



Experiencia de usuario.

PassBank



Profesor: Lucas Martin Rossi

Grupo 5

Gonzalo Guarnieri

Valentina Cuevas

Matias Martínez

Julieta Mendoza

Manuel Avendaño

Martina Duran

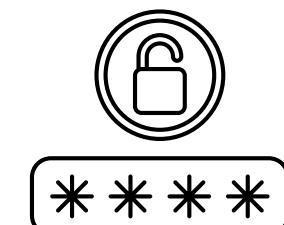


Introducción

Nuestro grupo ha optado por abordar una problemática relacionada tanto con la seguridad de los usuarios como con un problema cotidiano que a todos nos ha podido ocurrir.

Hoy en día nos sentimos **inseguros** con nuestras contraseñas, ya sea al guardarlas en nuestro navegador o al escribirlas en un papel. Además, cada vez somos **más vulnerables** a sufrir ataques por parte de personas que quieren acceder a nuestros datos personales. Por esta razón, utilizamos contraseñas más complejas, lo que nos hace más **propensos a olvidarlas**.

Hemos recopilado información sobre aplicaciones que han intentado resolver este problema en la era digital, junto con sus estadísticas y reseñas. Además, presentamos una nueva solución a esta problemática llamada Passbank.



Problemática



"Creemos que las personas tienen problemas al momento de **recordar** sus contraseñas y ponen en riesgo su **seguridad** además de su **confianza**"

Los usuarios necesitan unirse a plataformas digitales tales como redes sociales, instituciones de manera virtual o tiendas online, es necesario tener un email y una contraseña.

Así también, recordar contraseñas se hace una tarea fácil teniendo una sola cuenta de e-Mail, pero aquellos usuarios con múltiples correos conlleva a la creación de mas contraseñas.

Hoy en día las contraseñas necesitan de una buena combinación entre letras minúsculas, mayúsculas, numero y algún que otro símbolo, pero no todas las personas pueden manejar todas sus contraseñas, lo cual termina en 2 posibles resultados: que los usuarios terminen eligiendo por utilizar contraseñas fáciles, **poniendo en riesgo su seguridad**, o escribiéndolas en papel, corriendo el **riesgo de perderla**.

Esto conlleva a que la relación entre el usuario y su experiencia en sitios o servicios que requieran de una contraseña resulten en un deterioro y hasta en una relación amor-odio.



Objetivo



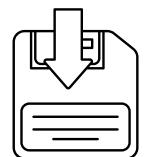
Lo que se busca es que los usuarios, independientemente si quieren optar por anotar o acordarse las contraseñas, **no pongan en riesgo la seguridad** de sus cuentas e información. Brindando una solución sencilla, intuitiva y segura, haciendo que sus datos no sean comprometidos y puedan seguir seguros en su entorno digital sin tener que **recuperar repetidamente** las contraseñas de sus correos.



Solución



Nuestra solución a esta problemática es crear una aplicación donde nuestro usuario pueda:



- Guardar sus contraseñas de sus respectivas cuentas de e-Mail (u otro servicio que requiera de ellas)



- Poder utilizar el tipo de autentificador que el deseé. (ya sea por biometría o por terceros como mensajes SMS)



- Sentirse seguros al poder ser los únicos que puedan acceder a su información personal.



Funcionalidades



- Utilizar datos biométricos.
- Actuar como una base de datos personal para las contraseñas y e-Mail del user.
- Poder desvincular la información de la aplicación en caso de robo.
- Tener diferentes maneras de acceso dependiendo de la necesidad de usuario.
- Tener un botón de seguridad para copiar la clave y devolver un mensaje de seguridad al momento de pegar la misma.
- Generador de claves inteligentes que sean tanto similares como seguras.

Notas Periodísticas



<https://www.20minutos.es/tecnologia/ciberseguridad/los-peligros-de-guardar-contraseñas-en-tu-navegador-o-usar-el-autocompletar-de-chrome-o-firefox-5011052/>



Los peligros de guardar contraseñas en tu navegador o usar el autocompletar de Chrome o Firefox

PABLO SEGARRA / NOTICIA / 07.06.2022 - 18:02H

¿Es seguro guardar las contraseñas en el navegador?

Para **Jesús F. Rodríguez-Aragón**, fundador de Iberbox, la comodidad muchas veces suele ir relacionada con la falta de seguridad. "Es un hecho que es muy cómodo tener guardadas las contraseñas en el navegador, pero eso implica tener una mayor conciencia de la falta de seguridad que supone y contrarrestar con mayores niveles de seguridad en nuestros dispositivos", aconseja.

Más crítico se muestra **Simon Marchand de Nuance**, compañía tecnológica de Inteligencia Artificial conversacional. En su opinión, "las contraseñas son herramientas arcaicas cuya eficiencia es cada vez más cuestionable; los PIN y las claves se venden en la dark web y se explotan para actividades fraudulentas", señala el responsable de Fraud Prevention.

¡Sigue!

Los rasgos biométricos, más seguros

Como alternativa, Marchand propone normalizar que los usuarios se acrediten con rasgos biométricos tales como la huella dactilar, el reconocimiento facial, etc. Es un sistema que “permite acreditarse al usuario de forma inmediata basándose en sus características únicas, eliminando la necesidad de recordar PINs, contraseñas y otras credenciales antiguas y propensas a ser explotadas por actores maliciosos”.

En la misma línea se expresa **Hervé Lambert de Panda Security**, quien apunta que “tus credenciales, si están guardadas en el navegador, están claramente en peligro”. El experto en ciberseguridad no los considera seguros frente a ataques de malware por diversos motivos, como “los retrasos en aplicar parches de seguridad cuando se encuentran vulnerabilidades de los sistemas de cifrado, almacenaje, comunicación...”, o simplemente porque “si alguien usurpa tu identidad y entra en tu navegador (da igual que sea del ordenador o el móvil), podría iniciar sesión en cualquiera de los servicios”, explica.

“Si no cuentas con una autenticación de doble factor como un gestor de contraseñas en otro dispositivo, si alguien se hace con tu móvil o tu ordenador te puede generar muchos problemas en sólo 3 minutos”, apunta Lambert.

“Si no cuentas con una autenticación de doble factor como un gestor de contraseñas en otro dispositivo, si alguien se hace con tu móvil o tu ordenador te puede generar muchos problemas en sólo 3 minutos”, apunta Lambert.

La unanimidad es total entre los expertos consultados. **Miguel Ángel Ordóñez, director de Ciberseguridad y Resiliencia de Kyndryl**, afirma que “muchos navegadores guardan esas claves en una lista de texto, y en algunos casos, ni si quiera cifrada”.

Consejos para escoger y almacenar contraseñas

Algunos de los expertos en ciberseguridad de España comparten sus métodos para elegir y guardar una contraseña.

En el caso de **Rodríguez-Aragón (Iberbox)**, “las contraseñas deben ser una palabra compleja, con un cierto tamaño, con números, mayúsculas, minúsculas, caracteres especiales, que no se pueda relacionar con nosotros (por ejemplo poniendo fechas de nacimiento, nombres, etc), que sea distinta para cada plataforma que utilizamos...” La premisa a seguir es que “cuanto mayor sea la complejidad de nuestra contraseña, mayor será la seguridad que tenemos”, explica el profesional.



Cada cuánto se olvidan las claves

La rapidez con la que una persona puede olvidar una nueva clave puede variar significativamente de un individuo a otro. Factores como la memoria a corto plazo de la persona, la frecuencia con la que utiliza la clave, su nivel de atención al crearla y otros aspectos relacionados con la memoria y la cognición pueden influir en el proceso.



Doctora Claudia Alves

"La velocidad a la que olvidamos nuevas claves es una cuestión multifacética. La memoria humana es selectiva y puede depender de la importancia percibida de la información. Los estudios indican que el olvido inicial puede ser rápido, especialmente si no se presta suficiente atención al crear la clave. Sin embargo, las estrategias de memorización, como el uso de mnemotecnia o la repetición, pueden mejorar la retención a largo plazo"



Doctira Olivia Wilson

"La teoría de la curva de olvido propuesta por Ebbinghaus ilustra cómo tendemos a olvidar rápidamente la información recién adquirida, y este principio puede ser aplicable a las claves. La relevancia de una clave y la frecuencia con la que la utilizamos desempeñan un rol fundamental en su retención. En el corto plazo, es común experimentar olvidos debido a la interferencia y la falta de consolidación de la información."

> Apps similares



Al momento de plantear el Problema pensamos en 3 aplicaciones similares o que reconocemos que cumplen una **función similar** a nuestra solución



Google Authenticator



1Password: Password Manager



KeePassDX



Google Authenticator



Pedro Jesús Quevedo Lora

⋮



★★★★★ 18 de julio de 2023

Excelente App, pero me gustaría que en vez de mostrar los codigos al iniciar solo lo muestre al piderselo a la cuenta deseada al pulsar, y que tenga un registro de cuando se abre en el cual no se pueda eliminar el historial para protegela de acceso no deseado.

Esta opinión le resultó útil a 1 persona

⋮



★★★★★ 24 de junio de 2023

Lograron actualizar y añadir una sincronización simultánea entre dispositivos, de tal manera que no es posible ya perder el acceso a los códigos 2FA, aun así queda remarcar que queda la encriptación de los mismos en la red.

Esta opinión les resultó útil a 6 personas



Agrega una capa adicional de seguridad a tus cuentas en línea mediante un **segundo paso de verificación** cuando accedes a tu cuenta.

Esto significa que, además de la contraseña, también deberás **ingresar un código** generado por la app del Google Authenticator en el teléfono.



Google Authenticator



kevin cadena

:



★★★ 24 de agosto de 2023

Es una buena opción en cuanto a authenticators pero deberían agregar seguridad al ingresar tanto con face id o sensor de huella para que terceros no puedan ingresar a la app, y mejoras de seguridad en la copia de seguridad

¿Te resultó útil?

