Generador de Contraseñas Seguras

Jean Pierre Peña Rendón

Institución Universitaria Pascual Bravo

Facultad de Ingeniería

Tecnología en Desarrollo de Software

Medellín

2024

Generador de Contraseñas Seguras

Jean Pierre Peña Rendón

Trabajo de grado para optar al título de Tecnólogo en Desarrollo de Software

Asesor

Jaime Ernesto Soto Urdaneta

Institución Universitaria Pascual Bravo

Facultad de Ingeniería

Tecnología en Desarrollo de Software

Medellín

2024

Contenido

Lista de Tablas

Lista de Figuras

Resumen

En un entorno digital donde la cantidad de contraseñas necesarias para la autenticación sigue en aumento, los usuarios a menudo recurren a prácticas inseguras, como el uso de contraseñas débiles o la reutilización de las mismas en diferentes plataformas. Este comportamiento expone a los usuarios a riesgos significativos, ya que, una vez comprometida una contraseña, otras cuentas pueden quedar vulnerables. La seguridad de las contraseñas es fundamental para proteger tanto la información personal como la corporativa.

Por este motivo, se propone el proyecto "Generador de Contraseñas Seguras" para abordar este problema mediante el desarrollo de una aplicación web que facilita la generación y gestión de contraseñas seguras y personalizadas. Esta herramienta no solo genera contraseñas fuertes, sino que también mejora la seguridad de los usuarios en un entorno digital cada vez más complejo.

Palabras claves: Gestor de contraseña, contraseña, seguridad, vulnerabilidad, criptografía.

Introducción

En la actualidad, la seguridad digital se ha convertido en un pilar fundamental en la protección de la información personal y corporativa. Con la expansión de servicios en línea y la dependencia de cuentas digitales para actividades cotidianas, los usuarios se ven obligados a gestionar un número creciente de contraseñas. Este incremento en la cantidad de contraseñas genera un desafío importante: garantizar la seguridad y accesibilidad de estas claves sin comprometer la protección de la información.

Los usuarios, ante la dificultad de recordar múltiples contraseñas seguras, recurren a prácticas que debilitan su seguridad, como la reutilización de contraseñas en varios sitios, la creación de contraseñas sencillas o predecibles, y el almacenamiento de las mismas en lugares inseguros. Estas prácticas facilitan el trabajo de los atacantes cibernéticos, que pueden comprometer cuentas a través de técnicas como el phishing, ataques de fuerza bruta y la reutilización de credenciales en plataformas distintas. Esta problemática subraya la necesidad de soluciones que ayuden a los usuarios a crear y gestionar contraseñas de manera segura y eficiente.

El manejo de contraseñas ha evolucionado con la introducción de gestores de contraseñas, herramientas diseñadas para crear, almacenar y recuperar contraseñas complejas. Estos gestores han ganado popularidad gracias a su capacidad para generar contraseñas seguras y almacenar información cifrada, protegiéndola del acceso no autorizado. Sin embargo, muchos de estos gestores presentan limitaciones, como la dependencia de servicios en la nube, lo que podría generar vulnerabilidades adicionales, o la complejidad en su uso, que disuade a usuarios menos experimentados.

En respuesta a estas necesidades, la tecnología ha avanzado en varias direcciones. Por un lado, se ha mejorado la usabilidad de los gestores de contraseñas, integrándolos con navegadores y dispositivos móviles para facilitar su uso. Por otro lado, se han desarrollado métodos de cifrado más robustos para asegurar que las contraseñas almacenadas no puedan ser accedidas por atacantes.

También se ha avanzado en la integración de autenticación multifactor (MFA), que agrega una capa adicional de seguridad al requerir múltiples formas de verificación antes de conceder acceso a una cuenta. Sin embargo, la implementación de estas tecnologías no está exenta de desafíos, incluyendo la complejidad en la configuración para usuarios no técnicos y la dependencia de dispositivos adicionales para la autenticación.

Este proyecto se apoya en estas bases teóricas y tecnológicas para desarrollar una solución que no solo aborde la necesidad de generar contraseñas seguras, sino que también facilite su gestión, asegurando que los usuarios puedan mantener sus cuentas protegidas en un entorno digital cada vez más amenazante.

1. Planteamiento del Problema

1.1. Descripción

En la era digital actual, la expansión de servicios en línea ha llevado a los usuarios a crear y mantener numerosas credenciales, lo que a menudo resulta en prácticas inseguras debido a la dificultad de recordar contraseñas complejas. La reutilización de contraseñas y el uso de combinaciones simples aumentan significativamente el riesgo de brechas de seguridad. Este problema se agrava por la falta de concienciación y herramientas adecuadas para la gestión efectiva de contraseñas. En Colombia, Nu (2023) reporta que contraseñas comúnmente utilizadas incluyen secuencias simples como "123456", "contraseña" y "qwerty", lo que revela una grave falta de seguridad y una alta susceptibilidad a ataques de fuerza bruta.

Tabla 1

Las contraseñas más inseguras del mundo

Las contraseñas más inseguras del mundo	
1	123456
2	123456789
3	qwerty
4	password
5	111111
6	12345678
7	abc123
8	1234567
9	password1
10	12345

Nota. Fuente: El autor.

El principal problema es que muchos usuarios emplean contraseñas débiles o reutilizadas debido a la dificultad para recordar y gestionar múltiples credenciales. Esto crea vulnerabilidades significativas en la seguridad personal y profesional. El uso de contraseñas fáciles de adivinar o repetidas en diferentes sitios web facilita el trabajo de los atacantes, quienes pueden comprometer varias cuentas con una sola contraseña expuesta (ODoherty, 2022). La ausencia de un sistema de gestión eficiente y seguro contribuye a estas malas prácticas, aumentando el riesgo de brechas de seguridad y pérdidas financieras.

