



---

## Especificación de requisitos de software

Proyecto: PassKeeper

Rocket Team by RocketInnovate 2024

Tutor: Viviana Guillen



# Ficha del documento

Fecha	Revisión	Autor	Verificado dep. Calidad.
26/08/2023	0	Soledad Fornasier	Creación del documento. Se perfilan los aspectos generales del proyecto.
28/08/2023	1	Adrian Camus Leonel Casi Joana Martinez	Se profundiza en la conceptualización del proyecto.
05/09/2023	2	Ariel Mícoli Adrian Camus Valeriya Lysikova Lautaro Palacio Marcos Barey Soledad Fornasier	Revisión de aspectos conceptuales referentes a los alcances que la aplicación tendrá. Determinación de contenido de los sprints. Diseño historias de usuarios.
02/10/2023	3	Soledad Fornasier Valeriya Lysikova	Actualización de la documentación correspondiente a los avances del sprint.
28/10/2023	4	Soledad Fornasier Marcos Barey	Actualización de la documentación correspondiente a los avances del sprint.
31/10/2023	5	Joana Martinez Marcos Barey Lautaro Palacio	Se realizaron correcciones.
20/04/2024	6	Ariel Mícoli Adrian Camus Valeriya Lysikova Marcos Barey Soledad Fornasier Nahuel Pardo Mateo Lopez Catriel Parde	Se realiza una actualización con cambios de diseño y nueva funcionalidad para diferenciar usuarios premium de freemium. Además, se vinculó la app con la nueva página web.



# Índice General

Ficha del documento	2
1 Introducción	4
1.1 Propósito	4
1.2 Alcance	4
1.3 Personal involucrado	6
1.4 Definiciones, acrónimos y abreviaturas	7
1.5 Referencias	8
2 Descripción general	8
2.1 Perspectiva del producto	8
2.2 Características de los usuarios	8
2.3 Restricciones	8
2.4 Terminología clave	8
3 Requisitos específicos	9
Product Backlog	9
Sprints	13
Anexo I: Navegabilidad de la aplicación	16
Anexo II: Diseño de interfaz	26
Bibliografía consultada	27
Resumen	27



# 1 Introducción

Este documento describe los requisitos funcionales y no funcionales para una aplicación móvil de administración de contraseñas. La aplicación debe ser fácil de usar, y debe ofrecer características que permitan a los usuarios almacenar y gestionar sus contraseñas de forma segura. Esta especificación se ha estructurado basándose en las directrices dadas por el estándar IEEE, Práctica Recomendada para Especificaciones de Requisitos Software ANSI/IEEE 830, 1998.

## 1.1 Propósito

El presente documento tiene como propósito definir las especificaciones funcionales para el desarrollo de un aplicativo móvil, el cual permitirá la generación, organización y almacenamiento de contraseñas. En términos generales, dicho sistema será una herramienta esencial en la implementación de contraseñas seguras conforme a las recomendaciones en materia de ciberseguridad.

## 1.2 Alcance

La aplicación móvil que desarrollaremos está pensada para gestionar de manera activa y efectiva los nombres de usuarios y contraseñas de los numerosos servicios digitales.

Entendemos que el creciente avance de la tecnología ha impactado en la sociedad de manera profunda, a tal punto que la generación de usuarios digitales con sus correspondientes contraseñas se ha vuelto imperativo no solo para servicios de entretenimiento (facebook, twitter, etc), sino también para la gestión de trámites institucionales, cursado de estudios de nivel terciario, universitario, pago de servicios y/ impuestos, etc.

El corolario de ello es la ingente cantidad de nombres de usuarios y contraseñas que una persona debe organizar.

A esta problemática debe sumarse el creciente número de ataques consumados por ciberdelincuentes.



La app que desarrollaremos está pensada para poder gestionar las contraseñas de una manera segura, la cual hemos llamado "PassKeeper". Su funcionamiento permitirá gestionar las contraseñas de todas tus redes, correos, apps, bancos, etc. y también generar una contraseña segura.

El cliente deberá generar su usuario e ingresar sesión para poder acceder al menú donde va a poder seleccionar entre varias opciones ya sea para cargar una contraseña o poder generar una contraseña segura.

El cliente al seleccionar la opción de contraseñas podrá visualizar una lista con la urls de las contraseñas guardadas donde podrá ver la contraseña de una determinada url, la fecha de última modificación y una descripción de la misma, también podrá guardar una nueva pulsando el icono correspondiente.