Sí

No



Rodrigo Sarre

★★★ 16 de agosto de 2023

Funciona muy bien pero Falta poner un pin para que solo yo vea los contraseñas, si me roban el teléfono cualquiera puede entrar a todas mis cuentas. Sería ideal un bloqueo con huella digital



Sombra de la Mariposa

★★★ 7 de junio de 2023

Al fin se sincroniza en la nube pero le falta mejorar, no tiene la opción de ingresar con huella, cualquiera que abra la app tiene acceso a los códigos, y la interfaz necesita mejorar

Esta opinión les resultó útil a 4 personas



¡Sin embargo! puede resultar **confuso** para algunos usuarios en la configuración inicial y **no ofrece sincronización** entre dispositivos, lo que puede ser inconveniente.

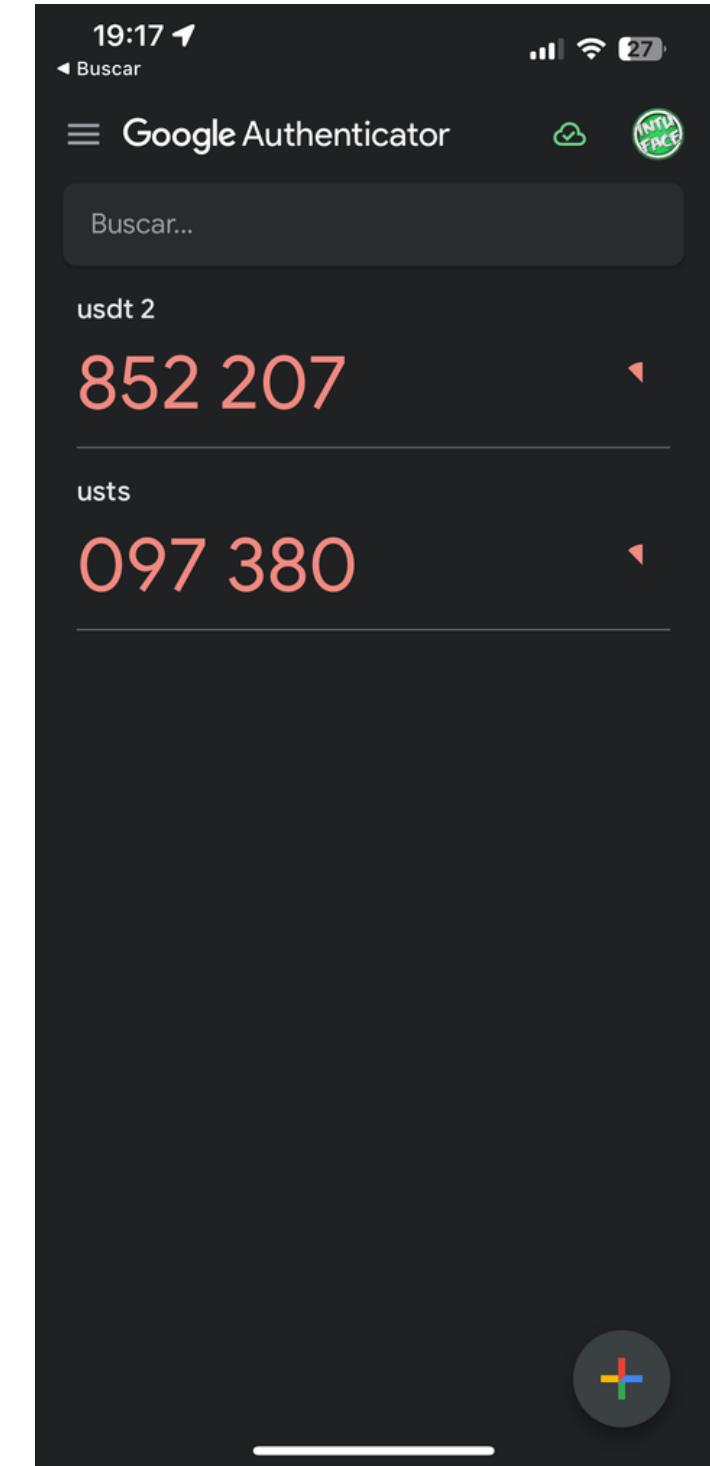
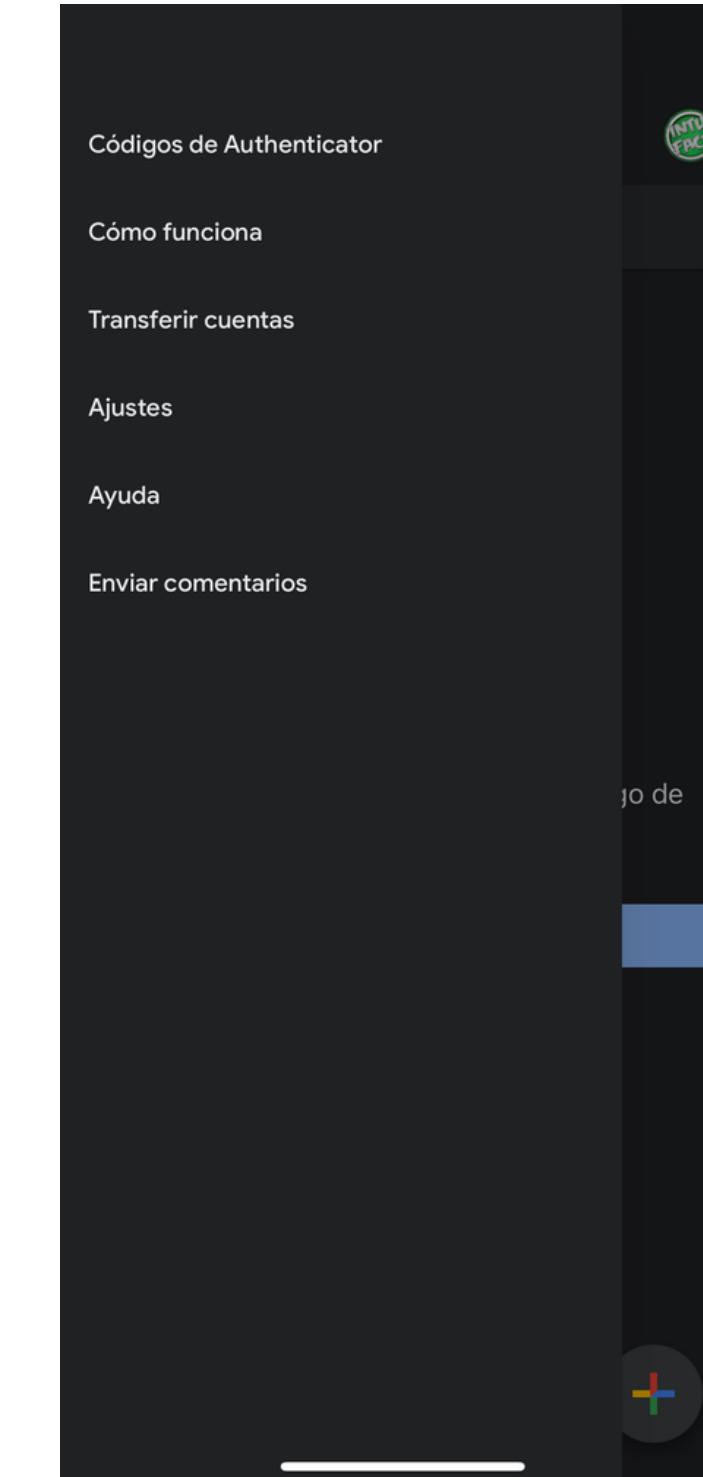
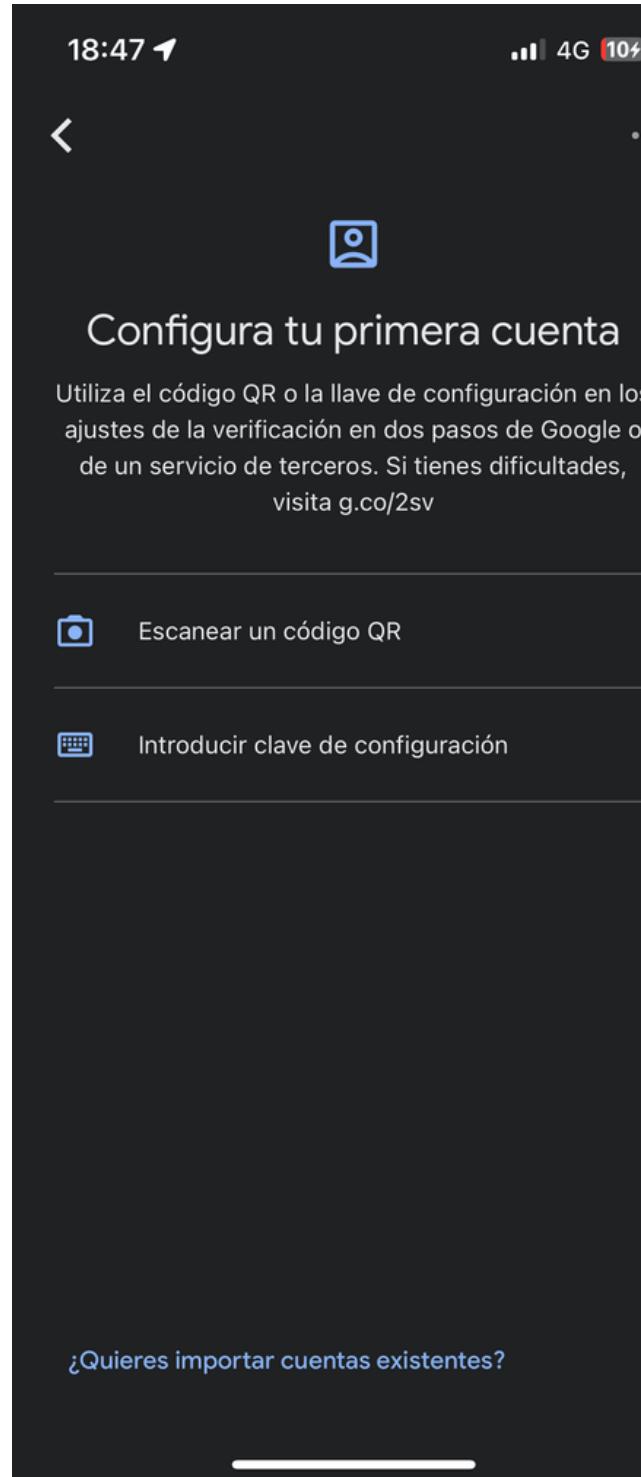
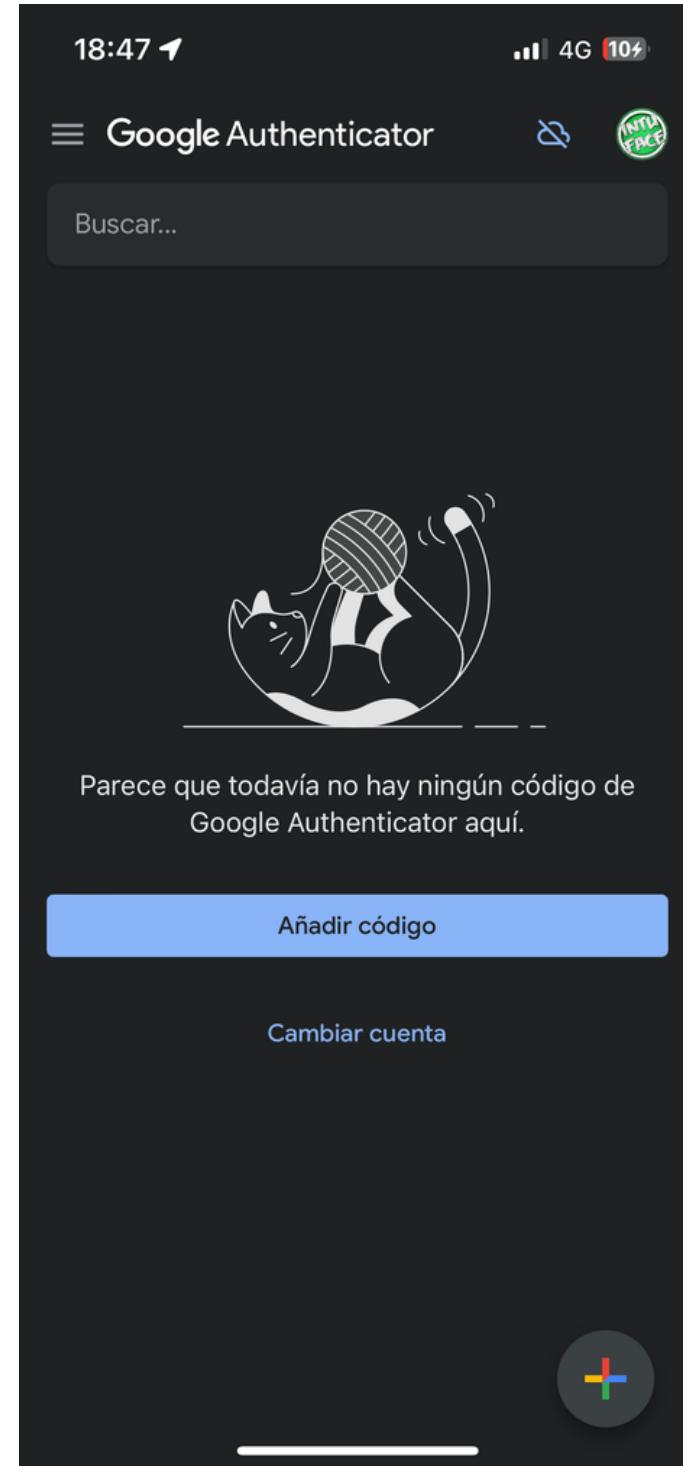
No ofrece una **opción de respaldo**, lo que significa que si pierdes tu dispositivo y no has anotado tus códigos de recuperación, podrías perder acceso a tus cuentas.