La importancia del problema radica en que las contraseñas comprometidas pueden llevar a robos de identidad, accesos no autorizados a cuentas financieras y filtraciones de información confidencial. Según eSoft (2021), la falta de una estrategia adecuada para la gestión de contraseñas puede resultar en pérdidas financieras y daños a la reputación de individuos y organizaciones. La falta de diversidad y complejidad en las contraseñas, como lo demuestra la prevalencia de contraseñas débiles en Colombia, refuerza la necesidad de soluciones que fomenten prácticas más seguras y efectivas.

La solución propuesta es el desarrollo de una aplicación web que facilite la generación y gestión de contraseñas seguras mediante el uso de un gestor de contraseñas. Esta herramienta permitirá a los usuarios crear contraseñas robustas basadas en configuraciones personalizables y acceder a ellas a través de una interfaz intuitiva. El Tiempo (2023) y MetaCompliance (2022) coinciden en que los gestores de contraseñas proporcionan una solución efectiva al problema de la gestión de contraseñas, mejorando significativamente la seguridad al ofrecer características como almacenamiento cifrado y generación automática de contraseñas seguras.

1.2. Pregunta de Investigación

¿Es posible construir una propuesta de un generador de contraseñas que permita la reducción de prácticas inseguras relacionadas con las contraseñas entre los usuarios?

2. Objetivos

2.1. Objetivo General

Desarrollar una aplicación web que permita a los usuarios generar contraseñas seguras para reducir la reutilización de contraseñas y fortalecer la protección de la información personal frente a posibles brechas de seguridad, con una interfaz fácil de usar y opciones que permitan personalizar la experiencia. Esto asegura que la aplicación sea accesible para cualquier usuario, brindando una experiencia positiva y adaptada a sus necesidades específicas.

2.2. Objetivos Específicos

1. Identificar los patrones comunes de reutilización de contraseñas en los usuarios para definir los requisitos de seguridad de la aplicación mediante encuesta, informes de reportes y estudios previos sobre seguridad de contraseñas y hábitos de los usuarios.

2. Evaluar los resultados obtenidos de la encuesta y documentación de los patrones comunes de reutilización de contraseñas en los usuarios con el fin de obtener los requisitos que permita empezar el diseño de la interfaz y algoritmo.

3. Diseñar y desarrollar una interfaz intuitiva y amigable a partir de los datos obtenidos de los patrones comunes de reutilización de contraseñas que permita a usuarios sin conocimientos técnicos generar contraseñas seguras de manera rápida y sencilla.

4. Implementar e integrar al sistema de información un algoritmo de generación de contraseñas seguras para ofrecer opciones de contraseñas únicas y robustas mediante parámetros personalizables como longitud, uso de caracteres especiales y complejidad.

3. Marco Teórico

En la actualidad, la protección de la información digital es una prioridad tanto para individuos como para organizaciones, ya que la seguridad de los datos personales y corporativos está constantemente amenazada por actores malintencionados. Las contraseñas continúan siendo uno de los métodos más utilizados para la autenticación de usuarios y la protección de cuentas en línea, pero también representan uno de los eslabones más débiles en la cadena de seguridad. A medida que la cantidad de servicios en línea y la frecuencia de su uso aumentan, los usuarios se enfrentan al desafío de crear y recordar múltiples contraseñas seguras, lo que a menudo resulta en prácticas inseguras como la reutilización de contraseñas o la creación de claves simples y predecibles.

Las estadísticas muestran que un gran número de violaciones de seguridad ocurren debido a contraseñas débiles o comprometidas, y esto se agrava por la falta de concienciación sobre las buenas prácticas de gestión de contraseñas. Las contraseñas reutilizadas en múltiples plataformas pueden convertirse en un punto de acceso para los atacantes, que utilizan técnicas como ataques de fuerza bruta, phishing y la reutilización de credenciales para comprometer la seguridad de los usuarios. La necesidad de contar con contraseñas robustas y únicas es evidente, pero también lo es la necesidad de herramientas que ayuden a los usuarios a gestionar estas contraseñas de manera segura y sin complicaciones.

Ante este escenario, la criptografía y las tecnologías de autenticación han evolucionado para ofrecer soluciones más seguras y efectivas. Los gestores de contraseñas han surgido como herramientas clave para abordar estas vulnerabilidades, al permitir a los usuarios generar, almacenar y recuperar contraseñas complejas y únicas con facilidad. Sin embargo, los desafíos persisten, la dependencia de estos gestores de servicios en la nube puede presentar

riesgos adicionales, y la adopción de estas herramientas aún no es universal, en parte debido a la complejidad percibida por los usuarios menos técnicos.

En respuesta a estos desafíos, este proyecto propone el desarrollo de un generador de contraseñas seguras que no solo facilite la creación de contraseñas robustas, sino que también ofrezca una interfaz accesible para todos los usuarios, independientemente de su nivel técnico. La solución busca mejorar las prácticas de gestión de contraseñas y contribuir a la reducción de las vulnerabilidades asociadas con las malas prácticas actuales, fortaleciendo así la seguridad digital en un entorno cada vez más interconectado.

3.1. Ciberseguridad

La ciberseguridad se ha convertido en una preocupación crítica en la era digital, donde los riesgos asociados al uso de tecnologías y plataformas en línea aumentan constantemente. En un contexto donde tanto individuos como organizaciones dependen de la tecnología para sus operaciones diarias, la protección de la información y los sistemas es esencial para evitar pérdidas económicas, daño a la reputación y compromisos de la privacidad (IBM, 2024). Este marco teórico explora la definición de ciberseguridad, los principales riesgos y amenazas que enfrenta, y las mejores prácticas para mitigarlos.

La ciberseguridad es definida como el conjunto de prácticas, procesos y tecnologías diseñados para proteger redes, dispositivos, programas y datos contra ataques, daños o accesos no autorizados. Su propósito principal es garantizar la confidencialidad, integridad y disponibilidad de la información (AWS, s. f.-a). Esta disciplina abarca diversas áreas, incluyendo la seguridad de redes, la seguridad de aplicaciones y la gestión de la identidad y el

acceso, siendo una parte fundamental de la protección de los activos digitales en todos los sectores.

