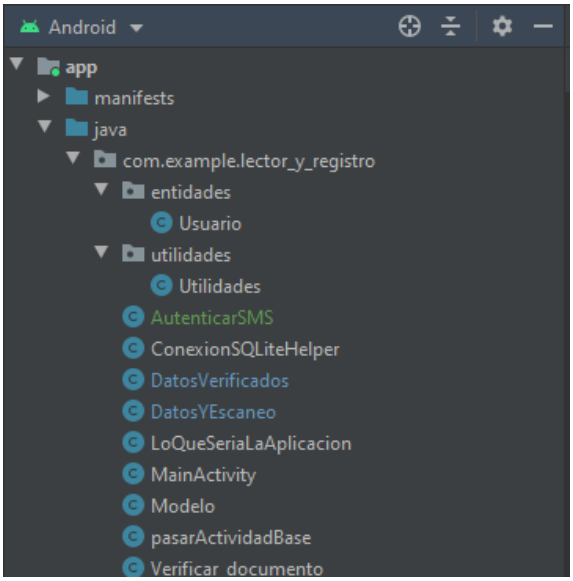
En este punto del proyecto, se confirmó que los recursos como diagramas, prototipos visuales y casos de uso fueran aceptados, para dar inicio formalmente a la fase de producción.

4.4. FASE DE PRODUCCIÓN

En esta fase se realiza la codificación, teniendo en cuenta las funcionalidades planeadas para este módulo. Como se menciona anteriormente en la metodología, las etapas se iteran hasta realizar por completo las tareas propuestas, por esta misma razón, se efectúan las etapas de planificación, trabajo y liberación para cada una de las funcionalidades por separado, hasta realizarlas por completo. Los recursos recolectados en las anteriores fases sirvieron para poder verificar la operación de cada funcionalidad y si realizaba las acciones pertinentes sin repercutir en las otras funcionalidades del módulo.

Dentro del ambiente de trabajo se estructuró el módulo con sus clases correspondientes a las funcionalidades propuestas desde la primera fase. También se elaboraron funcionalidades no visuales y que fueron importantes para relacionar las clases creadas, tales como la creación de la base de datos local y en la nube. La estructura del módulo se puede ver en la Figura 4-10.

Figura 4-10. Ambiente Android Studio y las clases correspondientes a funcionalidades



Fuente: Elaboración propia.

La Figura 4-10 muestra la estructura de las clases de la aplicación que se desarrolló por separado y que luego se implementó en el código fuente de la aplicación Conecta2.

Siguiendo el flujo de actividades del módulo de registro para la aplicación Conecta2, a continuación se explicará cada una de las funcionalidades implementadas.

4.4.1. Verificación de registro local y en la nube

Al iniciar la aplicación por primera vez, no debe existir en la base de datos local (SQLite) una base de datos llamada *database_usuario_Conecta2* ni un registro dentro de la tabla de usuario. Se desarrolló una actividad que se encarga de verificar la existencia de esta base de datos y, dado caso que no exista, crea una conexión para una nueva base de datos local.

Figura 4-11. Segmento de código encargado de buscar registros

```
62    public int buscarFilas(){
63
64        Modelo buscar = new Modelo();
65        SQLiteDatabase verificarFila = buscar.getConn( context: pasarActividadBase.this);
66        Cursor cursor = verificarFila.query(Utilidades.TABLA_USUARIO, columns: null,
67                selection: null, selectionArgs: null, groupBy: null, having: null, orderBy: null);
68        Log.d( tag: "mensajeGetRawC", msg: "count de getRow es: " + cursor.getCount());
69        verificarFila.close();
70        return cursor.getCount();
71    }
```

Fuente: elaboración propia.

El código de la Figura 4-11, se entra a un condicional de la Figura 4-12 para realizar una de las siguientes dos acciones; en el caso de que sea la primera vez que se ingresa a la aplicación, se crea una base de datos vacía y se redirecciona a una funcionalidad que le pide al usuario que ingrese su documento y verifica si existe un registro en la nube. Si no hay un registro previo de ese documento, inicia el proceso de registro de la persona.

Figura 4-12. Segmento de código de condicional encargado de pasar a la pantalla de verificar documento o a la pantalla principal de Conecta2.

```
23        if(buscarFilas() == 0){
24            Intent psarARegistro = new Intent( packageContext: pasarActividadBase.this, Verificar_documento.class);
25            startActivity(psarARegistro);
26            Log.d( tag: "consultar base de datos", msg: "no hay fila");
27        }
28        if(buscarFilas() == 1){
29            Intent psarAAplicacion = new Intent( packageContext: pasarActividadBase.this, LoQueSeriaLaAplicacion.class);
30            startActivity(psarAAplicacion);
31            Log.d( tag: "consultar base de datos", msg: "si hay fila");
32        }
```

Elaboración: elaboración propia

En el caso de que no encuentre ningún registro en la base de datos local, se pasará a la pantalla de verificar documento (Figura 4-13) para poder buscar si ya existe. La terminación de esta codificación permitió completar el caso de uso de la Tabla 4-4.

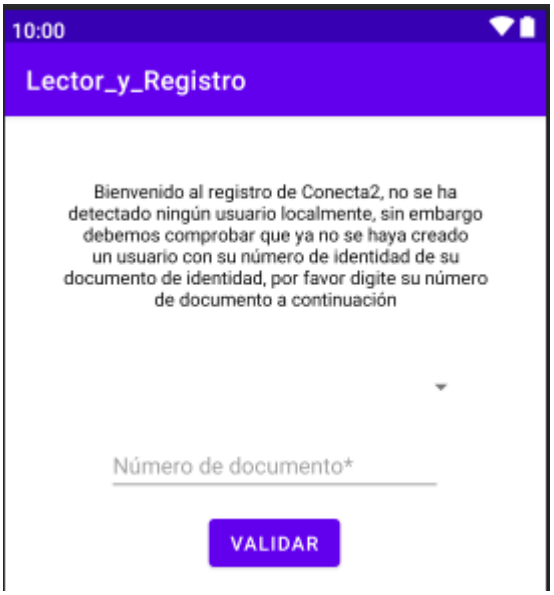
Tabla 4-4. Caso de uso para verificar la base de datos local

Identificador	Md_Rg_001	
Nombre de caso de uso	VERIFICAR BASE DE DATOS LOCAL	
Actor(es)	Sistema	
Indispensable / deseable	Indispensable	
Prioridad	Alta	
Visible / no visible	No Visible	
Autor	Andrés Felipe Barragán Jaimes	
Fecha de elaboración	01/02/2021	
Revisión	María del Pilar Salamanca Azula	
Última fecha de revisión	14/04/2021	
Resumen	El sistema verifica si existe un registro dentro de la base de datos del dispositivo.	
Entradas	Creación y conexión a la base de datos local.	
Salidas	Direccionamiento a pantalla de verificación de documento.	
Curso básico de uso	Usuario	Sistema
	1. Abre por primera vez la aplicación.	2. Verifica que no exista un registro en la base de datos local. 3. Redirecciona a la pantalla de verificar documento.
Caminos alternativos	Usuario	Sistema
	N/A	2.1. Encuentra un registro en la base de datos local 2.2 Redirecciona a la ventana principal de Conecta2.
Caminos de excepción	Usuario	Sistema
	N/A	N/A

Fuente: elaboración propia

La Tabla 4-4 presenta el flujo completo de la verificación de la base de datos local, mostrando lo que realiza el usuario y cómo responde el sistema.

Figura 4-13. Pantalla para verificar documento.



Fuente: Elaboración propia.

La Figura 4-13 es la pantalla de verificar documento a la cual llega el usuario al ingresar por primera vez a la aplicación luego de que el sistema comprueba que no hay ningún registro creado localmente con anterioridad. La persona debe seleccionar su tipo de documento e ingresar su número de documento para realizar la búsqueda del mismo en la nube.

Figura 4-14. Segmento de código que verifica si existe un registro en la nube.

```
public void validarNumFB() {

    String psarFrmtDcm = veriTipDcm.getSelectedItem().toString();
    String tipoDmcVerificar = tipoDocumenoPraVrf(psarFrmtDcm);
    String verifPersonKy = tipoDmcVerificar + numeroDocumentoPersona.getText().toString();
    Integer numeroDocuPerson = Integer.valueOf(numeroDocumentoPersona.getText().toString());


    miDocumDatos
            .whereEqualTo(PERSON_KEY_UNIQ, verifPersonKy).limit(1)
            .get()
            .addOnCompleteListener(new OnCompleteListener<QuerySnapshot>() {
                @Override
                public void onComplete(@NonNull Task<QuerySnapshot> task) {
                    if(task.getResult().isEmpty()){
                        Intent pass = new Intent( packageContext: Verificar_documento.this, MainActivity.class);
                        startActivity(pass);
                    }else{
                        Toast.makeText(getApplicationContext(),  text: "El documento " + +numeroDocuPerson +
                                " ya esta registrado, intente con otra " , Toast.LENGTH_SHORT).show();
                        Log.d(TAG,  msg: "No se obtiene resultado", task.getException());
                    }
                }
            });
}
```

Fuente: elaboración propia.

La Figura 4-14 verifica la existencia de un registro con el número de documento digitado luego de presionar el botón “Validar”; si el registro no existe, se redirecciona a la pantalla de ingresar datos Figura 4-15. Con la ejecución de la función de la Figura 4-14, se pudo completar el caso de uso de la Tabla 4-5.

Tabla 4-5. Caso de uso para verificar un registro en la nube.