Google Authenticator



Capturas.





1Password: Password Manager



Emiliano Colombino



★★★★★ 18 de marzo de 2023

Excelente. Recuerdo que hace varios años la había probado y no me convenció. Esta vez si. Buen trabajo rediseñando todo. Principalmente me gusta por la seguridad (complejidad) de las contraseñas que sugiere. 5/5. Lo único que me equivoqué yo, tendría que haber comprado el plan familiar, para separar en dos cuentas lo personal y laboral.. pero mala mía. Nuevamente: Excelente!

Esta opinión les resultó útil a 6 personas

⋮



Pedro GP

⋮

★★★★★ 3 de octubre de 2022

Un servicio imprescindible, la atención al cliente excelente. Todo se hace más fácil con esta aplicación, se aumenta muchísimo la eficiencia ahorrándote rellenar las contraseñas, con el auto completado o teniéndola tan bien almacenadas de forma segura.

Esta opinión les resultó útil a 4 personas



Ofrece un almacenamiento seguro de contraseñas y datos confidenciales, generación de contraseñas seguras, **autenticación de dos factores (2FA)**, llenado automático, almacenamiento de documentos sensibles, **acceso en múltiples dispositivos**, seguridad avanzada y opciones para compartir contraseñas de manera segura. **Simplifica la gestión de contraseñas y garantiza la seguridad de tus datos en línea.**



1Password: Password Manager



MARIO JIMENEZ MARTINEZ

:

★ ★ ★ ★ 28 de agosto de 2022



Antes se abría una ventana pequeña cuando te sugería llenar una password... Ahora ocupa toda la pantalla. NO FUNCIONA EL AUTOCOMPLETADO. Soy usuario de pago. Si no corigen este problema me doy de baja. Viendo que no mejoraba he tenido que volver a la versión anterior. Se puede si lo buscas un poco. Con la última versión 7 vuelve a funcionar el AUTOCOMPLETADO. Lo siento, me quedo en la versión 7 hasta que no mejoren la experiencia de la versión 8.

Esta opinión les resultó útil a 14 personas



Antonio Cuadra

:



★★★★★ 23 de agosto de 2022

El autocompletado no funciona. Deberían dejar la app anterior hasta solucionar esto porque es grave

Esta opinión les resultó útil a 7 personas



¡Sin embargo! La amplia gama de características puede resultar **abrumadora** al principio para los nuevos usuarios.

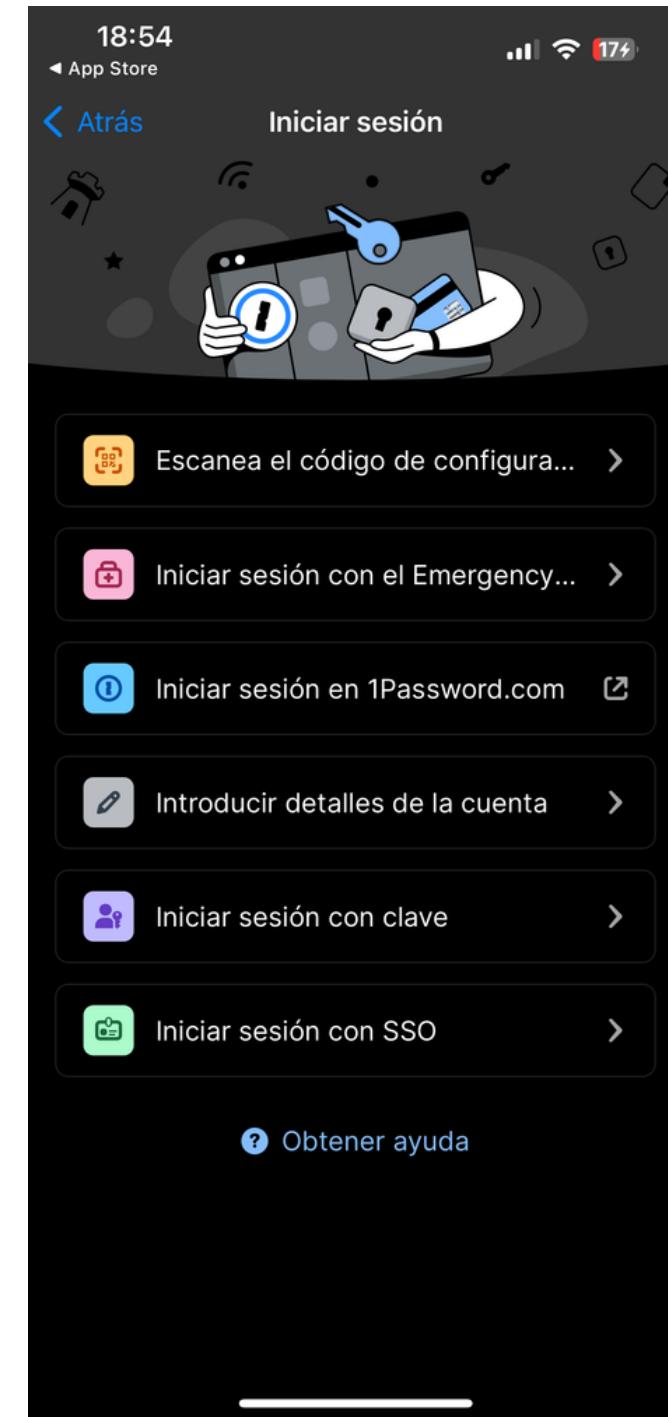
Para acceder a todas sus funcionalidades, es **necesario suscribirse** a la versión premium y, Además, algunos usuarios han informado que experimentan **problemas con la función de autocompletado**, lo que puede generar frustración y dificultades al acceder a sus cuentas en línea.



1Password: Password Manager



Capturas.





KeePassDX



Cristian Pacheco

⋮



★★★★★ 26 de mayo de 2023

Excelente app para guardar contraseñas, de las mejores que probé y hasta ahora nunca tuvo ningún fallo. La interfaz es poco intuitiva, pero no cuesta mucho tiempo familiarizarse



Miguel de Sande Moreno

⋮



★★★★★ 13 de octubre de 2021

La aplicación en sí es muy buena, me parece la mejor app para Android basada en KeePass, pero no hace más que generarme conflictos en Dropbox. Simplemente añado una contraseña o modifco algo y, sin tener la base de datos abierta en otro dispositivo, me genera otro archivo en conflicto con el original. Con otras apps no pasa. Por favor, arreglenlo. Muchas gracias. Edit: gracias por la respuesta, usaré otra nube alternativa a Dropbox. 5 estrellas entonces

Esta opinión les resultó útil a 10 personas



Es multifuncional y permite el almacenamiento y uso seguro de contraseñas, claves e identidades digitales. Se integra hábilmente con los estándares de diseño de Android, lo que facilita su uso y navegación en dispositivos móviles con este sistema operativo. Esto proporciona una experiencia de gestión de contraseñas eficiente y segura para los usuarios de Android.