Figura 1

Ciberseguridad

Nota. Adaptada de Iciberseguridad, por Riso, J, 2023 (https://iciberseguridad.org/wp-content/uploads/2023/10/Portada-Contexto-general-en-Ciberseguridad-01.png).

3.1.1. Riesgos y Amenazas

Los riesgos y amenazas en el ámbito de la ciberseguridad son diversos y cambian de manera acelerada. Entre las principales amenazas se encuentran el **malware,** un tipo de software creado con la intención de dañar sistemas o redes. Dentro de esta categoría se incluyen virus, troyanos, ransomware y spyware, cada uno diseñado para cumplir objetivos específicos como el robo de información, la extorsión a los usuarios, o la alteración de sistemas completos (Rodríguez, 2021). Este tipo de ataque puede ser devastador para las organizaciones, ya que no solo compromete la integridad de sus sistemas, sino que también puede afectar su reputación y operaciones.

Además de las amenazas derivadas del malware, otro riesgo creciente es **el phishing.** Esta técnica de manipulación psicológica, que se apoya en la confianza de los usuarios hacia fuentes aparentemente legítimas, es utilizada por los atacantes para obtener datos sensibles como contraseñas o información financiera (IBM, 2024). La facilidad con la que se pueden distribuir estos ataques, junto con la dificultad que tienen muchos usuarios para reconocer los mensajes fraudulentos, convierte al phishing en una de las formas más comunes de ataque. En combinación con el malware, el phishing puede facilitar la entrada de software malicioso en los sistemas.

Junto a estas amenazas, los **ataques de fuerza bruta** y los **ataques de día cero** representan otro desafío importante. Los primeros buscan descifrar contraseñas probando múltiples combinaciones posibles, mientras que los segundos aprovechan vulnerabilidades que aún no han sido identificadas por los desarrolladores, lo que los convierte en una amenaza especialmente peligrosa debido a la falta de defensas previas (AWS, s. f.-a). La combinación de estos métodos permite a los atacantes explotar los puntos débiles de los sistemas sin que las organizaciones tengan tiempo para reaccionar, lo que subraya la importancia de una vigilancia constante y la actualización de los sistemas.

Finalmente, las **amenazas internas** son otro factor crítico en la ciberseguridad. A menudo, los empleados u otros actores con acceso privilegiado pueden, intencionalmente o por descuido, ser la causa de brechas de seguridad, ya sea proporcionando acceso no autorizado a datos o exponiendo vulnerabilidades que los atacantes pueden explotar (Cano, 2022). Estas amenazas internas pueden ser más difíciles de detectar, ya que provienen de individuos con acceso legítimo, lo que requiere que las organizaciones implementen políticas de seguridad más estrictas y sistemas de monitoreo adecuados.

Figura 2

Tipos de vectores de ataque

Nota. Adaptada de ¿Qué es un vector de ataque?, por Akamai, 2022, (https://www.akamai.com/site/es/images/article/2022/common-types-of-attack-vectors.png).

Es fundamental reconocer que la naturaleza dinámica y persistente de estas amenazas exige una vigilancia continua y la adopción de estrategias proactivas de defensa. Las organizaciones y usuarios deben mantenerse al tanto de las tendencias emergentes en ciberseguridad y actualizar sus medidas de protección regularmente. La combinación de tecnologías avanzadas con una cultura de ciberseguridad robusta es clave para mitigar estos riesgos y proteger la información crítica en un panorama digital en constante cambio.

3.1.2. Buenas Prácticas

Para mitigar los riesgos relacionados con la ciberseguridad, se han desarrollado una serie de buenas prácticas que pueden ser implementadas tanto por individuos como por organizaciones. Entre estas, destaca el **uso de contraseñas seguras** y la **autenticación multifactorial (MFA)**. Las contraseñas deben ser complejas, únicas y actualizadas regularmente para evitar accesos no autorizados. La autenticación multifactorial agrega una capa adicional de seguridad, ya que requiere más de un método de verificación para autenticar a los usuarios, lo que reduce significativamente el riesgo de comprometer una cuenta con solo obtener la contraseña.

Junto con las contraseñas y la autenticación, una **actualización regular de software** es fundamental para protegerse contra las vulnerabilidades conocidas. Las actualizaciones a menudo incluyen parches de seguridad esenciales que corrigen debilidades explotables por atacantes. Sin mantener los sistemas al día, las organizaciones pueden quedar expuestas a ataques que se aprovechan de fallos previamente corregidos en las versiones más recientes del software.

Otra práctica clave es la **educación y capacitación en ciberseguridad**. Formar a los empleados en todos los niveles de una organización acerca de los riesgos cibernéticos y cómo reconocer amenazas como el phishing es crucial para reducir la susceptibilidad a este tipo de ataques (Rodríguez, 2021). La educación no solo empodera a los usuarios para que actúen de manera más segura, sino que también puede mejorar la respuesta organizacional a incidentes potenciales.

Además de la capacitación, la **implementación de políticas de seguridad** es esencial. Establecer políticas claras y procedimientos específicos de respuesta a incidentes ayuda a gestionar los riesgos de manera eficiente. Estas políticas deben incluir directrices sobre el uso adecuado de dispositivos, la gestión de datos y la respuesta ante posibles brechas de seguridad. Tener procedimientos bien definidos permite una actuación más rápida y coordinada en caso de incidentes, lo que mitiga los daños.

Finalmente, el **cifrado de datos** es una técnica indispensable en la protección de la información, tanto en tránsito como en reposo. A través del cifrado, los datos se convierten en ilegibles para cualquier persona que no posea las claves necesarias para descifrarlos, asegurando así que, incluso si se interceptan, no puedan ser utilizados de manera malintencionada.

En conclusión, la ciberseguridad es una disciplina esencial para proteger la información y los sistemas en un mundo cada vez más digital. A medida que las amenazas continúan evolucionando, la adopción de buenas prácticas y tecnologías avanzadas es clave para proteger a las organizaciones y a los individuos de una amplia gama de riesgos. Medidas como la autenticación multifactorial, la actualización continua de software y la capacitación en ciberseguridad son indispensables para mantener un entorno digital seguro y confiable (AWS, s. f.-a; IBM, 2024). En última instancia, la ciberseguridad no es solo una cuestión técnica, sino una necesidad estratégica para garantizar la continuidad y éxito de las operaciones digitales.