Identificador	Md_Rg_002
Nombre de caso de uso	VERIFICAR REGISTRO DE DOCUMENTO EN LA NUBE
Actor(es)	Sistema
Indispensable / deseable	Indispensable
Prioridad	Alta
Visible / no visible	Visible
Autor	Andrés Felipe Barragán Jaimes
Fecha de elaboración	01/02/2021
Revisión	María del Pilar Salamanca Azula
Última fecha de revisión	14/04/2021

Resumen	El sistema verifica si el documento ya está registrado en Firebase.	
Entradas	Conexión a la base de datos Firebase.	
Salidas	Redirecciona a la pantalla de ingresar datos, cuando el registro no existe.	
Curso básico de uso	Usuario	Sistema
	2. Elige el tipo de documento y digita el número de identificación. 3. Oprime el botón "Validar".	1. Muestra la pantalla de verificar documento. 4. Busca el documento en Firebase. 5. Si el documento no existe en Firebase, redirecciona a la pantalla Ingresar Datos.
Caminos alternativos	Usuario N/A	Sistema 5.1 Si el documento ya está registrado, informa al usuario y no le permite avanzar a la pantalla de ingreso de datos.
Caminos de excepción	Usuario N/A	Sistema N/A

Fuente: elaboración propia.

Al completarse el flujo normal de la Tabla 4-5, el usuario podrá pasar a la actividad para el registro manual de sus datos.

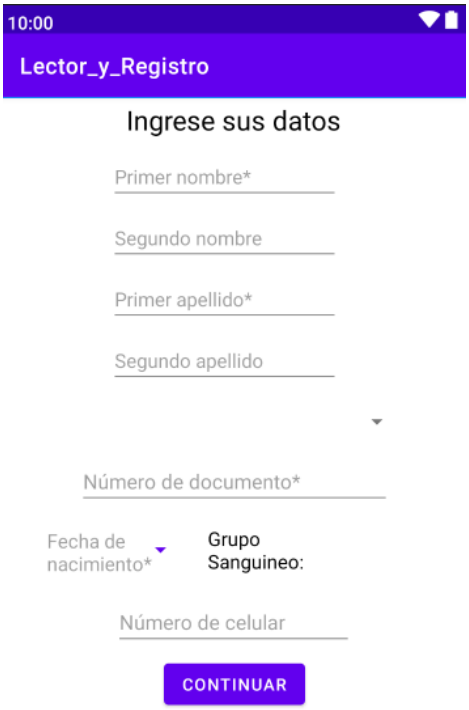
4.4.2. Registro manual de la persona

Al verificar que no existe un documento de identificación en la nube con los datos del usuario, se prosigue a solicitarle al usuario que ingrese los datos de manera manual. Los campos señalados con un asterisco se deben llenar de manera obligatoria, y en caso de que no llene todos los datos obligatorios, aparecerá un

indicador rojo en aquellos que hagan falta. Una vez complete todos los campos obligatorios, el usuario puede proseguir a la siguiente actividad.

La Figura 4-15 muestra la pantalla que verá el usuario donde deberá digitar los datos correspondientes. Al completar los campos solicitados, seguirá el flujo del caso de uso mostrado en la Tabla 4-6.

Figura 4-15. Pantalla para ingresar datos.



Fuente: Elaboración propia.

Tabla 4-6. Caso de uso para ingresar los datos.

Identificador	Md_Rg_003
Nombre de caso de uso	INGRESAR LOS DATOS DEL USUARIO
Actor(es)	Usuario
Indispensable / deseable	Indispensable
Prioridad	Alta
Visible / no visible	Visible

Autor	Andrés Felipe Barragán Jaimes	
Fecha de elaboración	01/02/2021	
Revisión	María del Pilar Salamanca Azula	
Última fecha de revisión	14/04/2021	
Resumen	El usuario ingresa los datos de su documento de identidad y se verifica que estén completos.	
Entradas	Datos ingresados manualmente: - Primer nombre (obligatorio) -Segundo nombre - Primer apellido (obligatorio) - Segundo apellido - Tipo de documento (obligatorio) - Número de identificación (obligatorio) - Fecha de nacimiento (obligatorio) - Grupo sanguíneo y RH (obligatorio) - Número celular (obligatorio)	
Salidas	Redirecciona a la pantalla de Datos para Verificar.	
Curso básico de uso	Usuario	Sistema
	1. Digita los datos solicitados. 2. Presiona el botón “Continuar”.	3. Valida si se ingresaron todos los datos obligatorios. 4. Redirecciona a la pantalla Datos para Verificar. 5. Guarda los datos digitados por el usuario y los muestra en pantalla.
Caminos alternativos	Usuario	Sistema
	1.1. Si el usuario quiere modificar alguno de los datos ingresados, se devuelve a la pantalla Ingresar Datos.	N/A
Caminos de excepción	Usuario	Sistema
	N/A	3.1. Si el usuario no ingresó alguno de los datos obligatorios, no puede continuar.

Fuente: elaboración propia.

Al continuar el flujo normal de la Tabla 4-6, cuando el usuario presione el botón “Continuar”, procederá a la pantalla de verificación de datos Figura 4-16.

4.4.3. Datos guardados listos para validar

Luego de que el usuario ingrese sus datos, se le redirecciona a la pantalla *Datos para Verificar,* que contiene una vista previa de los datos digitados. En esta pantalla, se le indica al usuario que esos datos deben corresponder con los de su documento de identidad pues la siguiente actividad se encargará de escanear y comparar los datos digitados con la información guardada en el código de barras de su documento.

Figura 4-16. Pantalla de datos para verificar.

Fuente: elaboración propia.

La Figura 4-16 muestra la pantalla que verá el usuario antes de presionar el botón "Verificar" para comparar los datos escritos con los datos guardados en el código de barras que se encuentra al respaldo del documento de identidad y el número celular donde esta realizando el registro. La Tabla 4-7 muestra el flujo de actividades que se realizan en la pantalla antes y después de verificar los datos.

Tabla 4-7. Caso de uso para validar con escaneo.

Identificador	Md_Rg_004
Nombre de caso de uso	VERIFICAR CON ESCANEO
Actor(es)	Usuario - Sistema
Indispensable / deseable	Indispensable
Prioridad	Alta
Visible / no visible	Visible

Autor	Andrés Felipe Barragán Jaimes	
Fecha de elaboración	01/02/2021	
Revisión	María del Pilar Salamanca Azula	
Última fecha de revisión	14/04/2021	
Resumen	Se escanea con el celular el código de barras presente en los documentos de identidad para validar la información manualmente diligenciada.	
Entradas	Los datos guardados en la pantalla Ingresar Datos sin.	
Salidas	Datos verificados luego de escanear el código de barras del documento de identificación.	
Curso básico de uso	Usuario	Sistema
	1. Tiene vista previa de los datos digitados. 2. Presiona el botón "Verificar". 3. Usa el smartphone para escanear el código de barras del documento.	4. Compara los datos ingresados con la información guardada en el código de barras del documento escaneado. 5. Informa que los datos coinciden y pasa a la pantalla Autenticar SMS.
Caminos alternativos	Usuario N/A	Sistema N/A
Caminos de excepción	Usuario N/A	Sistema 4.1. Si la información escaneada no coincide con los datos digitados, la aplicación devuelve al usuario hacia la pantalla de visualización de datos.

Fuente: elaboración propia.

Al seguirse el flujo normal de la Tabla 4-7, el usuario entrará a la pantalla de escaneo, para que coloque el documento frente a la cámara del teléfono (Figura 4-17), se lea el código de barras del documento y se redireccione a la pantalla de Autenticar SMS que se ve en la Figura 4.18.

4.4.4. Escaneo de documento

Luego de oprimir el botón “Verificar” (Figura 4-16) se procede a activar la cámara del teléfono y el usuario deberá centrar el escáner (colocar la línea roja horizontal) en la mitad del código de barras de su documento.

Figura 4-17. Actividad de escaneo.

Fuente: elaboración propia.

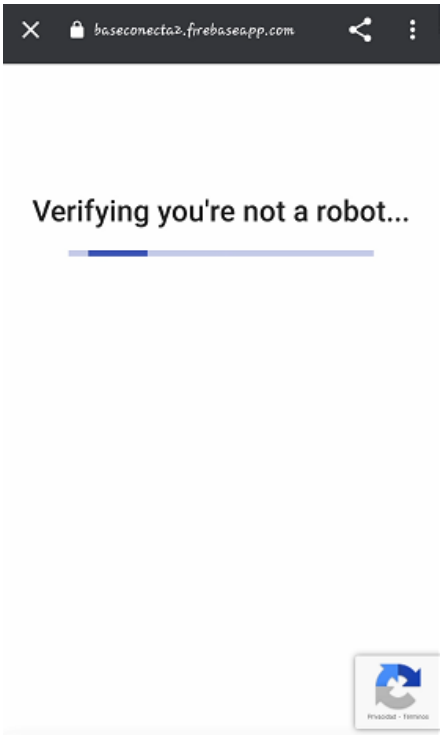
Al completar el escaneo que se muestra en la Figura 4-17, pasará una de dos cosas: la primera es que si los datos manualmente diligenciados coinciden con la información presente en el documento, se redireccionará al usuario a la pantalla de Autenticar SMS vista en la Figura 4-19. Si no coinciden los datos digitados con los del documento, la aplicación se devolverá a la pantalla anterior para que el usuario revise si los datos fueron escritos correctamente.

4.4.5. Autenticación por SMS

Esta actividad se ejecutará siempre que el escaneo haya sido completado con éxito. El usuario debío haber digitado el número de celular desde el cual está realizando

el registro y con el formato numérico correspondiente a Colombia, luego se hará una validación reCAPTCHA de la Figura 4.18 que verificará que el usuario no sea un *bot* y si el número que ingresó es correcto, recibirá un mensaje de texto con un código que el usuario debe escribir en el campo “Ingresar el código SMS” (Figura 4-19). Para finalizar, oprimirá el botón “Autenticar”. En el caso de que se complete con éxito la autenticación, se redireccionará a la pantalla principal de Conecta2.

Figura 4.18. Pantalla reCAPTCHA.



Fuente: elaboración propia

Figura 4-19. Pantalla de autenticar SMS.

Fuente: elaboración propia.