KeePassDX



Juan GS

★★★ 4 de febrero de 2022

La app funciona bien, es excelente. Lamentablemente en una actualización se me borró la base de datos, no entiendo muy bien porque o como, pero les recomendaría tener más copias de la base de datos, esto para evitar cualquier inconveniente y perder todo, tal como me paso a mí.



MATR1X

★★★ 28 de octubre de 2021

No te permite copiar las contraseñas fácilmente con un click, debería permitir copiar la contraseña sin tener que entrar a dónde está guardada la contraseña como en Dashlane. No tiene una sección fácilmente accesible para generar contraseñas sin tener que añadir algo como en Dashlane. Además la configuración por defecto del generador de contraseñas no me convence, debería ser como en Dashlane. Si mejoran todo eso la app estaría mucho mejor



Esta opinión les resultó útil a 2 personas

i ¡Sin embargo! algunos usuarios han reportado que su **interfaz** puede resultar algo **menos intuitiva** y amigable en comparación con otras aplicaciones de gestión de contraseñas.

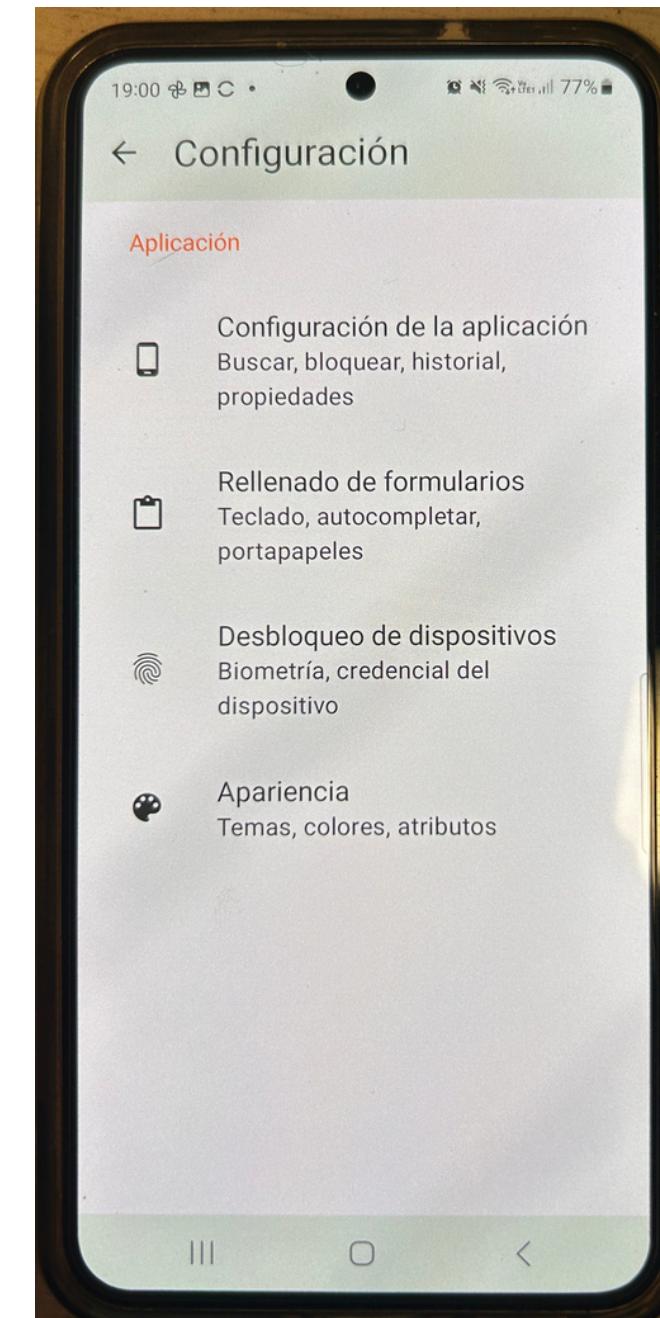
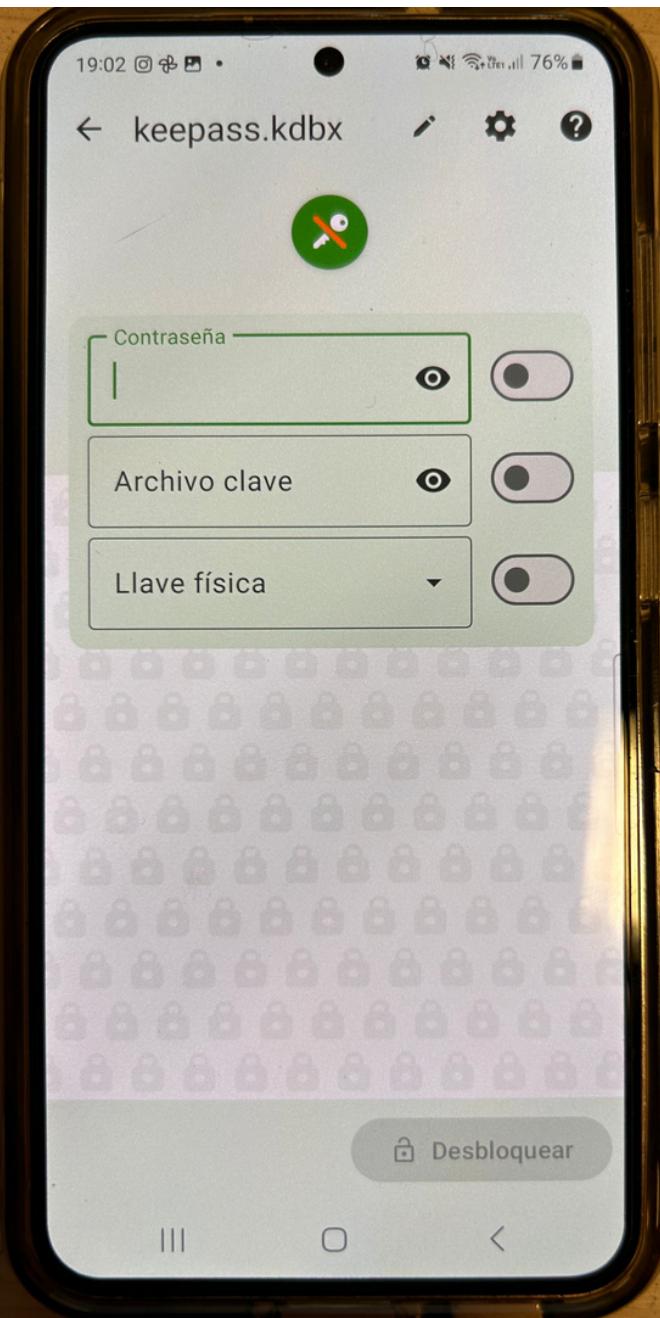
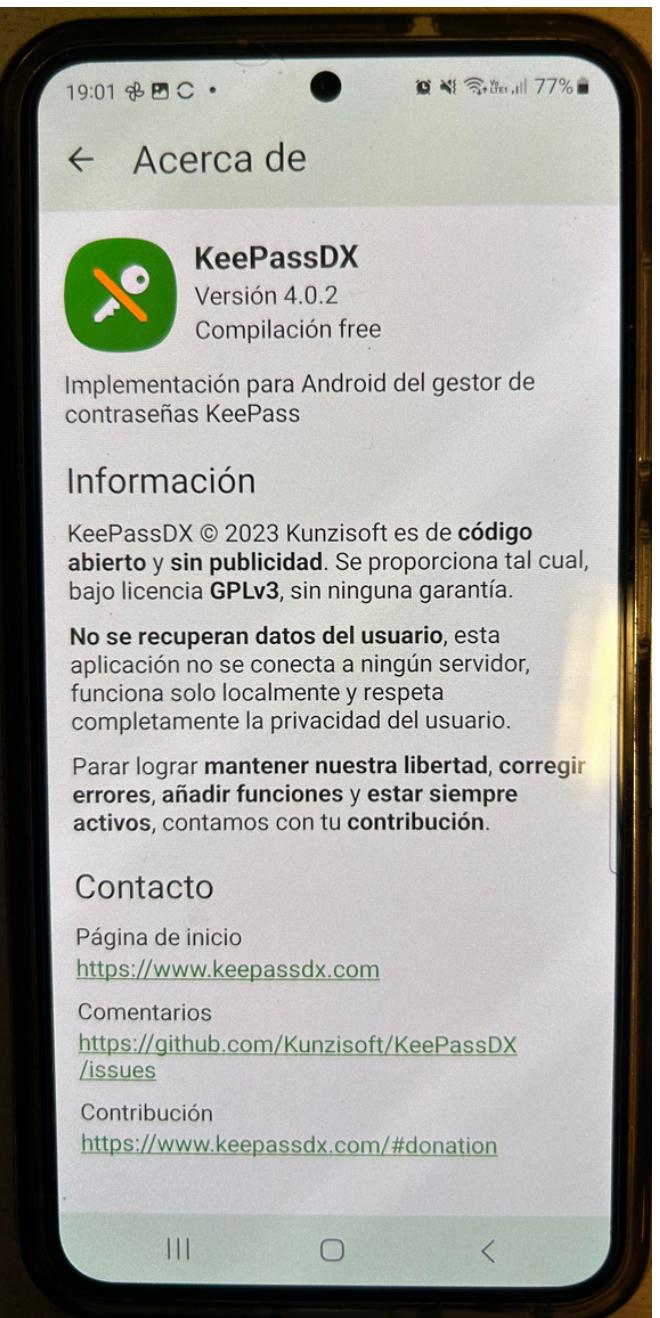
Además, la falta de integración nativa con sistemas operativos móviles como Android o iOS puede **dificultar la sincronización de contraseñas** en múltiples dispositivos, lo que podría requerir soluciones adicionales.