El cliente podrá también obtener una contraseña segura generada por la app.

La app también contará con seguridad biométrica (fingerprint) para poder acceder a la aplicación.



## 1.3 Personal involucrado

Nombre	Fornasier María Soledad
Rol	Scrum Master
Categoría Profesional	Estudiante
Responsabilidad	Llevar adelante el proyecto integrador
Información de contacto	<a href="mailto:soleforna@hotmail.com.ar">soleforna@hotmail.com.ar</a>

Nombre	Mícoli Ariel R.
Rol	Desarrollador
Categoría Profesional	Estudiante
Responsabilidad	Desarrollador de proyecto
Información de contacto	<a href="mailto:micoliarriel@gmail.com">micoliarriel@gmail.com</a>

Nombre	Adrian Edgardo Camus
Rol	Desarrollador
Categoría Profesional	Estudiante
Responsabilidad	Entregar el proyecto
Información de contacto	<a href="mailto:adrianedgardocamus@gmail.com">adrianedgardocamus@gmail.com</a>

Nombre	Marcos Barey
Rol	Desarrollador
Categoría Profesional	Estudiante
Responsabilidad	Entregar el proyecto
Información de contacto	<a href="mailto:caposelmarco@gmail.com">caposelmarco@gmail.com</a>

Nombre	Joana Gisela Martinez
Rol	Desarrollador
Categoría Profesional	Estudiante
Responsabilidad	Entregar el proyecto
Información de contacto	<a href="mailto:joanamartinez44@gmail.com">joanamartinez44@gmail.com</a>

Nombre	Valeriya Lysikova
Rol	Desarrollador
Categoría Profesional	Estudiante
Responsabilidad	Entregar el proyecto
Información de contacto	<a href="mailto:v.lysikova@gmail.com">v.lysikova@gmail.com</a>

Nombre	Nahuel Cruz Pardo Lesa
Rol	Desarrollador
Categoría Profesional	Estudiante
Responsabilidad	Entregar el proyecto
Información de contacto	<a href="mailto:nahuel.pardo74@gmail.com">nahuel.pardo74@gmail.com</a>

Nombre	Catriel Ignacio Pardo Lesa
Rol	Desarrollador
Categoría Profesional	Estudiante
Responsabilidad	Entregar el proyecto
Información de contacto	<a href="mailto:cartup90@gmail.com">cartup90@gmail.com</a>

Nombre	Mateo Joel Lopez
Rol	Desarrollador
Categoría Profesional	Estudiante
Responsabilidad	Entregar el proyecto
Información de contacto	<a href="mailto:thefilesystem1024@hotmail.com">thefilesystem1024@hotmail.com</a>



## 1.4 Definiciones, acrónimos y abreviaturas

Nombre	Descripción
Usuario	Toda persona que se registra como usuario y utiliza la aplicación

## 1.5 Referencias

Título del Documento	Referencia
Standard IEEE 830 - 1998	IEEE

# 2 Descripción general

## 2.1 Perspectiva del producto

El sistema PassKeeper es una herramienta orientada a la creación, almacenamiento y gestión de contraseñas seguras.

La aplicación proporcionará una interfaz intuitiva y amigable que le permitirá a los usuarios almacenar, organizar y acceder a sus credenciales de inicio de sesión de manera conveniente.

Esta herramienta permitirá poner en práctica con facilidad las principales recomendaciones en materia de ciberseguridad, tales como mantener contraseñas únicas para cada servicio, longitud y aleatoriedad en su conformación, modificaciones periódicas, etc.

Además, estará pensado para ofrecer una excelente experiencia de usuario, dado que su interfaz será amigable y sencilla, teniendo a su vez características de diseño y sofisticación orientada a los dispositivos móviles.