La Figura 4-19 es la pantalla que verá el usuario luego de que sus datos coincidan al escanear su documento. El flujo para este caso de uso se explica en la Tabla 4-8.

Tabla 4-8. Caso de uso para autenticar mediante SMS

Identificador	Md_Rg_005
Nombre de caso de uso	AUTENTICACIÓN SMS
Actor(es)	Usuario - Sistema
Indispensable / deseable	Indispensable
Prioridad	Alta
Visible / no visible	Visible
Autor	Andrés Felipe Barragán Jaimes
Fecha de elaboración	01/02/2021
Revisión	María del Pilar Salamanca Azula
Última fecha de revisión	14/04/2021

Resumen	Se verifica el número celular que el usuario ingreso de forma manual anteriormente, para finalmente recibir un mensaje con el código generado y luego escribirlo para autenticar.	
Entradas	Número celular de la pantalla de ingreso de datos. Mensaje con código de autenticación.	
Salidas	Autenticación exitosa.	
Curso básico de uso	Usuario	Sistema
	1.Luego de escanear los datos, procede a esperar el mensaje de texto con el código si el número de celular es correcto. 3. Recibe un mensaje de texto con el código, lo ingresa en el campo correspondiente y luego presiona "Autenticar".	2. Manda una solicitud para generar código con el número diligenciado y direccionar un ReCAPTCHA automático. 4. Autentica el código enviado y redirecciona a la pantalla de Foto y Registro.
Caminos alternativos	Usuario N/A	Sistema N/A
Caminos de excepción	Usuario	Sistema
	1.1. El usuario digita un código diferente al recibido.	2.1. Muestra un mensaje donde se le indice al usuario que digite correctamente el código o que solicite uno nuevo.
	1.2. El usuario se demora más de un minuto en digitar el código recibido.	2.2. Le informa al usuario que el código expiró y que debe solicitar uno nuevo.
	1.3. El usuario solicita 5 códigos consecutivamente.	2.3. Le informa al usuario que su dispositivo se bloqueó por actividad inusual y que lo intente más tarde.
	1.4. El usuario digita el número de teléfono que no corresponde al formato para Colombia.	2.4. Le informa al usuario que el formato no corresponde.

Fuente: elaboración propia.

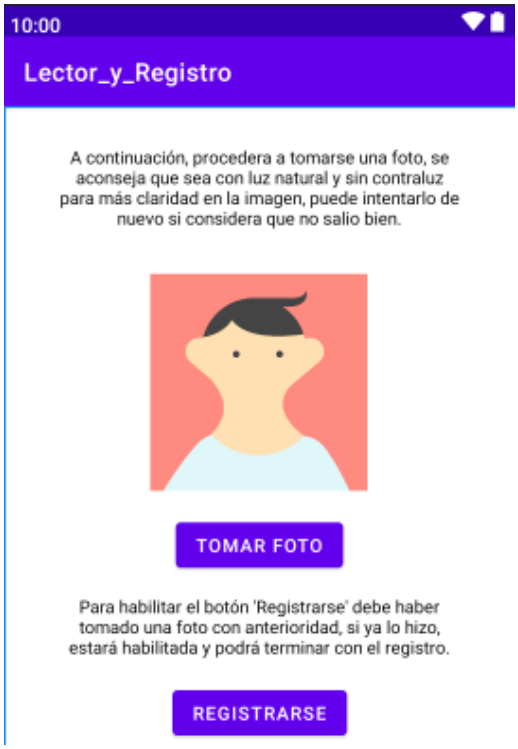
Al realizarse el flujo normal de la Tabla 4-8, el usuario será redireccionado a la pantalla de Foto y Registro (Figura 4-20) para que se tome una foto y se pueda registrar.

4.4.6. Toma de foto y registro

Si los datos coincidieron con el escaneo del documento, la anterior pantalla de Autenticar SMS redirecciona al usuario a la pantalla de foto y registro , sin embargo, primero debe tomarse una foto para luego poder usar el botón “Registrarse”. Cuando el usuario toma la foto, puede elegir cualquiera de las dos cámaras del celular, y si está de acuerdo con la foto tomada debe dar click en el botón “Aceptar”.

Cuando la foto ha sido tomada y aceptada, el usuario puede presionar el botón “Registrarse”. En ese momento, la aplicación verificará una vez más en la base de datos en la nube, si el documento del usuario ya se encuentra registrado. Si el registro de ese documento ya existe, no realizará ni la inserción local ni en la nube del registro diligenciado. La Figura 4-20 muestra la pantalla desde la cual el usuario puede tomar la foto y, posteriormente, hacer el registro.

Figura 4-20. Pantalla de toma de foto y registro.



Fuente: elaboración propia.

La Tabla 4-9 presenta el flujo para el caso de uso asociado a esta funcionalidad, denominado *Registrar Usuario*.

Tabla 4-9. Caso de uso para la pantalla de foto y registro.

Identificador	Md_Rg_006
Nombre de caso de uso	REGISTRAR USUARIO
Actor(es)	Usuario
Indispensable / deseable	Indispensable
Prioridad	Alta
Visible / no visible	Visible
Autor	Andrés Felipe Barragán Jaimes
Fecha de elaboración	01/02/2021
Revisión	María del Pilar Salamanca Azula
Última fecha de revisión	14/04/2021

Resumen	El usuario se toma una foto con ayuda del smartphone y realiza el registro del documento de identificación tanto en la base de datos local como en la nube.	
Entradas	Imagen en el formato en el que la cámara tome las fotos. Datos escaneados y verificados.	
Salidas	Se almacena localmente la foto del usuario. El documento de identificación queda registrado en la base de datos local y en Firebase.	
Curso básico de uso	Usuario	Sistema
	1. Luego de haber verificado sus datos mediante el escaneo de su documento, el usuario procede a tomarse una foto con la cámara que prefiera. 3. Acepta la foto que previsualizó anteriormente. 6. Presiona el botón "Registrarse".	2. Se muestra una previsualización de cómo quedó la foto que se tomó el usuario con la cámara. 4. Guarda la fotografía temporalmente hasta que ocurra el registro. 5. Regresa a la pantalla de Foto y Registro y se observa la foto recién tomada en la pantalla. 7. Registra al usuario en la base de datos local y en Firebase. 8. Informa al usuario que el registro fue exitoso. 9. Redirecciona a la pantalla principal de Conecta2.
Caminos alternativos	Usuario	Sistema
	3.1. Si el usuario no está de acuerdo con la foto previsualizada, presiona el botón "Reintentar" y la toma de nuevo. 5.1. Si el usuario quiere cambiar la foto, presiona el botón "Tomar Foto" y repite el proceso.	7.1. Si el registro ya existe, muestra un mensaje informándole al usuario que ese documento ya fue registrado.
Caminos de excepción	Usuario	Sistema

	N/A	7.1. Si el usuario no se tomó la foto previamente, le informa que debe tomársela para poder hacer el registro.

Fuente: elaboración propia.

Al presionar el botón “Registrarse”, se realiza el flujo de actividades de la Tabla 4-9, en donde principalmente ejecuta una de dos acciones importantes. Una es que si ya existe un usuario registrado en la base de datos en la nube, no se proseguirá con el proceso, pero si no existe ningún registro en la base de datos en la nube y la persona se tomó una foto de manera correcta, el usuario podrá registrarse con normalidad y será redireccionado a la pantalla principal de Conecta2 mostrada en la Figura 4-21.

Figura 4-21. Pantalla principal de Conecta2

Fuente: elaboración propia.

4.4.7. Conexiones requeridas por el módulo de registro de usuarios de Conecta2

A continuación, se explican las conexiones utilizadas por el módulo de registro y que son necesarias para su operación.

4.4.7.1. Conexión a la base de datos local

Una de las funcionalidades más importantes es la creación y conexión de una base de datos local, puesto que estas acciones se realizan en el momento en el que se abre por primera vez la aplicación. Es necesario tener presente una clase importante llamada Modelo, que permite la conexión a la base de datos local e inserción de datos, y que se observa en la Figura 4-22.

Figura 4-22. Clase Modelo dentro de Android Studio.

Modelo.java

```
1  package com.example.lector_y_registro;
2
3  import ...
9
10 public class Modelo {
11
12     public SQLiteDatabase getConn(Context context){
13         ConexionSQLiteHelper conn = new ConexionSQLiteHelper(context);
14         SQLiteDatabase db = conn.getWritableDatabase();
15         Log.d( tag: "getConn",  msg: "se ha creado la base de datos");
16         return db;
17     }
18
19 @   int insertarUsuario(Context context, Usuario dto) {
20         int res = 0;
21         String sql = "INSERT INTO "+Utilidades.TABLA_USUARIO+" ("+Utilidades.PERSON_KEY+","+Utilida
22                 "VALUES ('"+dto.getUniquePersonRegister()+"','"+dto.getDocumentoid()+"','"+dto.getN
23         SQLiteDatabase db = this.getConn(context);
24         try{
25             db.execSQL(sql);
26             res = 1;
27         }catch(Exception o){
28             Log.d( tag: "insertarUsuario",  msg: "algo malo paso");
29         }
30         Log.d( tag: "insertarUsuario",  msg: "el valor de res es de "+ res);
31         return res;
32     }
33 }
34
```

Fuente: Elaboración propia.

Al ser una clase que permite la conexión con la base de datos, se usa para que otras clases puedan ejecutar consultas creando un objeto de clase Modelo y llamar a la función getConn().