KeePassDX



Capturas.



> Google Trends

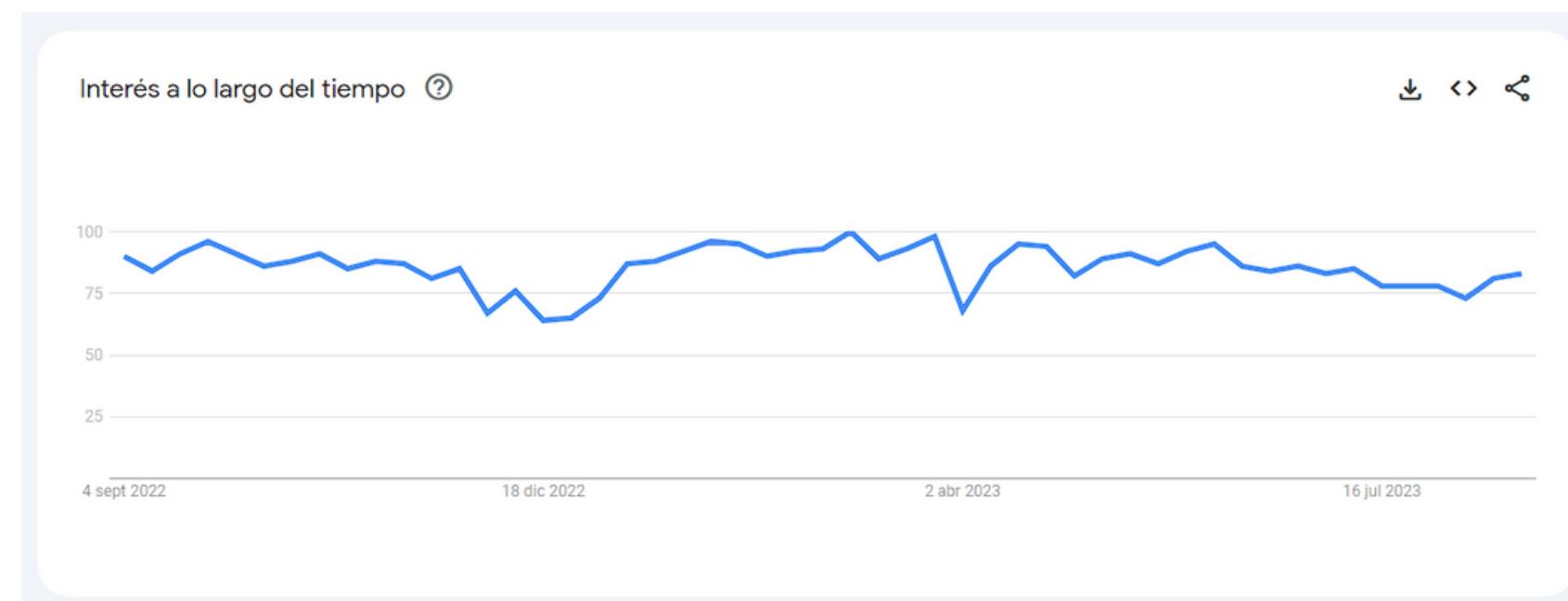


Esta herramienta llamada Google Trends nos permitirá obtener **datos y analíticas** sobre algún tema que sea ingresado.

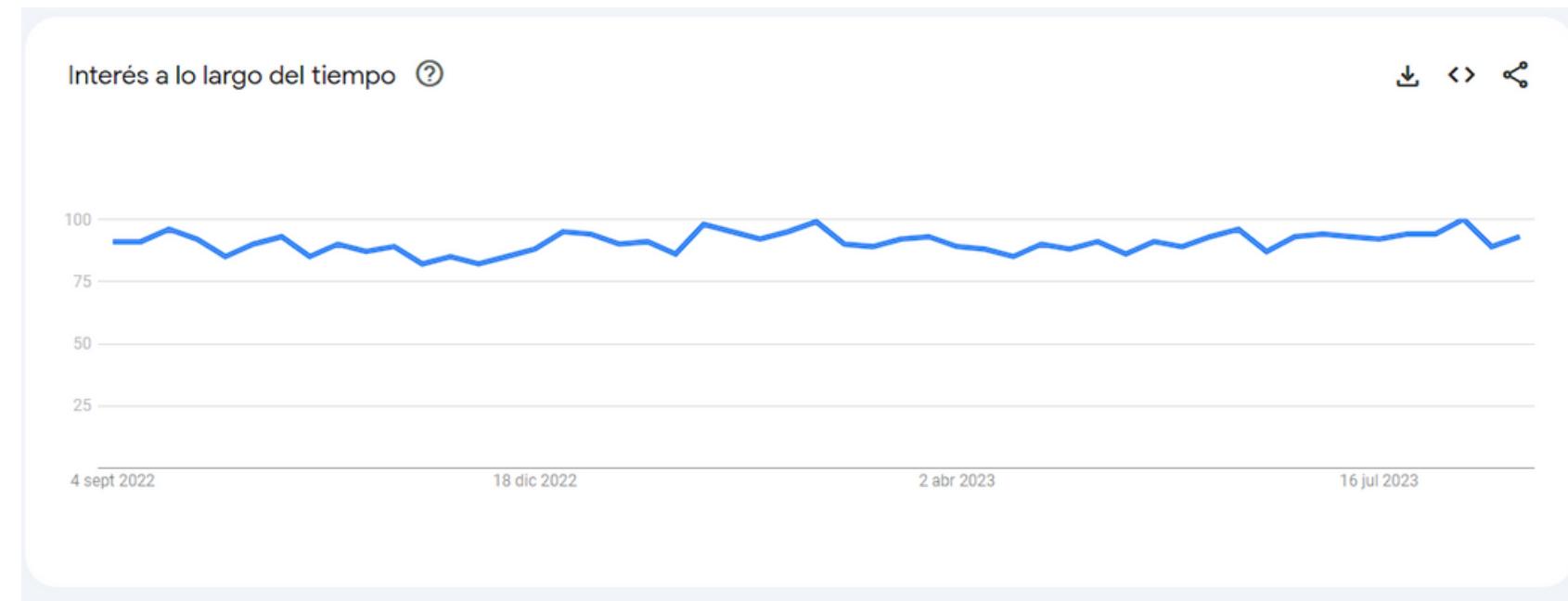
Es muy útil para saber si algún tema a tratar en mi proyecto será **relevante o no**, viendo si, esta en Trending (moda) o no.

Los números reflejan el **interés de búsqueda** en relación con el valor máximo de un gráfico en una región y un periodo determinados. Un valor de 100 indica la popularidad máxima de un término, mientras que 50 y 0 indican que un término es la mitad de popular en relación con el valor máximo o que no había suficientes datos del término, respectivamente.

SEGURIDAD:



PASSWORD:





Santiago Gómez

"Soy un amante de la tecnología que cree que la seguridad en línea es la clave para explorar el mundo digital con tranquilidad y confianza."

Tipo de Usuario:

Usuario consciente de la seguridad en línea.

Género:
Hombre.

Estado Civil:
Soltero.

Edad:
32 años.

Ciudad:
Ciudad de México.

Sobre Santiago:

Santiago es un ingeniero de software apasionado por la tecnología y la seguridad en línea. Trabaja para una empresa de desarrollo de software y pasa la mayor parte de su día frente a una computadora. Le encanta estar al tanto de las últimas tendencias tecnológicas y considera que la protección de su información personal y la de sus clientes es esencial en el mundo digital actual.

Objetivos y metas:

- Busca una solución que le permita administrar y recordar sus contraseñas de manera segura, sin tener que anotarlas en papel o recurrir a contraseñas simples.
- Quiere evitar posibles hackeos y pérdida de datos.
- Santiago desea ahorrar tiempo al acceder rápidamente a sus cuentas sin la necesidad de recuperar o cambiar contraseñas constantemente.

Motivaciones y frustraciones:

Frustraciones

- Olvidar contraseñas importantes.
- Pasar tiempo en procesos de recuperación o cambiar contraseñas periódicamente.
- Dificultad para Equilibrar Seguridad y Comodidad

Motivaciones

- Seguridad Personal.
- Eficiencia y Productividad.
- Dominar la Tecnología.



Nicolas Martinez

"Desea gestionar sus contraseñas de manera segura y eficiente, todo mientras optimiza su productividad y resguarda celosa mente sus datos personales en el vasto mundo digital"

Tipo de Usuario:

Usuario con temor al guardado de contraseñas en navegadores

Género:
Hombre.

Estado Civil:
Soltero.

Edad:
25 años.

Ciudad:
Catamarca

Sobre Nicolas:

Nicolas es una persona que se toma muy en serio la seguridad en línea. En un mundo donde la comodidad a menudo parece ser la norma, Javier se destaca como alguien que nunca guarda sus contraseñas en los navegadores, ya sea Chrome o Firefox. Para él, esta práctica es una línea infranqueable en la arena de la seguridad digital.

Objetivos y metas:

- Su principal objetivo es educar a otros sobre los riesgos de guardar contraseñas en navegadores como Chrome y Firefox.
- También trabaja para promover el uso de gestores de contraseñas seguros.
- A nivel personal, se esfuerza por mejorar continuamente su propia seguridad en línea.

Motivaciones y frustraciones:

Frustraciones

- Falta de Conciencia sobre los riesgos de guardar contraseñas en navegadores.
- Proriza la comodidad por sobre la seguridad.
- La constante aparición de vulnerabilidades de seguridad en navegadores y servicios en línea.

Motivaciones

- Seguridad Personal.
- Educar a otros sobre los riesgos y la seguridad en línea.
- Pasión por la Tecnología y Seguridad.



Abigail Lucero

"La seguridad en línea es una preocupación constante para mí. Quiero estar segura de que mis valiosos proyectos y datos personales estén protegidos de cualquier amenaza cibernética."

Tipo de Usuario:

Usuario propenso a frustrarse a la hora de recuperar contraseñas

Género:
Mujer

Estado Civil:
Soltero.

Edad:
33 años.