## 2.2 Características de los usuarios

Los usuarios de una aplicación de administración de contraseñas son personas que desean proteger sus contraseñas de forma segura. Estos usuarios pueden incluir:



- Personas que utilizan varias cuentas en línea: Estos usuarios pueden tener cuentas en redes sociales, sitios web de comercio electrónico, bancos, servicios de correo electrónico, etc. Es importante que estos usuarios utilicen contraseñas únicas y seguras para cada cuenta, pero esto puede ser difícil de recordar. Una aplicación de administración de contraseñas puede ayudar a estos usuarios a almacenar y gestionar sus contraseñas de forma segura.
- Personas que se preocupan por su seguridad en línea: Estas personas pueden ser conscientes del riesgo de ataques cibernéticos y quieren tomar medidas para proteger su privacidad y seguridad. Una aplicación de administración de contraseñas puede ayudar a estas personas a reforzar su seguridad en línea.
- Personas que no tienen tiempo o paciencia para gestionar sus contraseñas: Estas personas pueden encontrar que es difícil recordar y administrar contraseñas únicas y seguras. Una aplicación de administración de contraseñas puede ayudar a estas personas a automatizar este proceso.

## 2.3 Restricciones

- Lenguajes de programación: Java
- Entorno de desarrollo: Android Studio
- Base de datos: SQLite

## 2.4 Terminología clave

A efectos de entender el funcionamiento de la aplicación se aclaran los siguientes términos:

- Contraseña Maestra: es la serie de caracteres que se debe generar para poder ingresar por primera vez a la aplicación, y que se debe determinar simultáneamente con su correo electrónico. Resulta indispensable para poder acceder a la gestión de las contraseñas correspondientes a distintos servicios.
- Contraseña: es el registro completo con todos los datos de un servicio determinado.





Cada "contraseña" está integrada con los siguientes datos: nombre o denominación que utilizamos para registrar el servicio en la aplicación (por ejemplo "Banco Nación", "cuenta de lichess", etc); el usuario del servicio que se guarda (por ejemplo el nombre de usuario de facebook, o de instagram, etc); la contraseña concreta o "keyword" del servicio (la que se usa o utilizará en facebook, instagram, etc); la url del sitio donde se encuentra el servicio ([www.facebook.com](http://www.facebook.com)); la descripción que nos ayude a recordar el servicio que depositamos.

- **Keyword:** es la contraseña concreta de cada servicio. Si uno guarda un registro con los datos de su cuenta de facebook, por ejemplo, la contraseña concreta de facebook sería la keyword.

## 3 Requisitos específicos

### Product Backlog

- #US01:  
Como **usuario** quiero poder crear una cuenta y registrarme en el aplicativo para guardar mis contraseñas.  
  
#TK01: Crear sección de inicio de sesión  
  
#TK02: Crear formulario de registro
- #US02:  
Como **usuario** quiero poder generar una contraseña aleatoria segura para no tener que estar pensando nuevas contraseñas.  
  
#TK01: Implementar un botón de generar contraseña aleatoria.
- #US03:  
Como **usuario** registrado, quiero poder gestionar mis contraseñas de manera sencilla y amigable para garantizar la seguridad de mis cuentas en línea sin sentirme abrumado por la tecnología.  
  
#TK1: Implementar acceso a un menú de contraseñas guardadas.  
  
#TK2: Implementar las funcionalidades de visualización de la gestión de contraseñas.
- #US04:  
Como **cliente** busco una aplicación que sea fácil de usar y que me guíe a través del proceso para agregar contraseñas de manera sencilla.
  - #TK01: Facilitar el proceso de actualización de contraseñas con un solo clic.
- #US05:



Como usuario quiero apretar un botón y copiar la contraseña, para poder tenerla copiada en memoria y poder utilizarla donde lo necesite

#TK01: implementar una acción que copie el contenido descriptado de la contraseña.

- #US06:

Como usuario quiero poder buscar una contraseña para tener facil acceso a la misma.

#TK01: implementar una acción que me permita filtrar las contraseñas por su nombre.

- #US07:

Como usuario quiero poder editar una contraseña para poder corregir o cambiar valores.

#TK01: Facilitar el proceso de actualización de contraseñas con un solo clic.

- #US08:

Como usuario quiero poder borrar una contraseña que ya no uso para que no me aparezca a en el listado de contraseñas

- #TK01: Facilitar el proceso de actualización de contraseñas con un solo clic.

- #US09:

Como usuario quiero poder visualizar la última fecha de modificación de una contraseña para tener un seguimiento.

- #TK01: Implementar una acción que me permita visualizar la fecha de última modificación.

- #US10:

Como usuario quiero poder acceder a mi cuenta de manera segura para evitar que mi cuenta se vea comprometida

- #TK01: Implementar seguridad biométrica (fingerprint) para poder acceder a la aplicación.