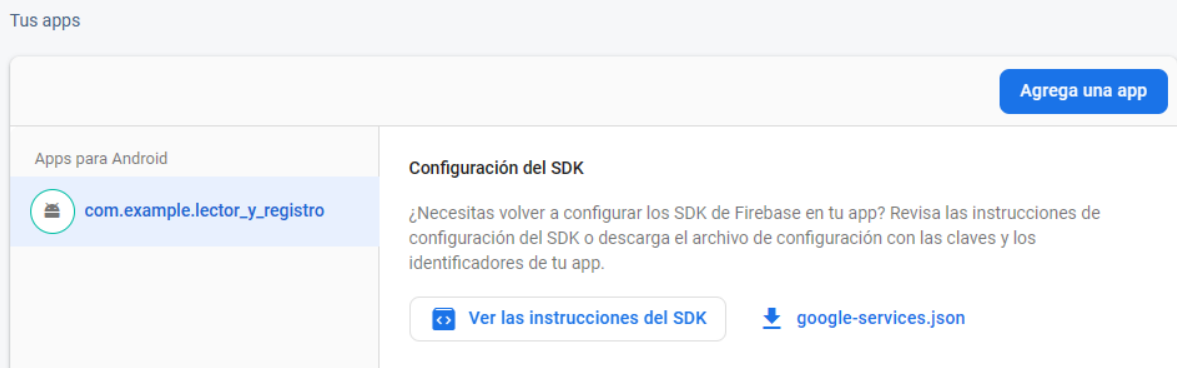
4.4.7.2. Conexión a la base de datos en la nube

Esta es la segunda conexión requerida para poder subir el registro a la nube. Su grado de dificultad depende de los datos que se requiera subir, pero para empezar, la conexión con el servicio de Firebase necesita 3 cosas básicas:

- Registrar la aplicación dentro de Firebase
- Modificar las dependencias en el graddle.app para permitir las librerías de Firebase dentro de la aplicación
- La creación de un documento JSON para el guardado de los datos en la nube.

La Figura 4-23 muestra la sección de Firebase en donde se pueden agregar aplicaciones que deseen usar los servicios que proporciona esta base de datos.

Figura 4-23. Aplicación registrada en Firebase.



Fuente: Elaboración propia.

La Figura 4-24 corresponde a la inclusión de las librerías de Firebase en Android Studio, las cuales se encuentran en el Gradle.app del programa.

Figura 4-24. Dependencias de firebase.

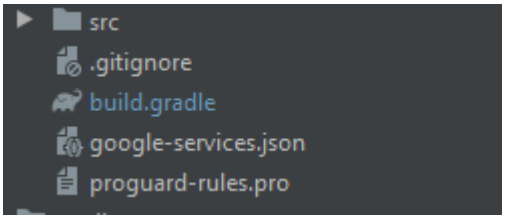
```
dependencies {

    // Import the BoM for the Firebase platform
    implementation platform('com.google.firebase:firebase-bom:28.1.0')
    // Declare the dependency for the Cloud Firestore library
    // When using the BoM, you don't specify versions in Firebase library dependencies
    implementation 'com.google.firebase:firebase-firestore'
```

Fuente: Elaboración propia.

En la Figura 4-25 se puede ver parte de la estructura de archivos del proyecto, donde el documento *google-services.json* es indispensable para la conexión con Firebase y poder usar sus servicios.

Figura 4-25. Archivo google-services. json

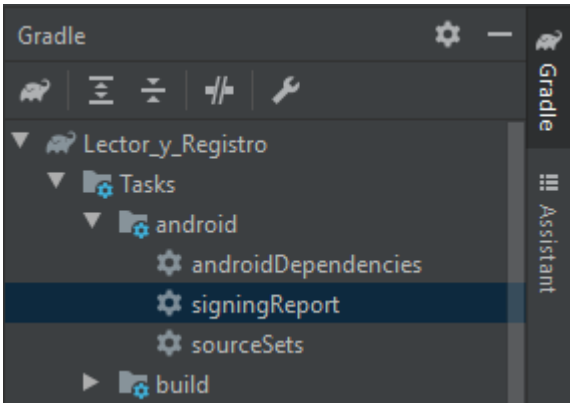


Fuente: Elaboración propia.

4.4.7.3. Conexión para autenticación móvil

Firebase permite diferentes tipos de autenticación. Para este desarrollo se decidió usar el número de celular, con el fin de que la aplicación valide que el número que el usuario digitó sea, en efecto, el del teléfono desde el cual está utilizando Conecta2. Para realizar la conexión, se busca el *hash* SHA1 dentro de la aplicación en Android Studio, esa clave servirá como una huella digital para *debuguear* aplicaciones en Firebase, y se debe registrar en la consola de Firebase. El SHA1 se encuentra en el lugar mostrado en la Figura 4-26.

Figura 4-26. Lugar donde se encuentra el SHA1 debugueable.



Fuente: Elaboración propia.

Luego, se copia el SHA1 y se ingresa en la configuración de Firebase como huella digital, colocándola en el espacio mostrado de la Figura 4-27 para poder conectarse a los servicios de Firebase Authentication.

Figura 4-27. Campo para huella digital en Firebase.

Fuente: Elaboración propia.

Para la etapa de liberación de toda la fase, se verificó que el módulo funcionara correctamente junto con la revisión de las bases de datos tanto local como en la nube.

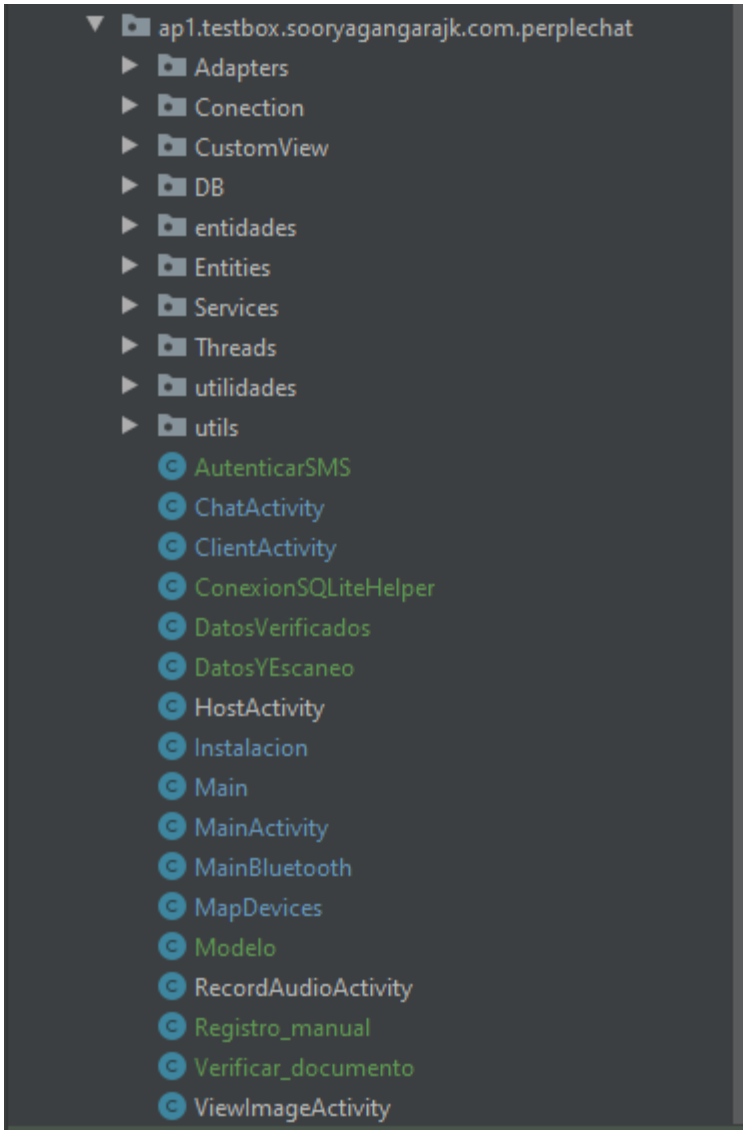
4.5. Fase de estabilización

Una vez se desarrolló con éxito la aplicación de registro de usuarios, se procedió a integrarla como un módulo dentro del código fuente de la aplicación Conecta2. Se actualizaron librerías que ayudaron a que la aplicación tuviera compatibilidad con las nuevas funcionalidades, entre las que se puede destacar la función de escaneo y la creación de bases de datos local y en la nube. Algunas de las librerías que estaban presentes desde la creación de Conecta2 fueron sustituidas por otras que implementan un mejor soporte general a las funcionalidades de la aplicación, permitiendo compilar de una manera correcta la integración del módulo de registro.

La integración del nuevo módulo de registro y sus clases a Conecta2, no repercutió en las funcionalidades principales de esta aplicación. Únicamente se cambió el proceso de registro antiguo, el cual únicamente le solicitaba al usuario ingresar su nombre y el nombre que le iba a dar al teléfono. Con el nuevo módulo de registro, el proceso se realiza de una manera más rigurosa, validando la identidad del usuario mediante la información contenida en su documento de identificación.

En la Figura 4-28 se pueden observar en color verde aquellas clases que se añadieron al código fuente principal, procurando que ninguna generara errores.

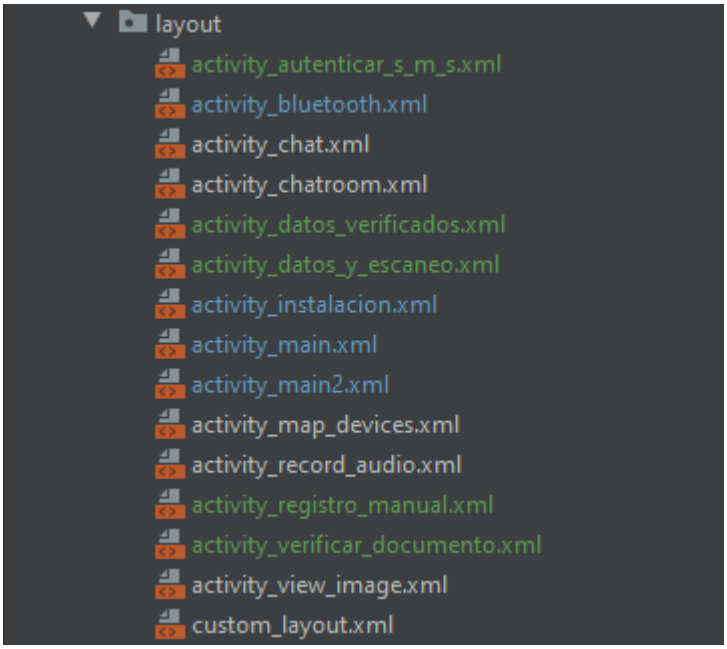
Figura 4-28. Estructura de las clases de la aplicación Conecta2.