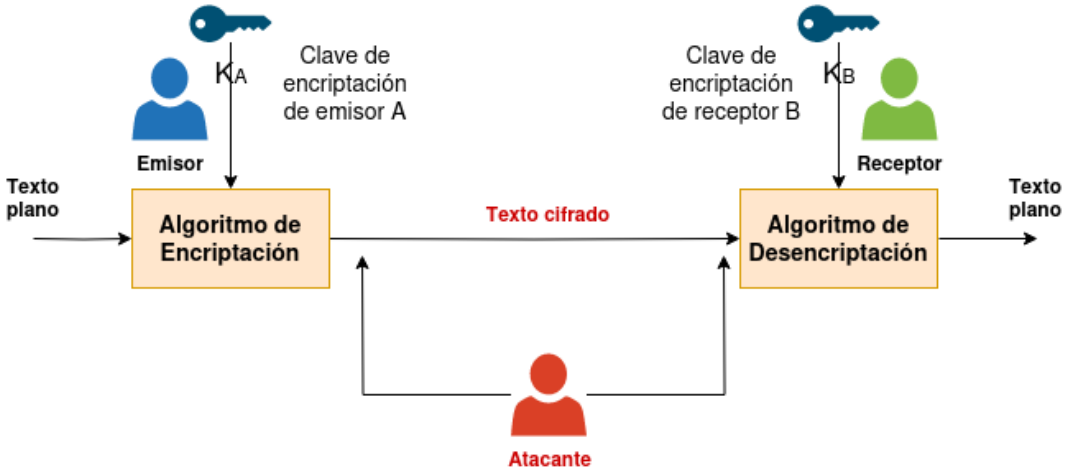
3.2. Criptografía

La criptografía es una disciplina esencial en el campo de la ciberseguridad, encargada de proteger la confidencialidad, integridad y autenticidad de la información a través de técnicas

de codificación y cifrado. Desde sus orígenes en la antigüedad hasta los complejos algoritmos computacionales de hoy, la criptografía ha evolucionado significativamente, adaptándose a los retos y amenazas de la era digital. Su aplicación es crítica en diversos ámbitos, incluyendo la protección de datos personales, transacciones financieras, y la seguridad de las comunicaciones digitales, lo que la convierte en un pilar fundamental de la seguridad informática contemporánea.

Figura 3

Criptografía



Nota. Adaptada de Introducción a la Criptografía, por Domingo, J, 2023 (https://www.josedomingo.org/pledin/assets/wp-content/uploads/2023/10/criptografia1.png).

La criptografía se define como el estudio y aplicación de técnicas que permiten asegurar la información y las comunicaciones mediante la transformación de datos legibles en un formato cifrado que solo puede ser interpretado por las partes autorizadas (AWS, s. f.-b). Este proceso de cifrado se realiza utilizando algoritmos matemáticos que aseguran que la información sea inaccesible para terceros no autorizados. Según IBM (2023), "la criptografía asegura la integridad de los datos al proteger la información sensible de alteraciones o accesos

no autorizados". Esta definición resalta la importancia de la criptografía en la protección contra las amenazas que buscan comprometer la privacidad y seguridad de los datos.

Existen diversos métodos y técnicas dentro de la criptografía, cada uno con sus propios mecanismos y aplicaciones. Los sistemas de cifrado se dividen principalmente en dos categorías: simétrico y asimétrico. La criptografía simétrica utiliza una única clave para cifrar y descifrar los datos, mientras que la criptografía asimétrica emplea un par de claves una pública y otra privada, facilitando la distribución segura de las claves y mejorando la autenticación y confidencialidad de la información (Paredes, 2006).

3.2.1. Algoritmos de cifrado simétrico y asimétrico

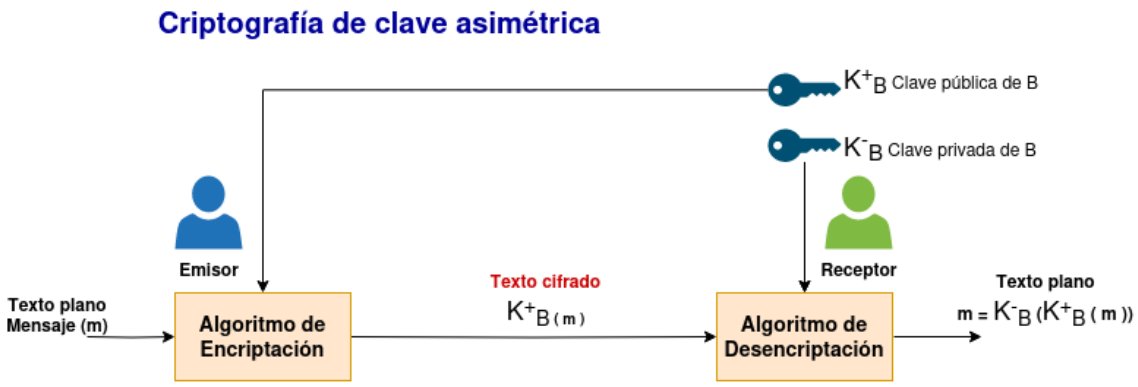
Los algoritmos de cifrado son el núcleo de la criptografía y se clasifican en dos tipos principales: **simétricos y asimétricos.** Los algoritmos de cifrado simétrico, como el DES (Data Encryption Standard) y el AES (Advanced Encryption Standard), utilizan la misma clave para cifrar y descifrar la información, lo que los hace altamente eficientes para manejar grandes volúmenes de datos. Sin embargo, uno de los desafíos principales de los algoritmos simétricos es la gestión y distribución segura de las claves, ya que ambas partes deben compartir la misma clave sin comprometer su seguridad (López, 2022).