- #US11: (nueva issue para la versión 2.0)

Implementar una conexión a un API REST en línea para consultar si el usuario es premium

- #TK01: Implementar una conexión a un API REST en línea para consultar si el usuario es premium.
- #TK03: Si el usuario no es premium ofrecer la compra de la versión mediante un link a la página web

- #US12: (nueva issue para la versión 2.0)

Como usuario de PassKeeper, quiero ver una estética mejorada en la nueva versión, para disfrutar de una experiencia visual más atractiva y moderna.



- **#TK01:** Realizar una mejora en la visualización de cada una de las pantallas de la mobile app
- **#US13:** **(nueva issue para la versión 2.0)**  
Como usuario de PassKeeper, quiero ver una estética mejorada en la nueva versión, para disfrutar de una experiencia visual más atractiva y moderna.
  - **#TK01:** Realizar una mejora en la visualización de cada una de las pantallas de la mobile app
  - 
  - **#TK02:** Agregar ícono que se haga visible solo para aquellos usuarios premium
- **#US14:** **(nueva issue para la versión 2.0)**  
Limitación de Almacenamiento de Contraseñas para Usuarios Freemium y Premium
  - **#TK01:** Los usuarios con suscripción freemium deben estar limitados a almacenar un máximo de 10 contraseñas.
  - **#TK02:** Los usuarios con suscripción premium deben poder almacenar un número ilimitado de contraseñas.

## Requerimientos Funcionales

Requerimiento	Descripción
Registro de usuario	Cada vez que se cree una nueva cuenta con los datos de cada usuario se deberá almacenar en la base de datos.
Iniciar sesión	<p>El usuario podrá ingresar al Sistema luego de proporcionar su usuario y contraseña.</p> <p><b>Versión 2.0:</b> Se validará si el usuario es premium y en caso de que no sea así, se mostrará una opción que redireccionará a la nueva web de Passkeeper desde donde podrá realizar el pago.</p>
Agregar una contraseña	<p>El sistema deberá permitir el registro de contraseñas en el sistema.</p> <p><b>Versión 2.0:</b> Se validará la cantidad de contraseña para el caso de que</p>



	el usuario no sea premium, limitando su almacenamiento a un número menor o igual a 10.
Modificar contraseña	Se podrá editar datos de contraseñas previamente guardados.
Eliminar contraseña	El sistema podrá borrar una contraseña asociada a un usuario registrado previamente.
Buscar contraseña	El sistema será capaz de buscar entre los registros de contraseñas aplicando filtros de búsqueda.
Listar contraseñas	El sistema será capaz de visualizar el listado de contraseñas asociados a un usuario registrado en el sistema.
Acceso biométrico	El sistema será capaz de reconocer la huella dactilar de un usuario.
Sistema adaptable	El sistema debe tener la capacidad de adaptarse a diferentes dispositivos.
Consultar una API externa	<b>Versión 2.0:</b> La aplicación debe conectarse a una API y consultar el estado del usuario actual para diferenciar usuarios premium
Vincular a una página web	<b>Versión 2.0:</b> Desde el About us de la app se podrá acceder a la web de passkeeper y conocer más acerca del equipo de desarrollo
Preguntas frecuentes	<b>Versión 2.0:</b> Se ofrecerá la nueva ventana de preguntas frecuentes referentes a la app.

## Requerimientos no Funcionales

Requerimientos	Descripción
Navegabilidad	El Sistema deberá poseer una interfaz sencilla e intuitiva para el usuario.



Seguridad	El sistema deberá contar con una verificación de los datos para el correcto acceso a la aplicación.
Manejo de datos	El sistema deberá crear un respaldo en la base de datos para asegurar la protección e integridad de la información.
Integridad de los datos	El sistema deberá poseer una validación para el ingreso de datos que se encuentren dentro de la aplicación.
Alertas	El sistema deberá manejar mensajes de errores y confirmaciones.