Fuente: elaboración propia.

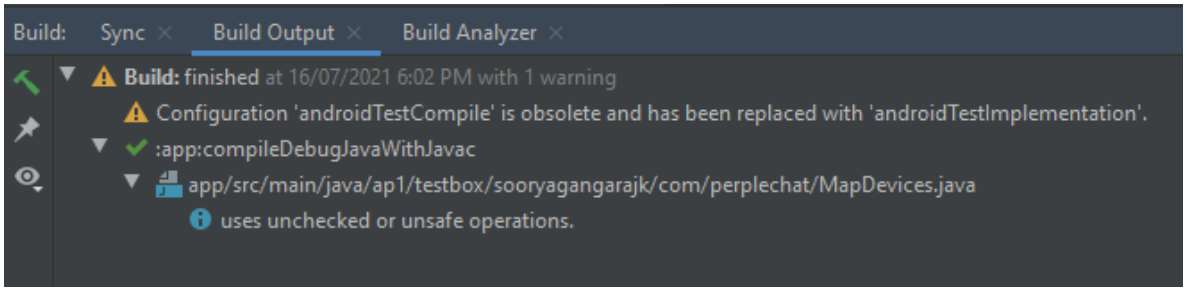
Al igual que en la Figura 4-28, en la Figura 4-29 se muestran en color verde las interfaces añadidas. También en varias de las interfaces antiguas de Conecta2 se llevó a cabo la actualización de librerías para el soporte gráfico de las pantallas y en la Figura 4-30 se muestra la correcta compilación de la integración del módulo.

Figura 4-29. Interfaces gráficas de Conecta2.



Fuente: elaboración propia

Figura 4-30. Compilación de código fuente de Conecta2.



Fuente: elaboración propia.

4.6. Fase de prueba y reparación

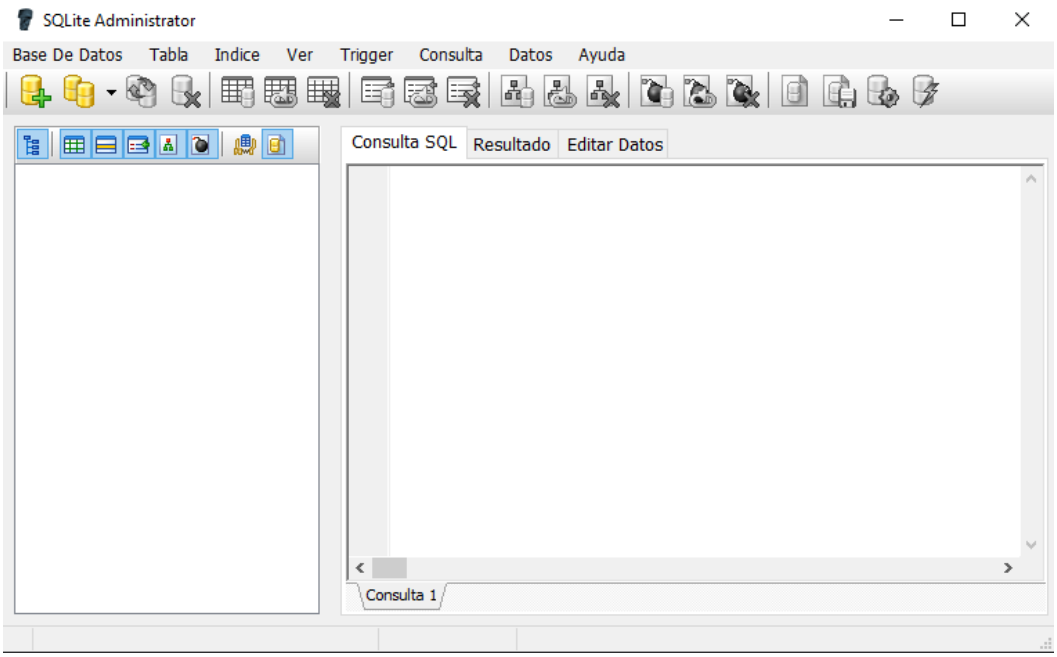
Para esta fase, se realizaron pruebas de uso de la aplicación para cada funcionalidad. Se hicieron pruebas en celulares con sistema operativo Android 7, Android 8 y Android 10. Junto con la directora se encontraron varios errores en las primeras versiones compiladas de la aplicación, principalmente porque no había un flujo de actividades y excepciones muy claro. Los errores y correcciones tanto funcionales como de interfaz gráfica y de entradas de datos más destacables, son los siguientes.

- Las entradas para números permitían escribir letras, se cambió el tipo de entrada de los recursos para que solo se digitaran números cuando fueran necesarios.
- En la pantalla de registro, el usuario podía poner cualquier tipo de información en el grupo sanguíneo. Se cambió por un *spinner* que despliega los grupos sanguíneos existentes.
- En la pantalla de toma de foto y registro, cuando el usuario oprimía “Tomar foto” pero salía y no la tomaba, para luego oprimir el botón “Registrarse”, la aplicación fallaba y se cerraba en un segundo o tercer intento de registro. Dependiendo de la versión de Android, se redirigía a otra pantalla que no estaba contemplada. Esto se arregló, haciendo que se verificara que antes de realizar un registro, existiera un recurso temporal de imagen para incluir en la base de datos local, producto de la fotografía capturada.
- Para terminar el registro, cuando el usuario oprimía el botón “Registrarse”, si el número de documento del usuario ya existía en Firebase, no se registraba de nuevo en la nube, pero sí se realizaba el registro en la base de datos local y pasaba a la pantalla principal de Conecta2. Esto se arregló, modificando el lugar desde donde se llamaba a la función de registro local y el lanzador de actividad para pasar a la pantalla principal. Las acciones se realizaban

cuando se verificaba que el documento no estuviera en la nube, puesto que si ya existía, no debería permitir pasar a la pantalla principal.

Las pruebas más importantes eran las inserciones de datos tanto locales como en la nube, pues el registro se realiza leyendo y verificando que no existan registros en el dispositivo celular y en Firebase. Android Studio solo posee un lector de recursos de dispositivos que permite ver los archivos existentes locamente, pero no posee una herramienta integrada para verificar que las bases de datos creadas tuvieran registros. Como se necesitaba una herramienta para verificar que se insertaran los datos sin necesidad de hacer muchas consultas dentro del código, se procedió a descargar el programa que se ve en la Figura 4.31. Esta herramienta permite leer los archivos de bases de datos, por lo que cuando se creaba un archivo de registro, se guardaba en una carpeta para luego buscarla con SQLite Administrator, que permite hacer consultas rápidamente luego de cargar la base de datos.

Figura 4.31. Programa SQLite Administrator



Fuente: elaboración propia

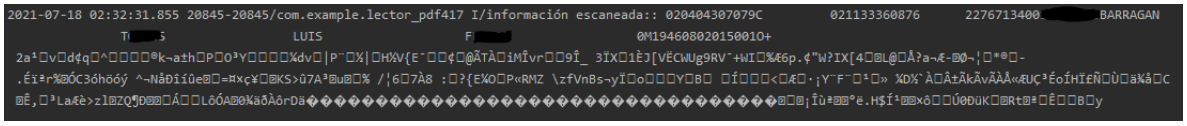
5. ANALISIS Y RESULTADOS

En este capítulo se evidenciará cómo, mediante las diferentes funcionalidades implementadas en el módulo de registro de Conecta2, se logró el cumplimiento de los objetivos propuestos para este proyecto.

5.1. LECTURA DEL CÓDIGO DE BARRAS DE LOS DOCUMENTOS DE IDENTIFICACIÓN

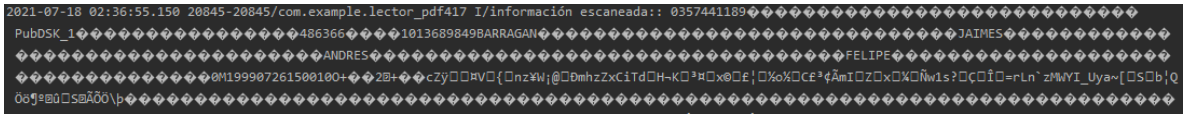
En el módulo de registro, el código de barras de los documentos de identidad se lee mediante el uso de la librería ZXing. Con esta librería se hizo inicialmente una pequeña aplicación únicamente para leer el código de barras, encontrando que la forma como se distribuye la información dentro del código de barras varía, aparentemente, según el año de expedición del documento de identidad. En la Figura 5-1, por ejemplo, se observa la información contenida en el código de barras de un documento expedido hace más de 20 años. En la Figura 5-2, a su vez, se presenta la información correspondiente a un documento expedido hace aproximadamente 4 años. Es interesante ver cómo entre un documento y otro cambia el tipo de caracteres que separan los datos de la persona, entre otras cosas. Aunque aquí se muestran solamente dos casos, esta situación se pudo evidenciar también en otros documentos escaneados.

Figura 5-1. Información de un documento expedido hace mas de 20 años



Fuente: elaboración propia

Figura 5-2. Información de un documento expedido hace aproximadamente 4 años



Fuente: elaboración propia

A pesar de haber buscado información en la Registraduría Nacional del Estado Civil que permitiera entender mejor cómo esta institución ha modificado la información en el código de barras a través del tiempo, no se encontró ningún recurso que explicara el tipo de estructura que posee la información y cuántos otros existen. En Colombia se comercializa software especializado en la tarea de obtener la información de los códigos de barras de los documentos de identificación, pero seguramente existe un acuerdo entre las empresas que desarrollan ese software y la Registraduría que les permite conocer en detalle cómo ha sido la evolución de los códigos de barras en los documentos colombianos. Una de las consecuencias de esta situación es que fue necesario dedicar más tiempo de lo planeado inicialmente en la codificación, mientras se buscaban alternativas para poder leer directamente la información de los documentos.