Ciudad:
Argentina

Sobre Abigail:

Es una diseñadora gráfica apasionada por la creatividad y la tecnología. Siempre está trabajando en proyectos emocionantes y colaborando con diferentes equipos. Sin embargo, a medida que se introduce más en el mundo digital, se le ha vuelto más complejo mantener un registro de todas sus contraseñas, convirtiendo esta situación en un desafío constante. Quiere asegurarse de que sus cuentas estén protegidas, pero recordar contraseñas seguras para cada servicio es un desafío real.

Objetivos y metas:

- Gestionar contraseñas de manera eficiente
- Ahorrar tiempo a la hora de recuperar contraseñas
- Asegurar sus cuentas en línea

Motivaciones y frustraciones:

Frustraciones

- Propensa a olvidar contraseñas.
- Inseguridad en línea.
- Tiempo perdido intentando recuperar contraseñas.

Motivaciones

- Simplicidad y eficiencia a la hora de acceder a sus cuentas.
- Seguridad personal ante amenazas cibernéticas.
- Confianza en la tecnología a la hora de ofrecer soluciones.



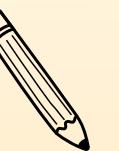
Para reducir estos riesgos, aquí hay algunos consejos

Tip 1º



- Utiliza una contraseña sólida para tu dispositivo y asegúrate de que esté bloqueado cuando no lo estés usando.
- Mantén tu navegador y sistema operativo actualizados.
- Sé cauteloso con los correos electrónicos y enlaces sospechosos que podrían llevar a sitios de phishing.

Tip 2º



- Evita guardar contraseñas en navegadores cuando utilices dispositivos compartidos o públicos.
- Siempre cierra la sesión y elimina las contraseñas guardadas después de usar el dispositivo.

Tip 3º



- Si necesitas acceder a cuentas en dispositivos compartidos, considera utilizar la navegación en modo incógnito o privado. Esto evitara que el navegador guarde tus contraseñas y datos de inicio de sesión

> Entrevistas



OBJETIVOS

- En primer lugar **validar nuestra hipótesis** “La relación entre el usuario y su experiencia en sitios o servicios que requieran de una contraseña resulten en un deterioro y hasta en una relación amor-odio”
- **Descubrir las necesidades** que tienen los usuarios ante la seguridad de sus cuentas y contraseñas.
- **Entender** en qué contexto utilizan productos similares o podrían llegar a utilizar el nuestro.
- **Obtener información** que nos permita validar los user persona.

> Entrevistas - Guión



INTRODUCCIÓN

“Buenos días/tardes/noches, primero que nada te agradezco de mi parte y todo mi equipo por tu participación en la entrevista de el día de hoy, mi nombre es ____ y junto a mis compañeros estamos realizando una investigación para la materia “Experiencia de Usuario” de la Carrera de Diseño y Programación web.

Nuestro objetivo es recaudar información sobre la problemática que pueden generar las multicuentas y la falta de seguridad que puede llegar a pasarnos por nuestra mente al momento de colocar nuestras contraseñas en algún dispositivo.

La idea es que sea una conversación un poco informal, no te sientas presionado/a, ya que buscamos que seas lo más sincero/a posible, no hay respuestas correctas o incorrectas.

Comenzaremos con algunas preguntas un poco generales y otras algunos temas un poco más particulares.”

> Entrevistas - Guión



ACLARACIONES

“Todo lo que hablemos a continuación será confidencial, por ende te quería consultar si me autorizas a grabar la charla, para más tarde pasar a revisarla por si algo se me paso por alto y detallar mejor lo que hablamos. ¿Estás de acuerdo en que sea grabada?

No hay problema si algún tema preferis no hablarlo o responder, comentame y seguimos adelante con lo siguiente.”

> Entrevistas - Guión



CIERRE

“Te agradezco nuevamente en nombre mio y de todo mi equipo por participar en esta entrevista, nos va a permitir poder continuar con nuestro proyecto y funcionalidades las cuales podríamos sumar.

Chequeando un poco lo hablado (Resumen de lo relevante) Te quería consultar si por casualidad tenes algún comentario que quieras sumar y no lo hablamos, o si te quedo alguna duda la cual quieras resolver y hablar, es tu espacio.

De no ser así, damos por finalizada la entrevista, nuevamente te agradezco por brindarnos tu tiempo.”



FRASES ENTREVISTA MANUEL - VICENTE

Entrevistador: ¿Tenés más de una cuenta de E-mail?

→ "Tengo Múltiples Cuenta de E-mail".

Entrevistador: ¿Con Cuanta Frecuencia olvidas tus claves?

→ "Medianamente frecuente", "De olvidármelas, me las olvido todo el tiempo, ya que hoy en día no sabría decirte cual es mi contraseña de Instagram"

Entrevistador: ¿Te es frustrante crear contraseñas para tus correos o usuarios de alguna cuenta?

→ "Si me es tedioso, en algunos casos más que otros, pero si"

Entrevistador: ¿Tenés inconvenientes al momento de cambiar o recuperar las contraseñas?

→ "En el caso de steam, pide varios pasos de verificación, es fastidioso"

Entrevistador: ¿Qué es lo más difícil al momento de elegir una contraseña?

→ "Lo más difícil creo yo, es encajar en el estándar que requiera la página, y después en que pueda recordar la contraseña"



FRASES ENTREVISTA MATIAS - MARCO

Entrevistador: ¿Tenés más de una cuenta de E-mail?

→ "Si Actualmente tengo 3 emails"

Entrevistador: ¿Confías en programas que guarden contraseñas?"

→ "No, no utilizo ningún programa que me guarde las contraseñas"

Entrevistador: ¿Te es frustrante crear contraseñas para tus correos o usuarios de alguna cuenta?

→ "Si la verdad que sí, volver a hacer una contraseña o cuenta la verdad que si"

Entrevistador: ¿Que te genera desconfianza y por qué no las guardas?

→ "Como es internet y todo el mundo puede acceder, no me genera confianza"

Entrevistador: ¿Qué es lo más difícil al momento de elegir una contraseña?

→ "Volver a escribirlas de nuevo, pensar otras"

Entrevistador: ¿En el trabajo que actualmente ejerces, se utilizan multipliques cuentas de correo?

→ " Se utilizan 2 cuentas de correo, como somos pocos todos tienen la contraseña"



FRASES ENTREVISTA GONZALO - BELÉN

Entrevistador: ¿Para vos es frustrante crear una clave nueva?

→ "Si re, las claves nuevas generalmente me las sugiere el celular"

Entrevistador: ¿Has tenido inconvenientes con tus cuentas?

→ "Si me ha pasado que me robaron el celular y no tenía protegido mercado pago"

Entrevistador: ¿Te es frecuente olvidar tus claves?

→ "Si siempre, nunca las recuerdo, porque tengo muchísimas claves de distintas cosas"

Entrevistador: ¿En el trabajo se utilizan múltiples cuentas de correo?

→ "En el trabajo solo una cuenta, son todas claves personales la de mails, y cada aplicación tiene su clave particular"

Entrevistador: ¿En cuánto tiempo aproximadamente se te olvida la contraseña?

→ "Siempre, tengo que recurrir a me olvide mi clave, por suerte tengo todo configurado con autenticación dos pasos"



Insights

 El entrevistado **Vicente** tiene 2 cuentas de mail, la primera la utiliza para registrarse en sitios donde sabe que luego, le pueden llegar notificaciones y correos basura. Quizás en algún pasado tuvo inconvenientes con cuentas llenas de correos basuras, impidiendo la limpieza y claridad en su cuenta de mail.

La segunda cuenta de mail la utiliza para asuntos más importantes y es la que ocupa recurrirmente para chequear que no tenga asuntos y mails importantes de trabajo o personales.

 El entrevistado **Marco** explica al final de la entrevista que, en su trabajo actual, todo su equipo posee las contraseñas de los emails que se utilizan, y comenta que es viable esa forma de trabajar, pero no segura ya que se puede filtrar la contraseña o la puede perder.

Quizás en algún momento se filtró la contraseña, ya que al poseer la contraseña mucha cantidad de personas, la seguridad de la contraseña se compromete.

> Conclusión

EN BASE A ESTAS ENTREVISTAS, PODEMOS CONCLUIR LO SIGUIENTE:

- La creación y gestión de contraseñas siguen siendo un desafío para las personas. La mayoría de los entrevistados encuentran frustrante crear contraseñas, y algunos olvidan sus contraseñas con frecuencia.
- La confianza en programas para gestionar contraseñas varía. Vicente utiliza una aplicación de generación de contraseñas, lo que es una buena práctica para mejorar la seguridad, mientras que Marco y Belén no confían en estos programas.
- La seguridad en línea es una preocupación. Varios entrevistados han experimentado problemas de seguridad, lo que subraya la importancia de adoptar medidas adicionales para proteger las cuentas en línea, como la autenticación de dos pasos.
- En entornos laborales, compartir contraseñas es común, pero puede ser riesgoso. Marco mencionó que en su trabajo, todos tienen acceso a la misma contraseña, lo que puede plantear problemas de seguridad y acceso no autorizado.



[Link al drive de las entrevistas](#)

> Benchmarking



Cantidad de pasos para:

Google Authenticator

1Password: Password Manager

KeePassDX

Generar código de verificación

2

3

3

Configurar una cuenta

2

3

2



Criterios de diseño

Limpio: Uso de espacios en blanco de manera efectiva para que los elementos importantes destaqueen y sea fácil de entender.

Google Authenticator

Simplicidad visual, uso eficiente del espacio negativo, organización lógica, tipografía clara, paleta de colores discreta, escasez de elementos decorativos y respeto por las convenciones de diseño. ✓

1Password: Password Manager

Interfaz intuitiva, diseño minimalista, tipografía legible, organización efectiva de datos, uso adecuado del espacio, paleta de colores atractiva y respeto por las convenciones de diseño. ✓

KeePassDX

Interfaz sencilla, organización lógica, tipografía clara, uso eficiente del espacio y opciones de personalización. ✓

Balanceado: Elementos visuales distribuidos de manera equilibrada.

Los elementos distribuidos de manera equilibrada, contribuye a una interfaz visualmente atractiva. ✓

Presenta una distribución equilibrada de elementos visuales en su interfaz. ✓

La aplicación mantiene un equilibrio en la distribución de elementos visuales en su interfaz. ✓

Lleno: Elementos no bien proporcionados y se hace mal uso del espacio.