## Sprints

Sprint Nro. 00	
Sprint Backlog	<p>Registrar la Especificación de Requerimientos mediante la documentación IEEE830</p> <p>Subir la Especificación de Requerimientos en una carpeta de GitHub en la rama main.</p> <p>Crear Project estilo Kanban con incorporación de Historias de Usuarios, tareas, e incidencias.</p> <p>Crear mapa del sitio</p> <p>Llevar registro de meetings y toda la información necesaria dentro de la Wiki de GitHub.</p>
Responsabilidades	Todo el grupo es responsable de participar en las diferentes issues y para tales fines se realiza una distribución de tareas adecuada conforme a las necesidades productivas del momento.
Calendario	<p><i>Fecha Inicio =</i></p> <p><i>Fecha de Fin = 05/09/2023</i></p>
Inconvenientes:	



Sprint Nro. 01	
Sprint Backlog	<p>Crear su propio DER y Modelo relacional para documentar las tablas en la DB.</p> <p>Crear un Diagrama de Clases y Casos de Uso para facilitar el modelado en POO.</p> <p>Script sql de la base de datos actualizada con las tablas nuevas.</p> <p>#US01: Como usuario quiero poder crear una cuenta y registrarme en el aplicativo para guardar mis contraseñas.</p> <p>#US02: Como usuario quiero poder generar una contraseña aleatoria segura para no tener que estar pensando nuevas contraseñas.</p> <p>#US03: Como usuario registrado, quiero poder gestionar mis contraseñas de manera sencilla y amigable para garantizar la seguridad de mis cuentas en línea sin sentirme abrumado por la tecnología.</p>
Responsabilidades	<p>Todo el grupo es responsable de participar en las diferentes issues y para tales fines se realiza una distribución de tareas adecuada conforme a las necesidades productivas del momento. Sin embargo</p>
Calendario	<p><i>Fecha Inicio = 05/09/2023</i> <i>Fecha de Fin = 01/10/2023</i></p>
Inconvenientes:	



Sprint Nro. 02	
Sprint Backlog	<p>#US04: Como cliente busco una aplicación que sea fácil de usar y que me guíe a través del proceso para agregar contraseñas de manera sencilla</p> <p>#US05: Como usuario quiero apretar un botón y copiar la contraseña, para poder tenerla copiada en memoria y poder utilizarla donde lo necesite</p> <p>#US06 Como usuario quiero poder buscar una contraseña para tener fácil acceso a la misma.</p> <p>#US07: Como usuario quiero poder editar una contraseña para poder corregir o cambiar valores.</p> <p>#US08: Como usuario quiero poder borrar una contraseña que ya no uso para que no me aparezca en el listado de contraseñas.</p> <p>Aplicar accesibilidad a la app movil.</p> <p>Video demo final.</p>
Responsabilidades	<p>Todo el grupo es responsable de participar en las diferentes issues planteadas en este sprint.</p>
Calendario	<p><i>Fecha Inicio = 01/10/2023</i> <i>Fecha de Fin = 29/10/2023</i></p>



Sprint Nro. 03	
Sprint Backlog	<ul style="list-style-type: none"><li>• <u>#TK02</u>: Implementar una conexión a un API REST en línea para consultar si el usuario es premium.</li><li>• <u>#TK02</u>: Si el usuario no es premium ofrecer la compra de la versión mediante un link a la página web</li></ul>
Responsabilidades	Todo el grupo es responsable de participar en las diferentes issues planteadas en este sprint.
Calendario	<i>Fecha Inicio = 12/05/2024</i> <i>Fecha de Fin = 03/06/2024</i>





## Anexo I

Navegabilidad de la aplicación.