Como resultado de los hallazgos descritos anteriormente, se encontró que una opción viable y fácil de usar era la creación de un formulario para que la persona digitara la información de su documento (Figura 5-3) y, posteriormente, escaneara el código de barras del mismo, esto con el fin de verificar que la información ingresada por la persona coincidiera exactamente con la de su identificación.

El proceso de escaneo y verificación posee dos flujos de actividades, el primero ocurre cuando la información digitada por el usuario coincide con la que se encuentra en el código de barras del documento. En ese caso, la aplicación le indica al usuario que la información es correcta, tal como se muestra en el *toast* de la Figura 5-4. El segundo flujo sucede cuando los datos ingresados por el usuario son diferentes de los guardados en el código de barras, en cuyo caso la aplicación le

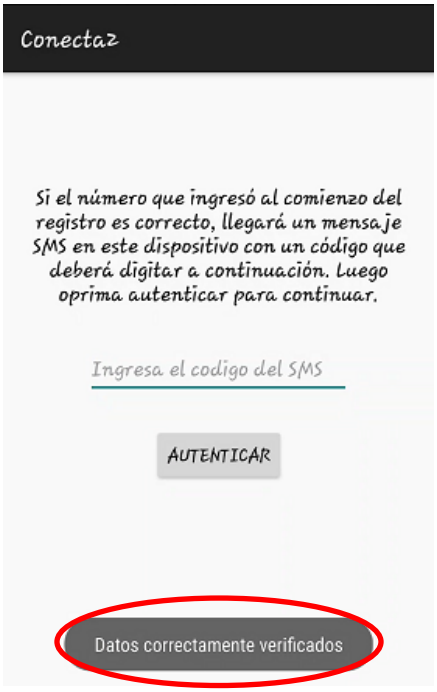
notifica al usuario, nuevamente mediante un *toast*, que los datos no coinciden (Figura 5-5).

En la Figura 5-3 se puede observar un ejemplo de los datos digitados (nombres, apelllidos, tipo de documento, número del documento, fecha de nacimiento, grupo sanguíneo y, adicionalmente, el número del celular desde el cual se está llevando a cabo el registro).

Figura 5-3. Datos diligenciados por el usuario.

Fuente: elaboración propia

Figura 5-4. Mensaje cuando el escaneo es correcto.



Fuente: elaboración propia.

Figura 5-5. Mensaje cuando la información escaneada no coincide.

Fuente: elaboración propia

De esta manera, mediante el proceso de digitación, escaneo y verificación de la información del documento de identidad que realiza el módulo de registro de Conecta2, se puede evidenciar que el primer objetivo del proyecto se cumplió.

5.2. VERIFICACIÓN DEL NÚMERO DE CELULAR MEDIANTE SMS

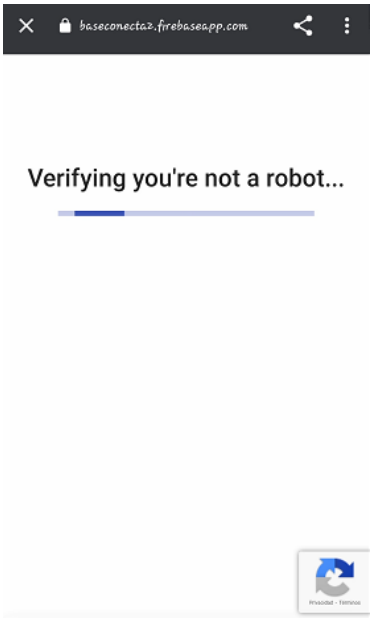
Una vez la aplicación comprueba que los datos ingresados por el usuario sí son los de su documento de identidad, prosigue a verificar el número del teléfono celular que el usuario digitó. Con ese propósito, la aplicación se conecta con el servicio de autenticación de Firebase, y realiza los siguientes procesos: primero verifica que quien esté realizando la acción no sea un *bot*, y luego envía un código mediante un mensaje SMS. Tan pronto reciba su código, el usuario deberá digitarlo y luego la aplicación verificará si es correcto o no.

No obstante, el flujo puede variar dependiendo de los datos que el usuario digite: si digitó un número que no se ajusta al formato, el sistema le dará un mensaje indicando que el formato es incorrecto (Figura 5-6); si el formato es correcto, se redirecciona al usuario a un reCAPTCHA (Figura 5-7) que verifica que no sea un *bot* quien realiza las acciones, y, en seguida, llegará un mensaje SMS con un código de verificación al dispositivo (Figura 5-8). Si el usuario digita el código equivocado, la aplicación le advertirá esta situación y deberá digitar el código correcto (Figura 5-9). Si se demora más de un minuto en digitar el código, le informará que el código es inválido y que debe pedir uno nuevo (Figura 5-10).

Figura 5-6. Mensaje cuando el número no cumple formato de celular.

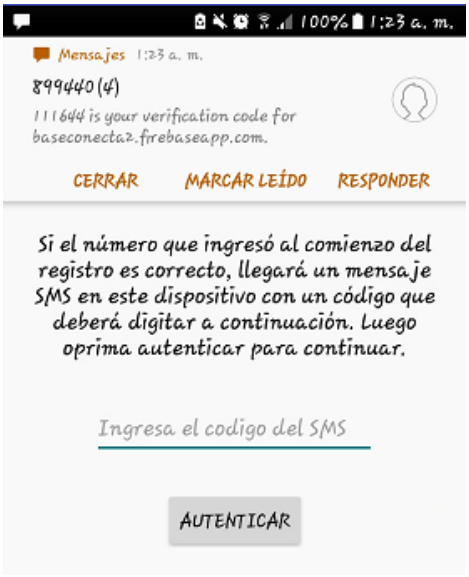
Fuente: elaboración propia.

Figura 5-7. Redirección web en celular de reCAPTCHA.



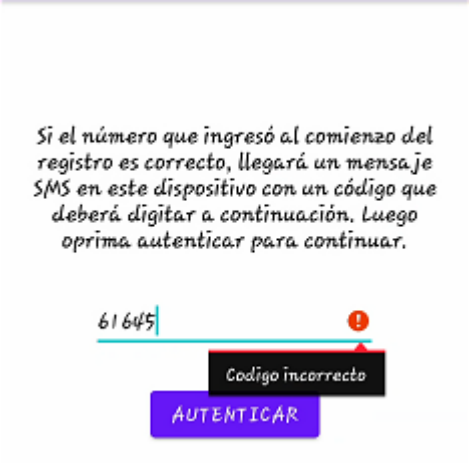
Fuente:elaboración propia.

Figura 5-8. Notificación del código por medio de un mensaje SMS.



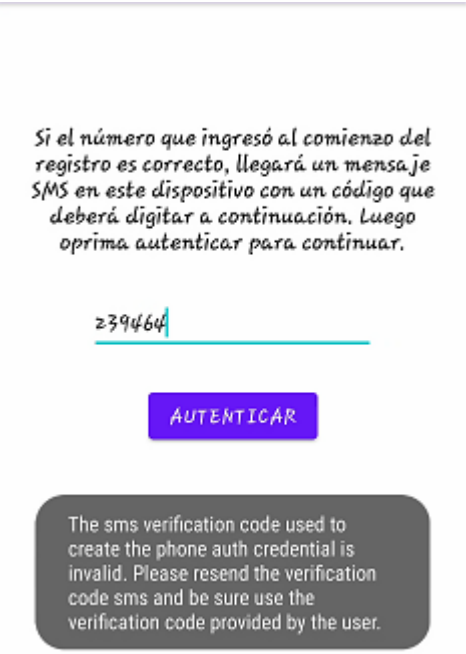
Fuente: elaboración propia.

Figura 5-9. Mensaje cuando código no es correcto



Fuente: elaboración propia

Figura 5-10. Mensaje cuando el código expira



Fuente: elaboración propia

La verificación del número celular mediante un mensaje SMS es el segundo objetivo específico y se demuestra así su cumplimiento.

5.3. INTEGRACIÓN DEL MÓDULO A LA APLICACIÓN CONECTA2

El tercer objetivo se refiere a la integración del módulo de registro a la aplicación Conecta2. Este proceso se puede verificar en el capítulo 4 sección 4.5, donde se explica la fase de estabilización y se evidencia desde Android Studio, en la Figura 4-28 así como en la Figura 4-29, cómo la integración dentro del desarrollo de Conecta2 fue exitosa.

En el flujo del módulo de registro, una vez el usuario presiona el botón “Registrarse” en la pantalla de Foto y Registro de la Figura 4-20, si el proceso de registro es exitoso, se le informa esta situación al usuario mediante un *toast* y aparecerá la pantalla principal de Conecta2 (Figura 5-11).