No está sobrecargada de elementos visuales y no hace mal uso del espacio. ✗

No sufre de elementos visuales desproporcionados ni de un mal uso del espacio. ✗

No está sobrecargada de elementos visuales y no hace un mal uso del espacio. ✗

Intuitivo: Guía a los usuarios de manera natural y sin confusiones a través de la aplicación.

Interfaz simple, flujo de trabajo lógico, iconografía reconocible, instrucciones claras y navegación fácil. ✓

Interfaz lógica, iconografía significativa, instrucciones claras y navegación eficiente. ✓

Configuración inicial complicada con abundancia de opciones avanzadas. ◆



Vocabulario

Cumple: Permite que el usuario pueda cumplir sus objetivos.

Error menor: si bien es un error, permite seguir haciéndolo

Errores mayores no permite operar, El usuario se pierde y no cumple su objetivo

Google Authenticator

Google Authenticator permite que los usuarios cumplan sus objetivos de autenticación de dos factores de manera efectiva.✓

Aunque es raro, puede haber errores menores en la generación de códigos de autenticación. Sin embargo, estos errores suelen ser temporales y se resuelven automáticamente.✓

En casos extremadamente raros, podría haber errores mayores que impidan la autenticación. Esto puede ocurrir si el dispositivo está desincronizado, pero es poco común.✗

1Password: Password Manager

Permite que los usuarios cumplan sus objetivos de gestionar contraseñas de manera efectiva.✓

Puede haber errores menores, como problemas de sincronización ocasional, pero generalmente no impiden que los usuarios accedan a sus contraseñas.✓

Los errores mayores son poco comunes y generalmente no impiden el acceso a las contraseñas almacenadas.✗

KeePassDX

Permite que los usuarios cumplan sus objetivos de gestionar contraseñas de manera efectiva.✓

Puede haber errores menores, como problemas de sincronización o dificultades en la configuración, pero generalmente se pueden solucionar.✓

Los errores mayores son poco comunes y no suelen impedir que los usuarios accedan a sus contraseñas, pero pueden requerir asistencia técnica en casos excepcionales.✗



Fortalezas / Debilidades

Fortalezas

- Fácil de usar
- Códigos temporales
- Sin conexión a internet
- Permite agregar muchas cuentas
- No almacena información personal

Debilidades

- Es solo para dispositivos móviles
- Sin copia de seguridad
- Sin recuperación si pierdes el dispositivo
- Dependencia del dispositivo

Google Authenticator

1Password: Password Manager

KeePassDX

- Autenticación de 2 factores
- Acceso a multiples plataformas
- Autentificación biométrica
- Notificaciones de violación de seguridad

- Código abierto
- Control total sobre tus datos
- Autenticación de 2 factores
- Acceso a multiples plataformas
- Exportación e importación de datos

- Es poco intuitiva
- Aprendizaje inicial complejo
- Sin sincronización en la nube integrada
- Orientada a usuarios técnicos o avanzados
- Sin notificaciones de violación de seguridad

Frustration al momento de tener que recordar sus claves

Frustration al no poder guardar sus claves para poder recordarlas

Frustration de no poder confiar en las app

¿Qué piensa y siente?

Lo que realmente importa
Principales preocupaciones
Inquietudes y preocupaciones



¿Qué oye?

Lo que dicen sus amigos
Lo que dicen sus familiares
Lo que dicen las personas influyentes

¿Qué ve?

En su entorno
En sus amigos
En el mercado

Note

En las redes sociales ve como proteger sus cuentas

Ve que en su entorno es muy común el robo de contraseñas

A varios de sus amigos se les olvidaron sus contraseñas

¿Qué dice y hace?

Actitud en público
Aspecto
Comportamiento hacia los demás

Escribe las claves en papeles que después pierde o no recuerda donde dejó

Elige usar la misma contraseña para múltiples cuentas

Elige segmentar sus cuentas y guardar las claves de las menos importantes en los buscadores

Miedos y frustraciones

El tiempo perdido a la hora de recuperar contraseñas

Las inseguridades en línea

Tener que crear contraseñas difíciles y recordarlas

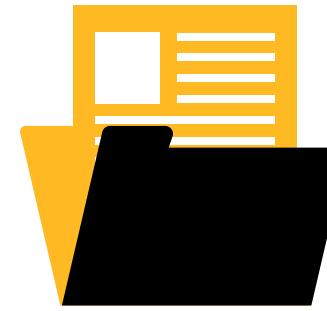
Deseos y necesidades

permanecer seguras las claves de seguridad, y que sea un fácil uso la app

Buscar una app segura donde confiar y donde no se vendan información

Desea encontrar sus contraseñas en un mismo lugar

MVP



ADMINISTRA TU SEGURIDAD

- Busca tus claves.
- Ve quienes acceden a tus contraseñas.
- Agrega datos biométricos y verificación SMS.



CREA TU SEGURIDAD

- Generador de claves seguras. (alfanumérica, caracteres especiales)
- Agrega las contraseñas que creaste directamente a tus aplicaciones.



ASEGURA Y GUARDA TUS CONTRASEÑAS

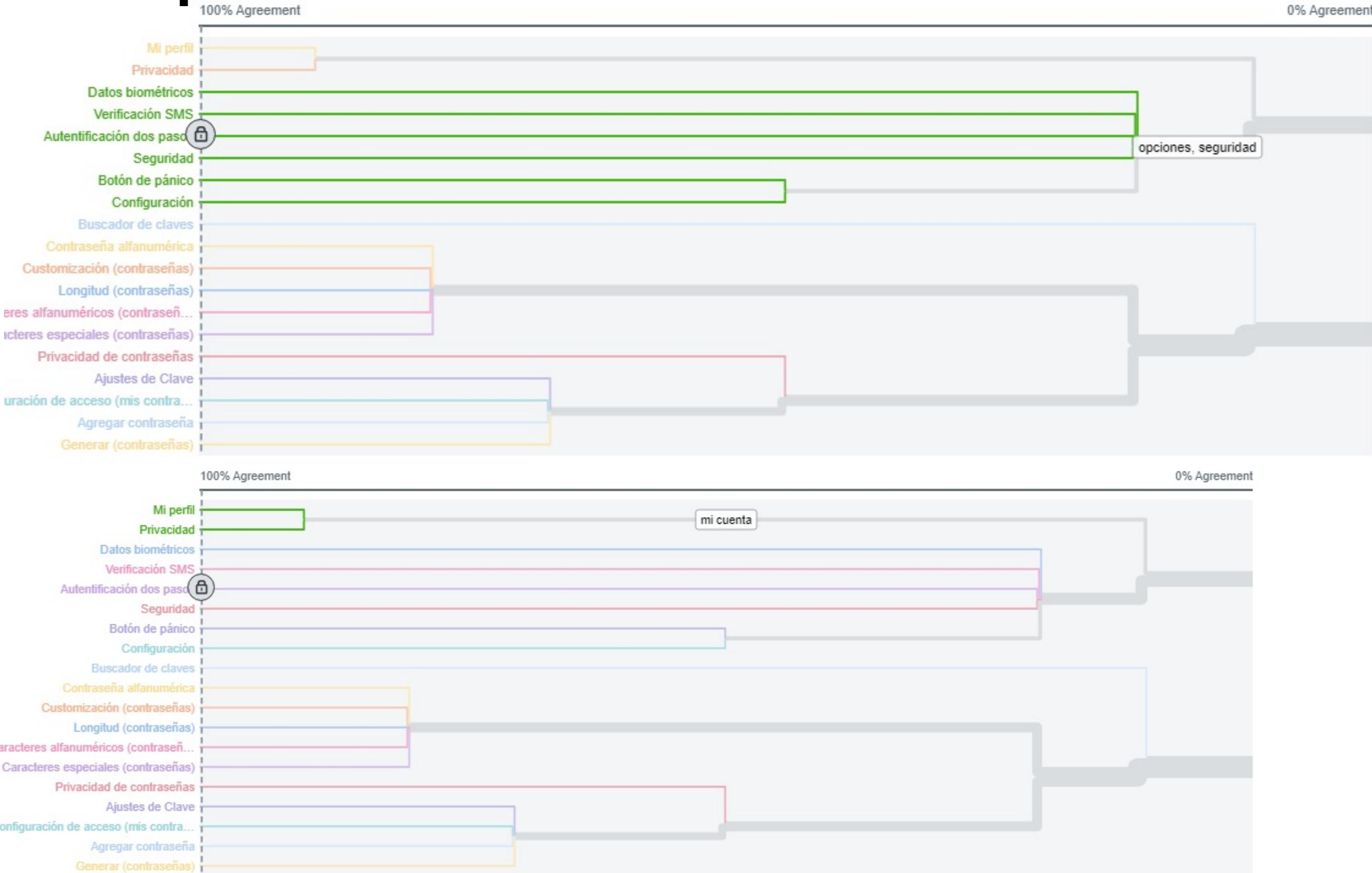
- Autentificación de dos pasos en tu perfil.
- Botón de pánico: bloquea y protege tus datos en la aplicación en caso de robo.
- Administra tu privacidad y seguridad.