Por otro lado, la criptografía asimétrica, representada por algoritmos como RSA (Rivest–Shamir–Adleman) y ECC (Elliptic Curve Cryptography), utiliza un par de claves distintas, pero matemáticamente relacionadas: una clave pública, que puede ser compartida abiertamente, y una clave privada, que debe mantenerse en secreto. Este enfoque permite una comunicación segura sin la necesidad de compartir previamente una clave común, resolviendo así uno de los problemas críticos de la criptografía simétrica (IBM, 2023). La criptografía asimétrica

proporciona una solución robusta para la distribución de claves y la autenticación de las comunicaciones, aunque con un mayor costo computacional.

Figura 4

Criptografía Asimétrica



Nota. Adaptada de Introducción a la Criptografía, por Domingo, J, 2023 (https://www.josedomingo.org/pledin/assets/wp-content/uploads/2023/10/criptografia3.png).

Los algoritmos asimétricos son particularmente útiles en la implementación de firmas digitales, que permiten verificar la autenticidad y la integridad de los mensajes, asegurando que no han sido alterados durante la transmisión. Aunque más lentos que los algoritmos simétricos, los algoritmos asimétricos son fundamentales en aplicaciones que requieren un alto nivel de seguridad, como el intercambio de claves y la autenticación de usuarios en sistemas bancarios y plataformas de comercio electrónico.

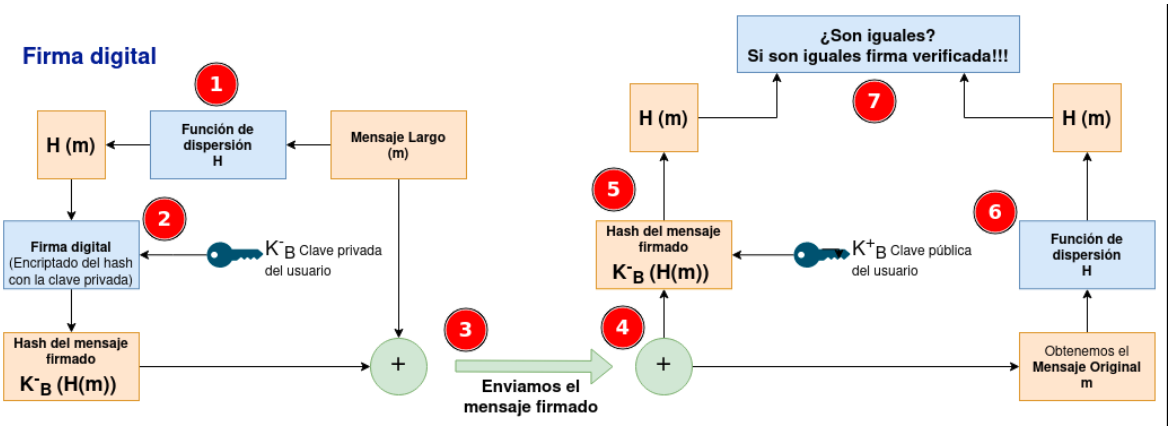
3.2.2. Funciones hash y su aplicación en la generación de contraseñas

Las funciones hash son algoritmos criptográficos que convierten una entrada de datos de cualquier tamaño en una cadena fija de caracteres, conocida como hash. Estas funciones

desempeñan un papel clave en la seguridad de la información, al proporcionar un medio para verificar la integridad de los datos y proteger las contraseñas en los sistemas de autenticación (AWS, s. f.-b). Las funciones hash, como SHA-256 (Secure Hash Algorithm 256 bits), generan un valor único para cada entrada, de manera que incluso un pequeño cambio en los datos originales producirá un hash completamente diferente, lo cual es esencial para detectar alteraciones no autorizadas (López, 2022).

Figura 5

Firma Digital



Nota. Adaptada de Introducción a la Criptografía, por Domingo, J, 2023 (https://www.josedomingo.org/pledin/assets/wp-content/uploads/2023/10/criptografia4.png).

En la gestión de contraseñas, las funciones hash son utilizadas para almacenar contraseñas de manera segura. En lugar de guardar las contraseñas en texto plano, los sistemas almacenan el hash de la contraseña, lo que significa que la contraseña original no puede ser recuperada directamente desde el hash. Durante el proceso de autenticación, el sistema compara el hash de la contraseña proporcionada por el usuario con el hash almacenado; si coinciden, el usuario es autenticado. Esta técnica mejora significativamente la

seguridad, ya que incluso si un atacante obtiene acceso a la base de datos de contraseñas, los hashes son inútiles sin la contraseña original (López, 2022).

La criptografía es un componente indispensable en la seguridad de la información moderna, proporcionando las herramientas necesarias para proteger los datos sensibles y garantizar la privacidad de las comunicaciones. Los algoritmos de cifrado simétrico y asimétrico ofrecen soluciones para diferentes necesidades de seguridad, desde la eficiencia y velocidad de los algoritmos simétricos hasta la robustez y flexibilidad de los asimétricos. Asimismo, las funciones hash juegan un rol crucial en la protección de contraseñas, proporcionando un mecanismo seguro para su almacenamiento y verificación.

En un mundo donde las amenazas digitales son cada vez más sofisticadas, la aplicación adecuada de técnicas criptográficas es esencial para salvaguardar la integridad y confidencialidad de la información. La continua evolución de la criptografía y su adaptación a nuevos desafíos tecnológicos refuerza su posición como un pilar clave en la defensa contra las amenazas cibernéticas.