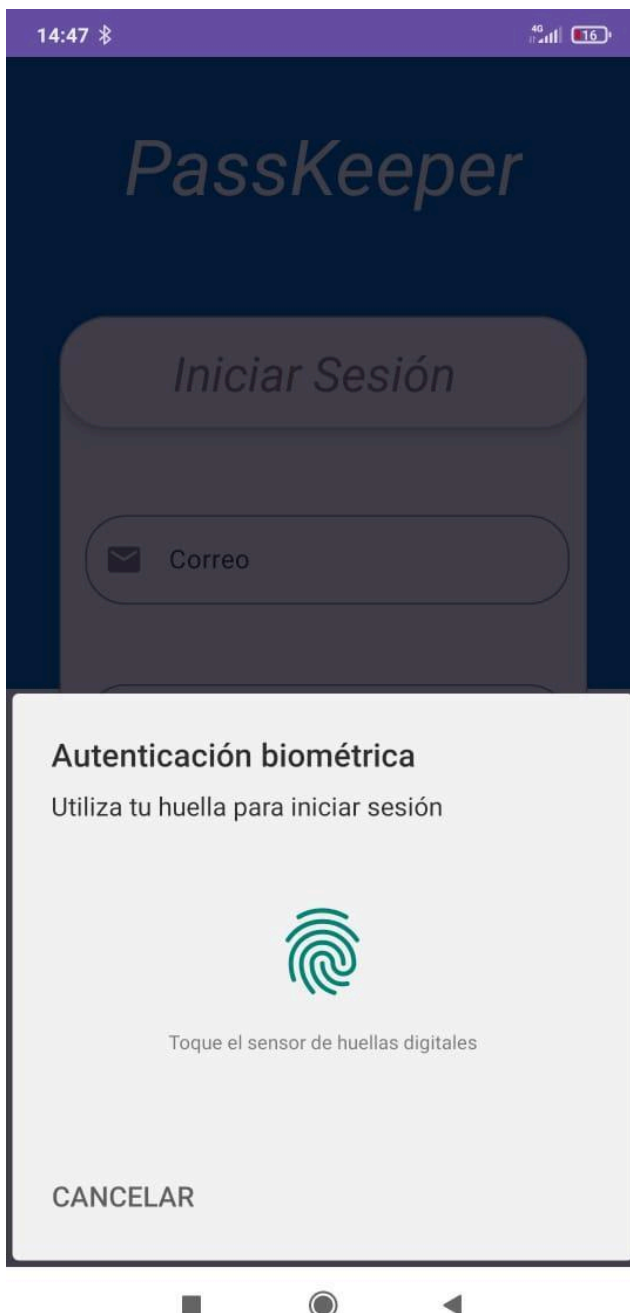
- Pantalla de inicio.



Esta es la primer pantalla con la que el usuario se encontrará en el caso de que su dispositivo móvil no cuente con la capacidad de trabajar con datos biométricos. En esta pantalla el usuario iniciará sesión si ya tuviera una cuenta creada. Caso contrario deberá ingresar en el link "No estás registrado?"



- Pantalla de inicio II.



Si su dispositivo celular cuenta con los datos biométricos habilitados, esta será la primer pantalla que verá.



- Pantalla de Registro.

A screenshot of a mobile application's registration screen. The screen has a blue header with the 'PassKeeper' logo. Below the header is a white rounded rectangle containing the registration form. At the top of this rectangle is a back arrow and the title 'Registrarse'. The form has three input fields: 'Correo' with an envelope icon, 'Contraseña' with a lock icon and a toggle for visibility, and 'Repetir Contraseña' with a lock icon and a toggle for visibility. Below the fields is a link that says 'Ya tiene una cuenta?'. At the bottom of the form is a blue button labeled 'REGISTRARSE'. The entire screen is framed by a black bar at the bottom with standard Android navigation icons.

En esta pantalla el usuario creará su cuenta, la cual le permitirá ingresar a las herramientas de gestión de contraseñas.

En este caso el usuario está generando su Contraseña Maestra.

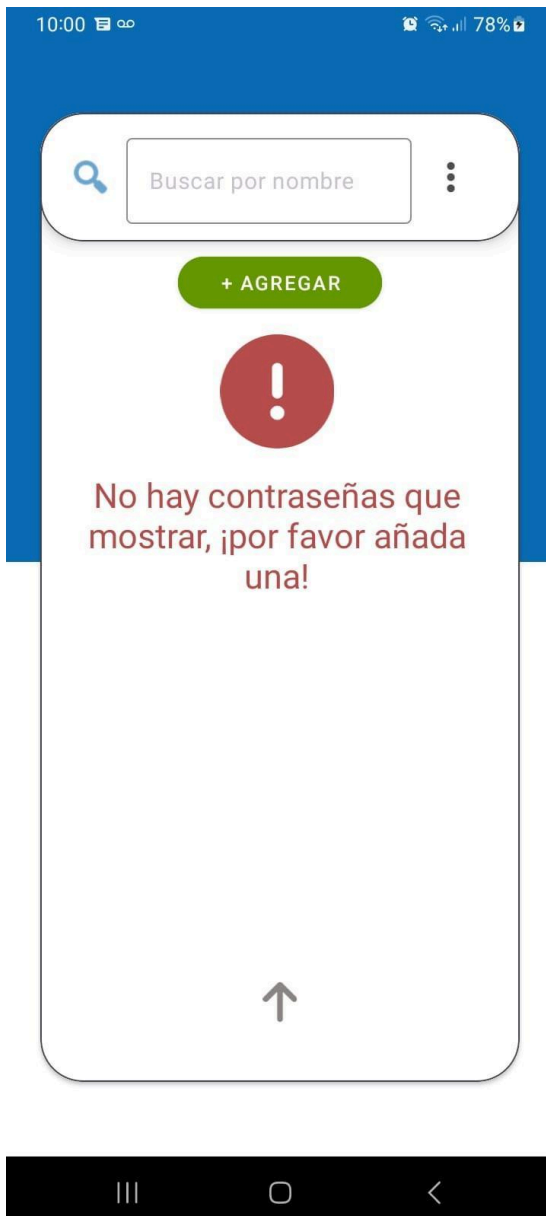


-Una vez creada su cuenta, el usuario ingresa al sistema.