Figura 5-11. Mensaje de registro exitoso

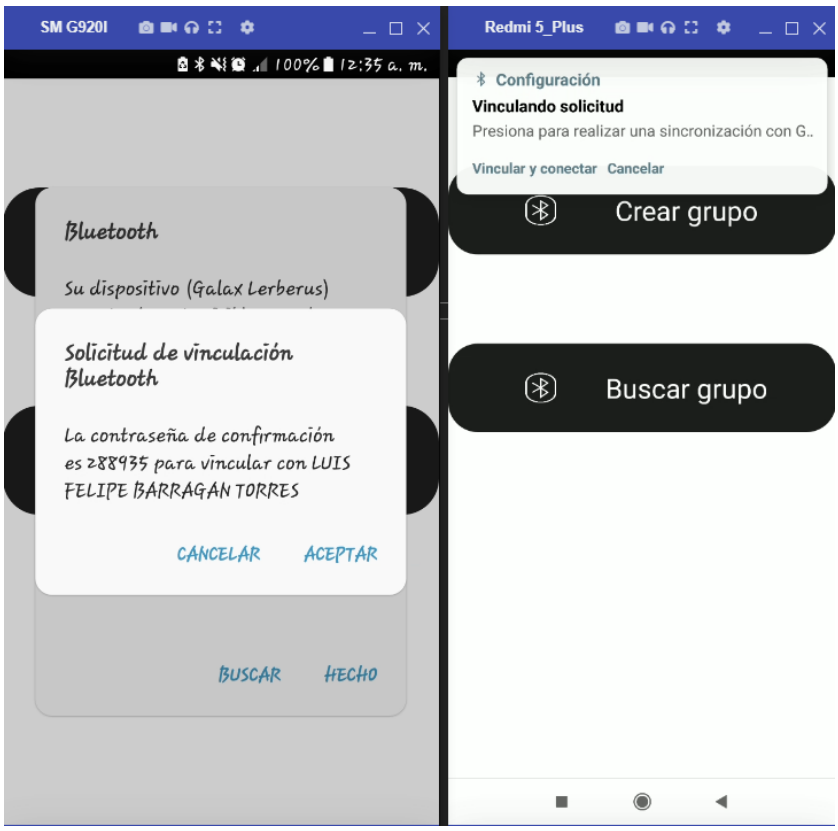
Fuente: elaboración propia

5.4. NOMBRE AGREGADO EN LOS DEMÁS MÓDULOS DE CONECTA2

Cuando el usuario se ha registrado exitosamente, Conecta2 lo reconoce por los nombres y apellidos presentes en su documento de identificación. Es por ello que, en cada módulo, aparecerá identificado tal como se observa en la parte superior de la Figura 5-11, a la derecha de la palabra *Hola*. Sin embargo, se encontró que en algunas versiones de Android, el nombre que se toma para el módulo de Bluetooth no siempre es aquel con el que se registró el usuario sino que se toma el nombre del teléfono móvil. Por ahora se desconoce qué ocasiona esto, por lo que se recomienda que más adelante en el desarrollo, se indague qué cambios se deben hacer dentro del código de Conecta2 para que haya compatibilidad con todos los dispositivos.

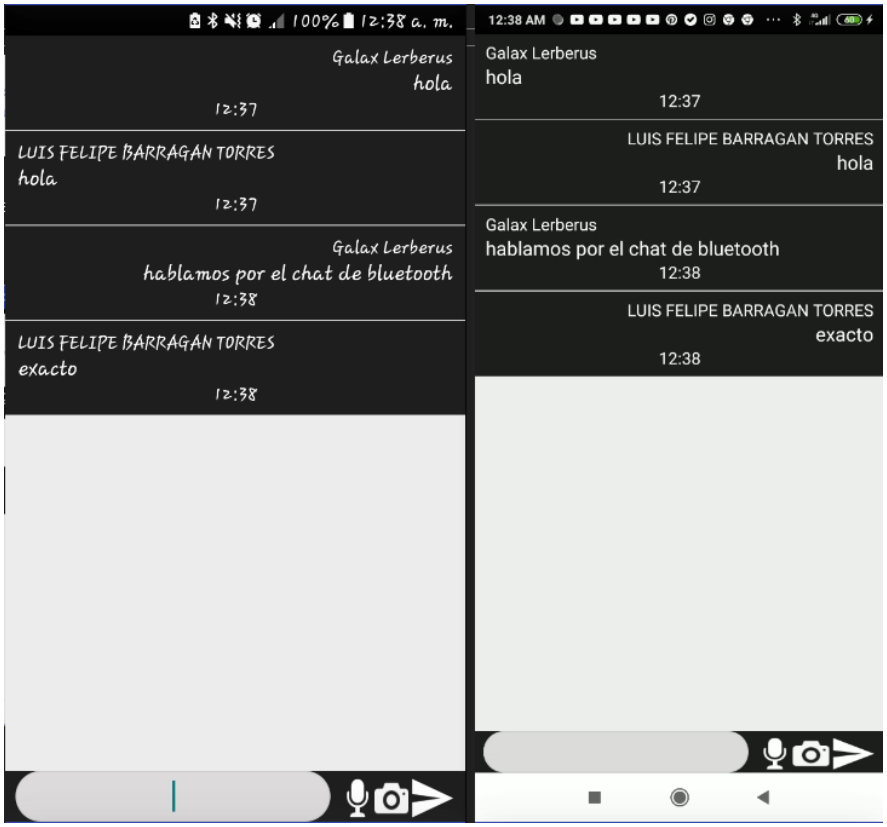
En la Figura 5-12, se puede ver el módulo de Bluetooth en ejecución en 2 dispositivos cuando ocurre el emparejamiento de los teléfonos, y en la figura 5-13 manteniendo un chat. Se puede observar que en uno de los celulares sí cambió el nombre, mientras que en el otro no (un celular tiene Android 7.0, el otro Android 8.1). Sin embargo, para la Figura 5-14 y Figura 5-15 ejecutando el módulo de Wifi Direct, los dispositivos encontrados poseen el nombre completo de la persona que se haya registrado.

Figura 5-12. Módulo de Bluetooth en dos dispositivos



Fuente: elaboración propia

Figura 5-13. Chat Bluetooth entre 2 dispositivos

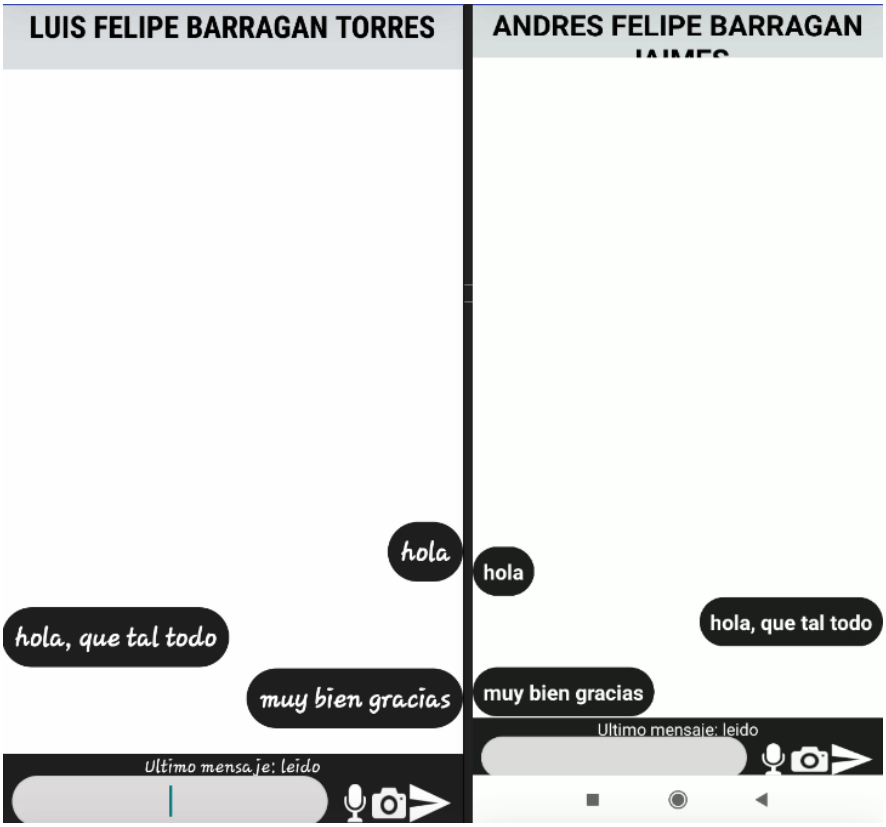


Fuente: elaboración propia

Figura 5-14. Dos dispositivos se encuentran por Wifi Direct

Fuente: elaboración propia

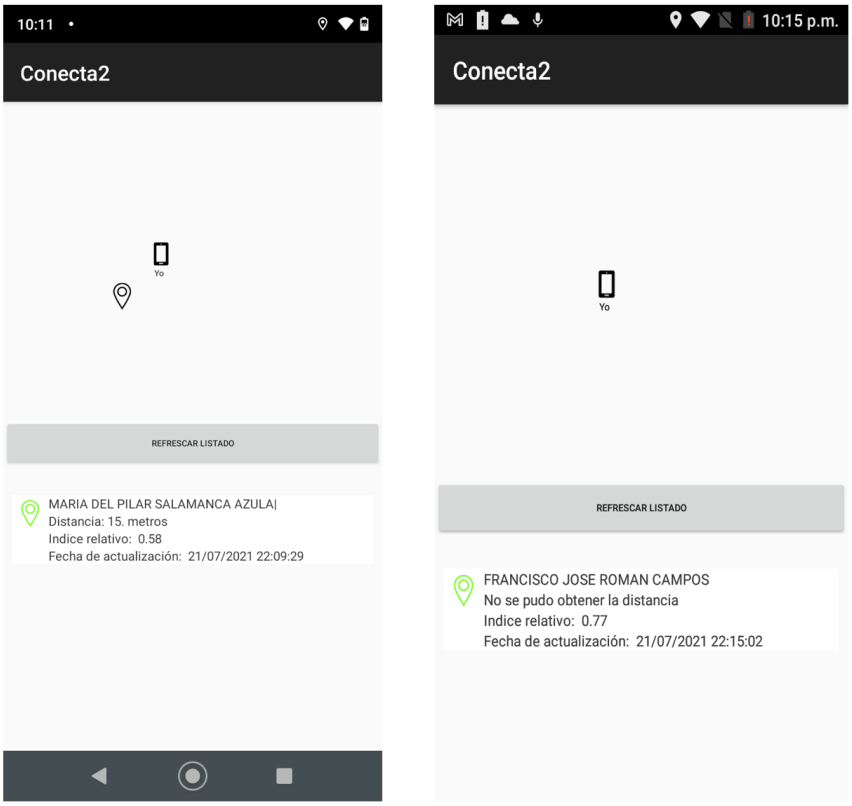
Figura 5-15. Chat por WiFi Direct entre 2 dispositivos con su nombre correspondiente



Fuente: elaboración propia

Finalmente, en la Figura 5-16 se encuentra el módulo de localizar dispositivos ejecutandose, aquí se muestran los dispositivos donde uno posee el nombre y el segundo no, pues no se configura el nombre del dispositivo por posibles permisos que aun no se pueden controlar, pero para otros dispositivos si es posible cambiar el nombre predeterminado del sistema.