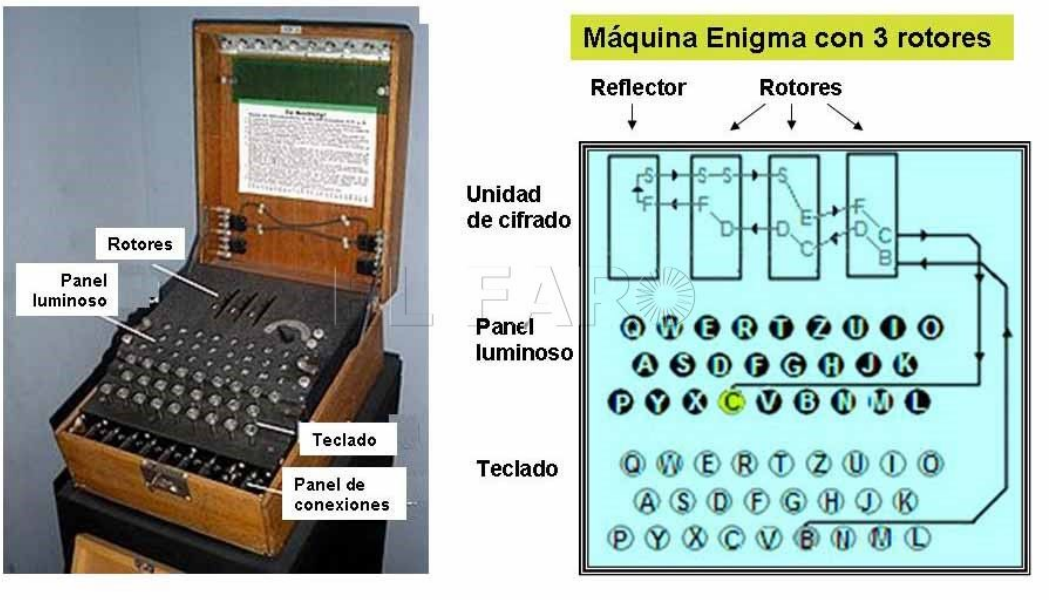
3.2.3. La Máquina Enigma

La máquina Enigma fue un dispositivo criptográfico que jugó un papel crucial en la Segunda Guerra Mundial, permitiendo a los alemanes asegurar sus comunicaciones. Su desarrollo y posterior implementación en el ejército alemán marcaron un antes y un después en la historia de la criptografía. Aunque su diseño y funcionamiento parecían impenetrables, la Enigma presentaba debilidades que fueron aprovechadas por los aliados. Para entender mejor el impacto de esta máquina, es importante analizar sus características fundamentales, las

mejoras realizadas a lo largo del tiempo y cómo los errores en su uso permitieron su descifrado.

Figura 6

Máquina Enigma



Nota. Adaptada de Historias de la Enigma, la máquina cifradora utilizada en la II Guerra Mundial, que se expone en Melilla, por El Faro, 2022 (https://elfarodemelilla.es/wp-content/uploads/2022/07/WhatsApp-Image-2022-07-04-at-10.03.14-AM.jpeg?v=1656922622).

En 1923, el ingeniero alemán Arthur Scherbius patentó la máquina Enigma, un dispositivo diseñado para facilitar la codificación de mensajes de manera segura. A simple vista, la Enigma era similar a una máquina de escribir, pero escondía un complejo mecanismo que la convertía en una poderosa herramienta criptográfica. Los mensajes eran introducidos a través del teclado, y la máquina cifraba automáticamente el texto, iluminando las letras cifradas en un panel. La clave de este proceso residía en las posiciones iniciales de tres rotores, los cuales se conectaban a un sistema de contactos y cableados que determinaban el cifrado de

cada letra. Este avance fue considerado revolucionario, ya que la rotación constante de los rotores generaba nuevas combinaciones con cada pulsación de tecla (López, 2022). Esta capacidad para cambiar continuamente las claves de cifrado aumentaba la dificultad para descifrar los mensajes interceptados.

A medida que se fue adoptando el uso de la Enigma en el ejército alemán, también se implementaron diversas mejoras técnicas para aumentar su seguridad. Una de las primeras modificaciones incluyó el "stecker" o clavijero, un sistema que permitía intercambiar seis pares de letras antes de comenzar el cifrado. Este añadido incrementaba enormemente las combinaciones posibles y hacía aún más difícil su descifrado. Además, los rotores fueron diseñados para ser intercambiables, lo que permitía que el operador eligiera tres rotores de entre cinco disponibles y los dispusiera en diferentes órdenes, aumentando exponencialmente el número de combinaciones posibles. Posteriormente, se añadió un cuarto rotor para elevar aún más la complejidad del cifrado. Sin embargo, a pesar de estas mejoras, la máquina presentaba vulnerabilidades tanto en su diseño como en los procedimientos utilizados para operarla. Estas debilidades serían explotadas más tarde por los criptoanalistas aliados (López, 2022).

A pesar de la complejidad técnica de Enigma, fue el uso repetitivo de patrones y errores humanos lo que facilitó su descifrado. El primer avance significativo en este sentido fue realizado por el servicio de inteligencia polaco, que en 1931 recibió información crucial sobre el funcionamiento interno de la máquina. Este conocimiento fue obtenido por espías franceses que sobornaron a un miembro de la oficina de cifras alemana, permitiendo así que los polacos construyeran una réplica funcional de Enigma. Gracias a este esfuerzo, los polacos comenzaron a descifrar algunos mensajes alemanes, aunque la situación se complicó a medida que los alemanes añadieron más rotores y complejidades al sistema. A medida que la guerra

avanzaba, los polacos compartieron sus avances con los británicos, quienes bajo la dirección de Alan Turing y su equipo en Bletchley Park, lograron desarrollar métodos aún más sofisticados para romper el código de Enigma. Este esfuerzo colaborativo resultó fundamental para cambiar el curso de la guerra, ya que proporcionaba a los aliados información crítica sobre los movimientos del ejército alemán (López, 2022).

Así, aunque la máquina Enigma fue concebida para asegurar las comunicaciones alemanas, las fallas en su diseño y el uso repetitivo de patrones facilitaron su descifrado por parte de los aliados. El éxito en romper el código de Enigma no solo fue un hito en la historia de la criptografía, sino que también influyó directamente en el resultado de la Segunda Guerra Mundial. La historia de Enigma es un claro recordatorio de que, por más complejo que sea un sistema criptográfico, los errores humanos y las vulnerabilidades pueden ser su mayor debilidad. En última instancia, el trabajo de los criptoanalistas polacos y británicos demostró la importancia de la inteligencia en tiempos de conflicto, y la capacidad de la colaboración internacional para superar desafíos aparentemente insuperables.