A mobile app login screen for 'PassKeeper'. The screen has a blue header with the app name 'PassKeeper' in white. Below the header is a white rounded rectangle containing the login form. At the top of this rectangle is the title 'Iniciar Sesión'. Below it are two input fields: 'Correo' with an email icon and the text 'test@gmail.com', and 'Contraseña' with a lock icon, a series of dots, and an eye icon to toggle visibility. Below the password field is a link that says 'No estas registrado?'. At the bottom of the white rectangle is a blue button with the text 'INICIAR SESIÓN'. The entire screen is framed by a purple status bar at the top showing '14:43', signal strength, and '66%' battery. At the very bottom is a black Android navigation bar with three icons: a square, a circle, and a triangle.



-Pantalla de visualización de contraseñas.



En esta pantalla se visualizarán las contraseñas (registro de los datos) que el usuario ya tenga depositadas.

Se ha implementado una función de filtrado de contraseñas en la parte superior de la pantalla.

Si aún no se cuenta con ninguna contraseña, se deberá ingresar al botón "+ Agregar".

-Pantalla de Nueva Contraseña.

The screenshot shows a mobile app interface with a blue header and a white content area. At the top, there's a back arrow icon and the title 'Nueva Contraseña'. Below this, there are five input fields, each with a label and an icon: 'Nombre' (globe icon) with the value 'Banco', 'Usuario' (envelope icon) with the value 'test\_usuario', 'Contraseña' (lock icon) with the value 'F-a)faE3Z>#e' and a green plus icon to its right, 'URL' (link icon) with the value 'www.banco.com', and 'Descripción' (pencil icon) with the value 'banco plazo fijo en dólares'. At the bottom of the form is a blue button labeled 'GUARDAR'. The status bar at the top shows the time 10:03, signal strength, and 79% battery.

En esta pantalla se podrá agregar una contraseña, es decir un registro de datos correspondiente a un servicio concreto.

El icono verde representado por un símbolo "+" que se está ubicado a la derecha en el input correspondiente a la keyword, cuenta con un algoritmo capaz de generar de manera aleatoria una cadena de caracteres. Esta cadena podrá ser utilizada por el usuario como su keyword.



-Pantalla de visualización de todas contraseñas generadas.



Luego de haber agregado una nueva contraseña, ahora el usuario podrá visualizar, modificar o eliminar la contraseña ya generada. Para ello emplea los tres iconos respectivos.



-Pantalla Ver Contraseña.

The screenshot shows a mobile application interface with a blue header and a white content area. At the top, there's a back arrow icon and the title 'Ver Contraseña'. Below this, there are five input fields, each with a label and an icon: 'Sitio Web' (globe icon) with the value 'Banco', 'Usuario' (envelope icon) with 'test\_usuario', 'Contraseña' (lock icon) with 'F-a)faE3Z>#e', 'URL' (chain link icon) with 'www.banco.com', and 'Descripción' (pencil icon) with 'banco plazo fijo en dólares'. To the right of the password field, there are two icons: a crossed-out eye and a copy icon. At the bottom, there's a black navigation bar with three white icons: a hamburger menu, a circle, and a back arrow.

Esta pantalla permite visualizar la contraseña que hemos generado y además nos da la posibilidad de copiar la keyword, para lo cual se implementó el icono que se encuentra ubicado a la derecha del input correspondiente a la keyword.