Similarity matrix ②

Datos biométricos																					
100	Verificación SMS																				
83	83	Botón de pánico																			
50	50	66	Configuración																		
50	50	50	66	Mi perfil																	
33	33	33	50	83	Privacidad																
50	50	50	16	33	50	Autentificación dos pasos															
33	33	33	33	33	50	83	Seguridad														
0	0	0	16	0	16	33	50	Privacidad de contraseñas													
0	0	0	0	0	16	33	33	83	Configuración de acceso (mis contraseñas)												
0	0	0	0	0	16	33	33	83	100	Aregar contraseña											
0	0	0	0	0	16	33	33	66	83	83	Generar (contraseñas)										
16	16	0	0	0	16	33	33	66	83	83	83	83	Ajustes de Clave								
16	16	16	0	0	0	33	16	33	33	33	50	33	33	Contraseña alfanumérica							
16	16	16	0	0	0	33	16	33	33	33	50	33	100	Customización (contraseñas)							
16	16	16	0	0	0	33	16	33	33	33	50	33	100	100	Caracteres especiales (contraseñas)						
33	33	33	16	16	16	16	0	16	16	16	33	16	83	83	83	Longitud (contraseñas)					
33	33	33	16	16	16	16	0	16	16	16	33	16	83	83	83	100	Caracteres alfanuméricos (contraseñas)				
33	33	33	33	33	50	33	16	50	50	50	33	33	33	33	33	50	50	Buscador de claves			

Optimal Workshop

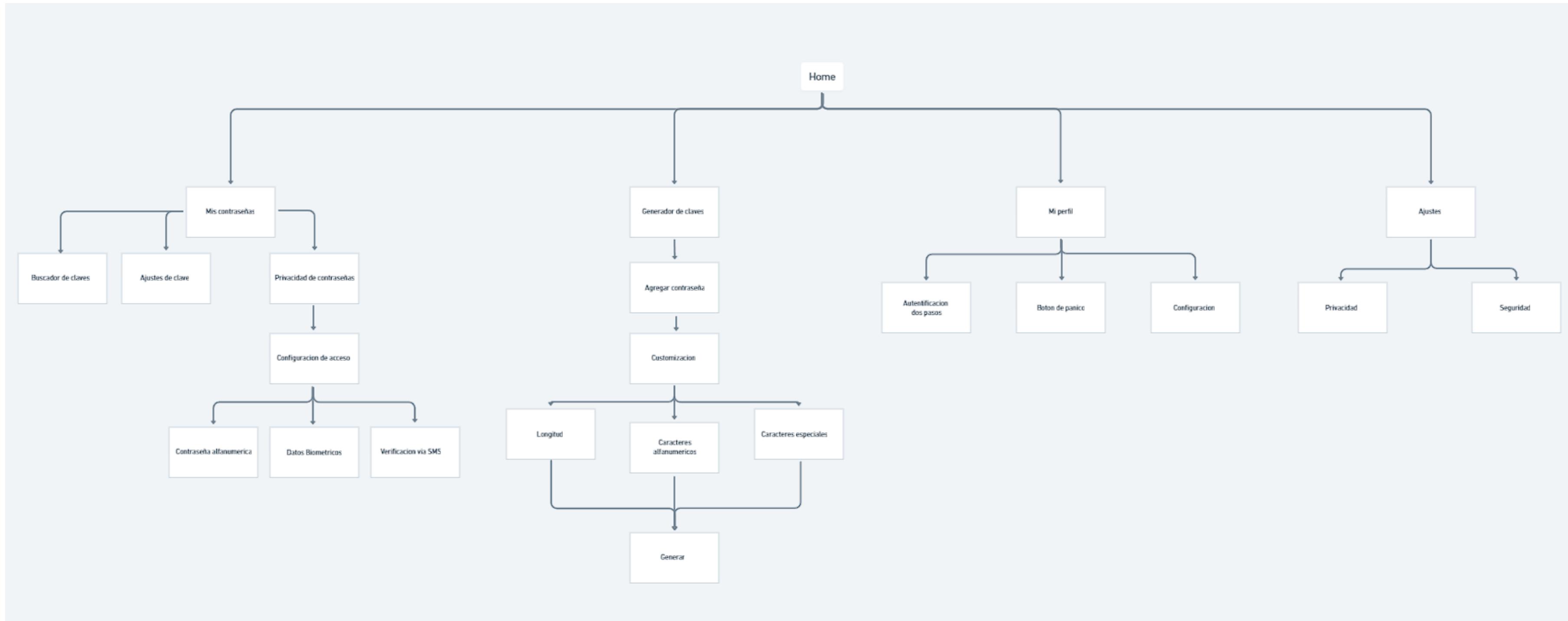


Optimal Workshop



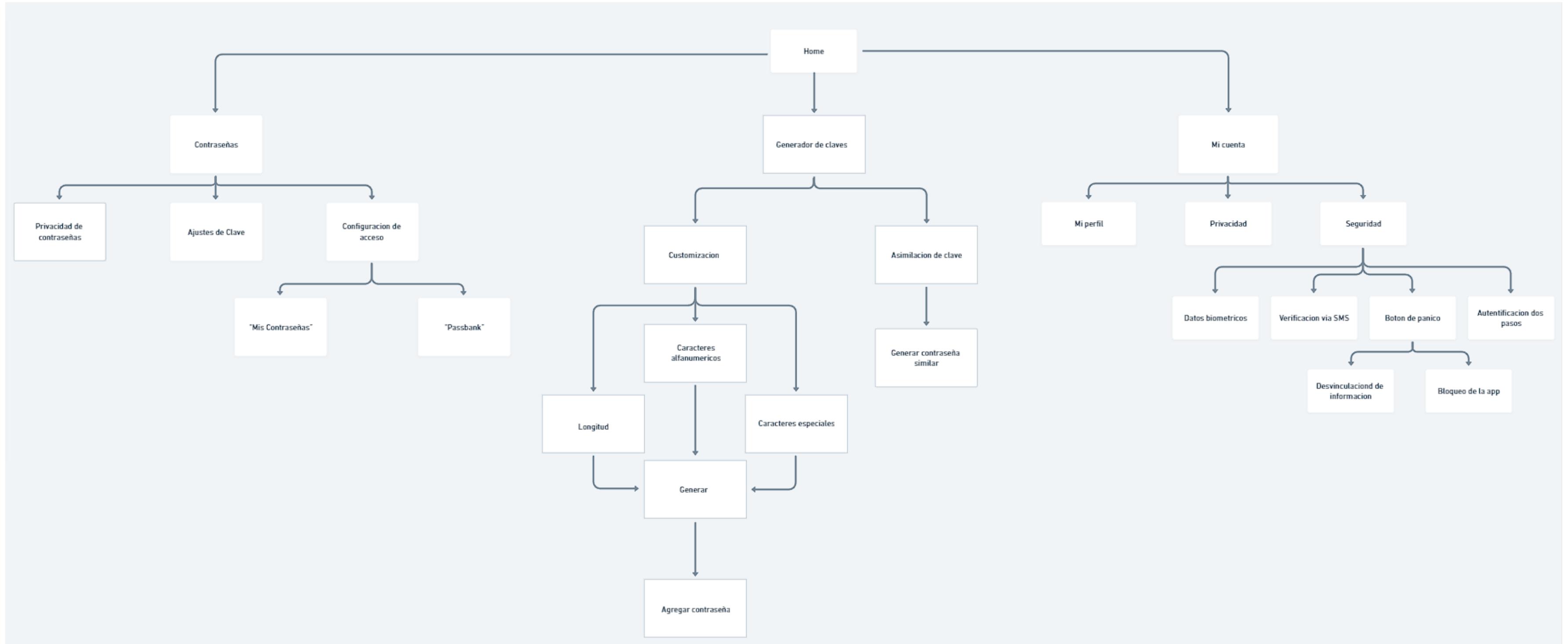
Optimal Workshop

Arquitectura de información.



Optimal Workshop

Iteración de arquitectura de información.



> Conclusion

En la propuesta original de la arquitectura de información, se segmentaron las categorías en cuatro, pero los usuarios encontraron esta organización incómoda y decidieron realizar ajustes, resultando en tres categorías principales:

- Contraseñas: Esta es la primera categoría que abarca toda la información relacionada con las contraseñas creadas por el usuario. Aquí se centralizan todas las claves de cuentas, lo que proporciona una organización más ordenada.
- Generador de contraseñas: La segunda categoría se enfoca en la generación de contraseñas. Se divide en dos subcategorías, lo que mejora la eficiencia de esta función. Una subcategoría permite al usuario generar una contraseña nueva y personalizable, mientras que la otra facilita la generación de una contraseña similar a una proporcionada por el usuario.
- Mi cuenta: La última categoría, "Mi cuenta", es una categoría amplia que abarca aspectos relacionados tanto con la seguridad general de la aplicación como con la seguridad de la cuenta del usuario. Aquí se fusionaron categorías y subcategorías, priorizando la seguridad y centralizando todas las funciones relevantes a nivel de aplicación y cuenta.

En la iteración de la arquitectura de información, los usuarios optaron por una organización más detallada, subcategorizando y priorizando la categoría "Mi cuenta". Esta elección refleja un mayor énfasis en la seguridad y una mejor organización de las funciones relacionadas con la aplicación y la cuenta. Además, la categoría "Contraseñas" se dividió en segmentos separados para las contraseñas y las claves de las cuentas, lo que mejoró la claridad y el orden.

En resumen:

Los usuarios reorganizaron la arquitectura de información de manera más eficiente y centrada en la seguridad, destacando la importancia de la gestión de contraseñas y la seguridad de la cuenta en la aplicación. Esto demuestra una respuesta efectiva a las necesidades y preferencias de los usuarios, lo que debería mejorar la experiencia general del usuario en la aplicación.



Cierre

Trabajar en equipo en este proyecto fue una experiencia altamente positiva tanto a nivel personal como profesional. La diversidad de puntos de vista y la colaboración de cada miembro del equipo enriquecieron nuestras perspectivas y nos permitieron abordar de manera más efectiva los desafíos que enfrentamos. Las entrevistas con terceros revelaron una variedad de opiniones y necesidades, lo que confirmó la relevancia del problema que Passbank busca resolver: la inseguridad de las contraseñas y la relación entre el usuario y sus credenciales.

A nivel de desarrollo profesional, este proyecto nos desafió a investigar a fondo las necesidades de los usuarios y a aplicar nuestras habilidades para organizar tareas de manera eficiente en un entorno de equipo. Nos sumergimos en el mundo de la experiencia del usuario, lo que nos permitió ver el potencial de mejora en una aplicación existente. En resumen, esta experiencia fue una oportunidad valiosa para aprender, crecer y aplicar nuestros conocimientos de manera colaborativa, y nos dejó con la satisfacción de haber contribuido a la creación de una solución innovadora en el campo de la seguridad de contraseñas.

Grupo 5



Gonzalo Guarnieri

Julieta Mendoza

Valentina Cuevas

Manuel Avendaño

Matias Martínez

Martina Duran