3.3. Normativas y Estándares de Seguridad

Las normativas y estándares de seguridad son esenciales para garantizar la protección de la información y minimizar los riesgos a los que están expuestas las organizaciones en el entorno digital. A medida que la ciberseguridad se convierte en una prioridad global, las empresas adoptan normativas internacionales para implementar medidas adecuadas de control y protección de sus activos. Entre las más destacadas se encuentran las normas ISO 27001 e ISO 27002, que proporcionan un marco sólido para gestionar y mejorar la seguridad de la información. Estas normativas ayudan a las organizaciones a establecer políticas coherentes, prácticas efectivas y una estructura clara para enfrentar los crecientes desafíos en seguridad.

La norma ISO 27001 es reconocida a nivel mundial como el estándar más importante para la gestión de la seguridad de la información. Su propósito es proteger los datos y sistemas críticos mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma proporciona un enfoque sistemático para gestionar la información sensible, asegurando su confidencialidad, integridad y disponibilidad. Las organizaciones que adoptan ISO 27001 demuestran un compromiso serio con la seguridad, ya que deben identificar los riesgos potenciales, implementando controles adecuados para mitigarlos y mejorando continuamente sus prácticas de seguridad (Solutions, 2023a)

Por su parte, la norma ISO 27002 complementa a la ISO 27001, proporcionando un conjunto detallado de controles de seguridad que las organizaciones pueden implementar para salvaguardar la información. Este estándar ofrece una guía práctica sobre cómo aplicar los controles establecidos en el marco de la ISO 27001, adaptándose a las necesidades específicas de cada organización. Además, la ISO 27002 ayuda a personalizar las medidas de seguridad de acuerdo con el contexto de la empresa, abordando aspectos clave como la gestión de riesgos, el control de accesos, la criptografía y la protección frente a amenazas externas. La aplicación de estas normativas es crucial en la mejora continua de las políticas de ciberseguridad (Solutions, 2023b).

El cumplimiento de las normas ISO no solo proporciona una estructura clara y consistente para gestionar la seguridad de la información, sino que también refuerza la confianza de los clientes, socios y empleados. Las organizaciones que certifican sus SGSI bajo ISO 27001 y aplican las directrices de ISO 27002 no solo reducen los riesgos de ciberataques, sino que también mejoran su capacidad para responder ante incidentes de seguridad. En un

entorno donde las amenazas evolucionan constantemente, seguir estos estándares permite a las empresas mantenerse resilientes y preparadas para enfrentar los desafíos de la era digital.

Las normativas y estándares de seguridad, como las ISO 27001 y 27002, son fundamentales para que las organizaciones gestionen de manera eficaz la seguridad de la información. Al implementar estos estándares, las empresas no solo protegen sus activos más valiosos, sino que también fortalecen su posición en un mercado cada vez más competitivo. La adopción de un enfoque proactivo basado en normas reconocidas internacionalmente es clave para garantizar la seguridad en el entorno digital actual.

3.4. Contraseñas

Figura 7

Contraseñas

Nota. Adaptada de Día de la contraseña: ¿la tuya es segura?, por Plonsak, H, 2022 (https://expansion.mx/tecnologia/2022/05/05/como-hacer-contrasena-segura).

En el mundo moderno, las contraseñas desempeñan un papel crucial para proteger la información personal y corporativa. Desde tiempos antiguos, la humanidad ha buscado mecanismos de protección, como las cerraduras de hace más de 4,000 años, que eran clave

para resguardar los bienes. En la actualidad, la seguridad informática sigue una lógica similar: proteger datos confidenciales mediante credenciales de acceso como los nombres de usuario y las contraseñas. Sin embargo, estas credenciales no siempre son suficientes para garantizar la seguridad, debido al crecimiento y sofisticación de las herramientas que los ciberdelincuentes tienen a su disposición para vulnerarlas (Goujon, 2013). Aunque las contraseñas siguen siendo el principal medio de protección, se ha demostrado que, cuando son débiles, pueden convertirse en un acceso fácil para los atacantes. Según un informe de NordPass, en países como Chile, Colombia y México, las contraseñas más utilizadas siguen siendo combinaciones simples como "123456" o "admin", lo que demuestra la persistencia de malos hábitos entre los usuarios, quienes no dimensionan la importancia de contar con contraseñas seguras (Axity, 2024).

Los ataques a contraseñas han evolucionado a lo largo del tiempo. Entre los más notables están los casos de robo masivo de contraseñas, como el incidente de LinkedIn, donde se expusieron 6.5 millones de contraseñas, o el ataque a Yahoo! en 2012, que comprometió 450,000 credenciales a través de una inyección SQL. Estos ejemplos ilustran que las contraseñas, aunque fundamentales, no son infalibles, y deben ser reforzadas con medidas adicionales de seguridad, como la autenticación multifactor, que añade una capa extra de protección (Goujon, 2013). Este tipo de ataques evidencian que incluso grandes plataformas son vulnerables, resaltando la necesidad de aplicar buenas prácticas y utilizar herramientas avanzadas para proteger los datos sensibles.

3.4.1. Buenas prácticas

Para mantener una adecuada seguridad digital, es fundamental que las contraseñas sean lo suficientemente robustas para resistir intentos de vulneración, como los ataques de

fuerza bruta. En ese sentido, una de las primeras recomendaciones es que las contraseñas tengan una longitud mínima de entre 8 y 12 caracteres, ya que mientras más larga sea la clave, más difícil será descifrarla. Asimismo, se sugiere incluir una combinación de letras mayúsculas, minúsculas, números y caracteres especiales, lo que añade complejidad y dificulta aún más los ataques. Microsoft, por ejemplo, destaca la importancia de utilizar contraseñas largas y complejas como una de las principales estrategias para asegurar las cuentas personales y corporativas (Axity, 2024).