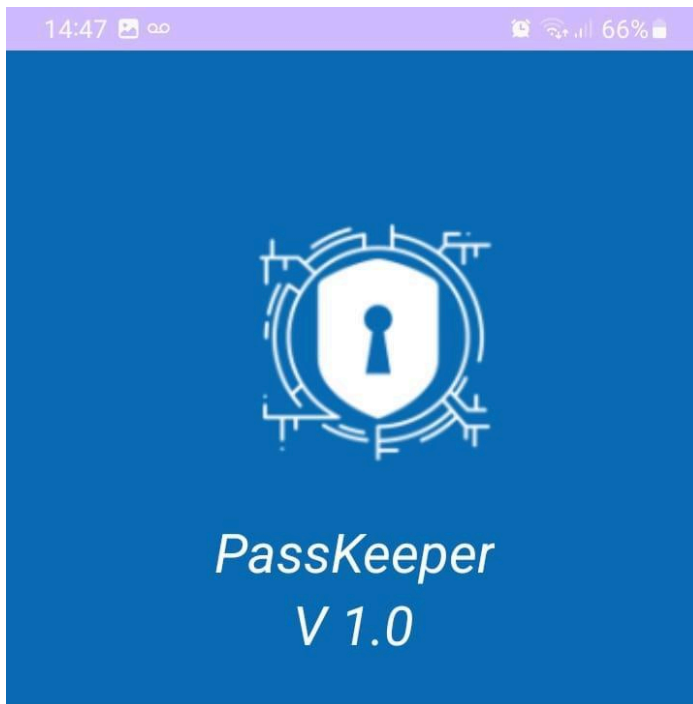
-Pantalla de edición de contraseña.

En esta pantalla podemos modificar cualquier dato que queramos respecto a la contraseña guardada.

The screenshot shows a mobile application interface for editing a password entry. At the top, there's a blue header bar with a white back arrow icon and the text 'Editar Contraseña'. Below this, there are five input fields, each with a label and an icon: 'Nombre' (globe icon) with the value 'Banco', 'Usuario' (envelope icon) with the value 'test\_usuario', 'Contraseña' (lock icon) with the value 'F-a)faE3Z>#e' and a toggle icon, 'URL' (link icon) with the value 'www.banco.com', and 'Descripción' (pencil icon) with the value 'banco plazo fijo en dólares'. At the bottom of the form is a large blue button labeled 'GUARDAR'. The status bar at the top shows the time 10:11, battery level 80%, and various connectivity icons. The bottom of the screen shows the standard Android navigation bar with three icons: a square, a circle, and a triangle.



-Finalmente se cuenta con una pantalla informativa con el nombre del equipo de trabajo.



### *Un desarrollo de Rocket Team*

*Adrián E. Camus      Marcos Barey*

*Valeriya Lyskova      Ariel R. Micoli*

*Joana G. Martinez      Lautaro Palacios*

*M. Soledad Fornasier      Leonel Casi*

VOLVER





## AnexoII

Diseño de Interfaz: [Prototipo en FIGMA](#)

[Video Accesibilidad](#)



# Bibliografía consultada.

- Página web oficial de Android Studio.  
Google. (2023, agosto). Desarrollar UI. [Página web]. Recuperado de <https://developer.android.com/develop/ui?hl=es-419>
- Página de referencia de SQLite en Android Studio  
Google. (2023, agosto). Referencia de SQLite. [Página web]. Recuperado de <https://developer.android.com/reference/android/database/sqlite/SQLiteDatabase>
- Libro: UML MODELADO DE SOFTWARE PARA PROFESIONALES: RECURSOS PARA PROFESIONALES DE SISTEMAS  
Fontela, C. (2023). UML MODELADO DE SOFTWARE PARA PROFESIONALES: RECURSOS PARA PROFESIONALES DE SISTEMAS. Madrid, España: Marcombo. ISBN: 9788426717955
- Canal de YouTube Innova Domotics. (2021, 23 de septiembre). Android Studio - Desde Cero - Java [Vídeo]. YouTube.  
<https://www.youtube.com/watch?v=QYgujl5kogs&t=1403s>

## Resumen.

Este documento consta de tres secciones. En la primera sección se realiza una breve introducción en donde se define el propósito para desarrollar la app mobile, cuya funcionalidad principal es la gestión y seguridad de las contraseñas de un determinado usuario, asimismo se establece cual va a ser el personal involucrado encargado de llevar a cabo las diferentes etapas del proyecto y los roles asignados.

En la segunda sección se realiza una descripción general de la aplicación, sus características y restricciones, sin hacer un detalle pormenorizado.

Finalmente, en la tercera y última sección se precisan los requerimientos funcionales pretendidos y los plazos estipulados para el desarrollo de la aplicación.