Figura 5-16. Módulo de localizar dispositivos



Fuente: elaboración propia

Estas evidencias demuestran el cumplimiento del cuarto objetivo de la tesis, pues el nombre de la persona se puede identificar en los módulos disponibles de la aplicación.

6. CONCLUSIONES Y RECOMENDACIONES

El nuevo módulo de registro de la aplicación Conecta2 hace más riguroso y robusto el proceso de registro de usuarios en el sistema. Con este módulo, los usuarios diligencian en un formulario los datos presentes en su documento de identidad junto con su número de celular. Luego, con ayuda de una API que permite escanear códigos de barras, el módulo verifica si los datos ingresados son correctos y si pertenecen al documento de identidad, para finalmente verificar el número del teléfono celular mediante el envío de un mensaje SMS. Originalmente, el proceso de registro en Conecta2 era muy simple y sin ningún tipo de verificación, pues el usuario debía digitar su nombre, apellido y el nombre que recibiría su dispositivo, y podía editarlo las veces que quisiera, esto implicaba que el teléfono se podría anuncia con cualquier nombre en la red puesto que no había ninguna verificación de los datos ingresados.

Si bien durante el proceso de registro del usuario se verifican y almacenan, además de los nombres, el grupo sanguíneo, la fecha de nacimiento, el número de documento y el número de celular, desde Conecta2 únicamente se están anunciando en la red, los nombres y apellidos del usuario. El proyecto de investigación decidirá más adelante, qué otra información se podrá mostrar en la red y quienes podrán verla (por ejemplo, rescatistas). La gran ventaja es que esa información junto con la fotografía que el usuario se toma, ya está disponible para el desarrollador y para usarla solo tendrá que realizar la consulta en SQLite. Esa misma información queda almacenada en los servicios de Firebase, exceptuando la fotografía, que es de alcance local exclusivamente.

La autenticación SMS añadida al módulo, resulta ser muy útil para corroborar que la persona realiza el registro desde el número celular que indicó en el formulario y, adicionalmente, también se hace una validación de que quien esté haciendo el

proceso de registro no sea un *bot.* Cabe resaltar que realizar la conexión con los servicios de Firebase es un procedimiento sencillo, pues hay muy buena documentación disponible en Internet.

A pesar de que existe documentación que explica el proceso para guardar información en la base de datos en la nube, fue un buen hallazgo encontrar recursos para poder eliminar el usuario y adaptarlo a la codificación del módulo. Esto se debe a que es diferente el proceso de eliminación que el de adicionar un nuevo documento, ya que los documentos creados en la nube poseen un nombre único con varios caracteres y es difícil buscar con exactitud qué documento está asociado a cada usuario registrado. Por esta razón, se debió acceder a los campos dentro del documento, referenciar el archivo JSON y crear una combinación de los datos existentes para obtener un dato único; esto evidencia que se pudo realizar un CRD (CREATE, READ, DELETE) pero no un CRUD (Create, Read, Update, Delete) completo, pues la idea es que el usuario no cambie datos que existen en su documento de identidad, los cuales debió verificar al comienzo de su registro.

La implementación de un módulo nuevo en una aplicación ya creada ayudó a entender las cosas que se debían tener en cuenta a nivel de compatibilidades y las complejidades de interpretar la codificación ajena, pues se debe comprender qué es lo que hace por dentro la aplicación. También se adquirieron conocimientos para conectar bases de datos en la nube y usar los diferentes servicios que se ofrecen para la creación de aplicaciones móviles.

Para esta versión del módulo de registro no fue posible añadir las políticas para el tratamiento de datos personales pues no se tiene los suficientes conocimientos legales y desde el proyecto de investigación se solicitará ayuda jurídica para poder diseñar las políticas y así poder notificarle con exactitud a todo tipo de usuario, el correcto tratamiento que tendrán sus datos personales al guardarlos en la nube.

Lo anteriormente dicho, además de lo evidenciado en el capítulo 5, deja en claro que los objetivos propuestos desde el inicio del proyecto fueron cumplidos con éxito.

Se recomienda como trabajo a futuro, evaluar las compatibilidades entre las versiones de Android para evitar inconvenientes al cambiar el nombre de los dispositivos, tal como se evidenció en el módulo de Bluetooth.

REFERENCIAS BIBLIOGRÁFICAS

Balaguera, Y. (2015). *Metodologías ágiles en el desarrollo de aplicaciones para dispositivos móviles*. Estado actual. *Revista de Tecnología*, *12*(2). https://doi.org/10.18270/rt.v12i2.1291

https://ayudaleyprotecciondatos.es/2018/09/10/suplantacion-identidad/

Alcaldía mayor de Bogotá. (28 de enero de 1982). *Ley 23 de 1982.* Recuperado el 22 de Abril del 2020, de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431

Ayudaley (s.f.). *Suplantación de identidad: todo lo que debes saber y nadie te ha contado*. Recuperado el 11 de Mayo de 2020, de https://ayudaleyprotecciondatos.es/2018/09/10/suplantacion-identidad/

Auronix. (4 de febrero de 2020). *Todo lo que necesitas saber sobre utilizar SMS en tu empresa*. Recuperado el 8 de Mayo del 2020, de https://www.auronix.mx/blog/beneficios-del-sms-en-la-comunicacion-empresa-cliente

Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (2013). *Mobile Ad Hoc Networking: Cutting Edge Directions: Second Edition* (2nd ed.). John Wiley & Sons, Inc. https://doi.org/10.1002/9781118511305

Castañeda, C. (2019). *Aplicación móvil para la comunicación de sobrevivientes de un desastre*. Universidad Antonio Nariño.

Cognex. (s.f). *Códigos de barras PDF417 - Simbología en códigos de barras* | Recuperado el 26 de Abril del 2020, de https://www.cognex.com/es-co/resources/symbologies/stacked-linear-barcodes/pdf417-bar-codes

Cloudflare. (s.f). *¿Qué es un bot?*. Recuperado el 28 de Julio del 2021, de https://www.cloudflare.com/es-es/learning/bots/what-is-a-bot/

CSIRT-CV. (s.f). *Seguridad en aplicaciones móviles.* Recuperado el 16 de Mayo del 2020, de https://www.csirtcv.gva.es/es/paginas/seguridad-en-aplicaciones-móviles.html

Dirección nacional de derecho de autor (s.f.). *Decisión Andina*. Recuperado el 22 de Abril del 2020, de http://derechodeautor.gov.co/decision-andina

Espacios Comunes. (s.f). *Registro y autenticación.* Recuperado el 18 de Mayo del 2020, de https://www.commonspaces.eu/en/help/register/

Función Pública. (2012). *Ley 1581 de 2012 - EVA.* Recuperado el 22 de April 22 del 2020, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Grupo Ático34. (s.f). *Suplantación de identidad - Qué es, Tipos, Consecuencias, Delito...* Recuperado el 8 de Mayo del 2020, de https://protecciondatos-lopd.com/empresas/suplantacion-de-identidad/

IBM (s.f). *Identificación y autenticación*. Recuperado el 16 de Mayo del 2020, de https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009740_.html

IONOS. (s.f). *El modelo en cascada en el desarrollo de software* - Recuperado el 17 de Abril del 2020, de https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/el-modelo-en-cascada/

Gomez, J., Hernandez, D. (s.f.). *Mobile D (programacion dispositivos moviles)*. Recuperado el 11 de del 2020, de https://es.slideshare.net/pipehernandez1020/mobile-d-programacion-

dispositivos-moviles

Ministerio de Relaciones Extreriores, M. de C. (s.f). *CÉDULA DE EXTRANJERÍA*. Recuperado el 18 de Mayo del 2020, de https://www.supernotariado.gov.co/portalsnr/images/archivosupernotariado/normatividad2013/circulares/circular692de2013/circular692de2013anexo.pdf

MDirector.com. (s.f). *Verificación de usuarios a través de SMS, cómo funciona*. Recuperado el 16 de Mayo del 2020, de https://www.mdirector.com/sms-marketing/verificacion-de-usuarios-a-traves-de-sms.html

RedIRIS (s.f). *Autenticación de usuarios*. Recuperado el 11 de Mayo del 2020, de https://www.rediris.es/cert/doc/unixsec/node14.html

Registraduría Nacional del Estado Civil. (s.f). *Cédula de Ciudadanía* -. Recuperado el 18 de Mayo del 2020, de https://www.registraduria.gov.co/-Cedula-de-Ciudadania,3689-.html

Registraduría Nacional del Estado Civil. (s.f). *Tarjeta de Identidad*. Recuperado el 18 de Mayo del 2020, de https://www.registraduria.gov.co/-Tarjeta-de-Identidad,3688-.html

Sgoliver (9 de Junio del 2011). *Notificaciones en Android (I): Toast*. Recuperado el 28 de Julio del 2021, de https://www.sgoliver.net/blog/notificaciones-en-android-i-toast/

VIU. (s.f). *¿Qué es la seguridad informática y cómo puede ayudarme?* Recuperado el 16 de Mayo del 2020, de https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

Verifíquese Cédula. (s.f). Recuperado el 19 de Abril del 2020, de https://www.verifique.se/

Zomwi (17 de septiembre del 2012). *Leer y generar códigos con Zxing*. Recuperado el 28 de Julio del 2021, de http://zomwi.blogspot.com/2012/09/zxing.html