Figura 8

Buenas Prácticas

Nota. Adaptada de Cómo crear contraseñas sólidas y otras maneras de proteger sus cuentas, por Consumidor, 2023 (https://consumidor.ftc.gov/articulos/como-crear-contrasenas-solidas-y-otras-maneras-de-proteger-sus-cuentas).

Además de la complejidad y longitud, es crucial evitar el uso de información personal fácilmente accesible, como nombres de familiares o fechas de nacimiento, pues los ciberdelincuentes suelen utilizar esta información para intentar descifrar las contraseñas. Otra recomendación es no reutilizar la misma contraseña en diferentes cuentas, ya que, si un atacante descubre una de ellas, tendría acceso a todas las demás. Finalmente, es aconsejable

actualizar regularmente las contraseñas, idealmente cada 60 días, lo que reduce el riesgo de que una contraseña comprometida se mantenga activa durante mucho tiempo (Axity, 2024). En este sentido, las contraseñas deben ser tan robustas que un ataque de fuerza bruta resulte imposible de realizar, lo que garantiza una mayor protección frente a los ciberdelincuentes (Infante Montero, 2013).

A pesar de seguir estas buenas prácticas, no es raro encontrar comportamientos inadecuados entre los usuarios. Muchos de ellos optan por almacenar sus contraseñas en lugares poco seguros, como notas en sus dispositivos o incluso en papel. Esto facilita el acceso no autorizado a la información, lo que pone en riesgo no solo sus cuentas personales, sino también la seguridad de las organizaciones a las que pertenecen. La recomendación es utilizar gestores de contraseñas, que permiten almacenar y gestionar múltiples claves de forma segura, o bien recurrir a la memoria, que aunque menos práctica, sigue siendo una opción válida en ciertos casos (Axity, 2024).

3.4.2. Problemas Comunes y Malos Hábitos de los Usuarios

Una de las mayores amenazas para la seguridad digital es el comportamiento del usuario. A pesar de los avances en la protección de contraseñas, los errores humanos siguen siendo uno de los factores más críticos que comprometen la seguridad. El uso de contraseñas débiles o predecibles, la reutilización de contraseñas en múltiples plataformas y la falta de actualización regular son prácticas que ponen en peligro la seguridad de la información. Los ciberdelincuentes aprovechan estas debilidades para realizar ataques de fuerza bruta, phishing y otros tipos de ciberataques que, en muchos casos, podrían haberse evitado con medidas básicas de precaución (Goujon, 2013).

El phishing, por ejemplo, sigue siendo una de las principales formas de ataque utilizadas por los ciberdelincuentes para obtener credenciales de acceso. Este tipo de fraude electrónico se basa en la suplantación de una entidad legítima para engañar a la víctima y obtener sus datos confidenciales. A pesar de la creciente conciencia sobre este tipo de ataques, muchos usuarios continúan cayendo en trampas de phishing, lo que demuestra la necesidad de mayor educación y conciencia sobre las buenas prácticas en seguridad digital (Goujon, 2013). Asimismo, los usuarios suelen subestimar la importancia de actualizar regularmente sus contraseñas, lo que facilita que los ciberdelincuentes puedan acceder a sus cuentas mediante ataques que, aunque básicos, siguen siendo altamente efectivos en la actualidad.

Un aspecto igualmente preocupante es el almacenamiento inadecuado de las contraseñas. A pesar de que existen soluciones tecnológicas como los gestores de contraseñas, que permiten mantener las claves seguras y organizadas, muchos usuarios continúan optando por métodos inseguros, como escribir sus contraseñas en papel o guardarlas en archivos sin protección. Esto aumenta el riesgo de que terceros accedan a esa información, comprometiendo no solo las cuentas personales, sino también los sistemas corporativos. En este sentido, es imprescindible fomentar el uso de herramientas seguras para la gestión de contraseñas y promover una mayor conciencia sobre la importancia de proteger adecuadamente las credenciales de acceso (Axity, 2024).

Finalmente, los ciberdelincuentes también han desarrollado malware específico para robar contraseñas de usuarios y empresas, como en el caso del gusano Dorkbot, que logró infectar más de 80,000 computadoras y robar 1,500 cuentas de correo corporativo en América Latina. Este tipo de ataques demuestran que las contraseñas siguen siendo un objetivo prioritario para los ciberdelincuentes, y que las empresas deben tomar medidas adicionales,

como la implementación de la autenticación multifactor, para mitigar el riesgo de robo de credenciales y garantizar la seguridad de sus sistemas (Goujon, 2013).

3.5. Autenticación

La autenticación es el proceso mediante el cual se verifica la identidad de un usuario, sistema o dispositivo antes de otorgar acceso a un recurso o servicio. Este proceso es esencial para garantizar la seguridad en el ámbito digital, ya que permite confirmar que la persona o entidad que intenta acceder a información o sistemas es quien dice ser. La autenticación es uno de los pilares fundamentales de la ciberseguridad moderna, y su importancia ha crecido en paralelo con el aumento de las amenazas cibernéticas. En el contexto actual, donde los datos son uno de los activos más valiosos, el uso de mecanismos de autenticación robustos se ha convertido en una necesidad ineludible para proteger la privacidad y la integridad de la información. Estos mecanismos pueden variar en complejidad y efectividad, dependiendo del tipo de autenticación implementada y de las tecnologías involucradas (Microsoft, s. f.).

Figura 9

Autenticación

Nota. Adaptada de ¿Cómo funciona la autenticación de dos factores (2FA)?, por Molinari, D, 2022 (https://www.avast.com/es-es/c-how-does-two-factor-authentication-work).

El crecimiento del entorno digital ha traído consigo nuevos retos en cuanto a la protección de la información. La autenticación no solo se centra en permitir o denegar el acceso, sino en garantizar que las credenciales presentadas sean legítimas. Existen varios tipos de autenticación, desde las más tradicionales, como el uso de contraseñas, hasta métodos más avanzados que involucran biometría o autenticación multifactor. Las contraseñas, aunque siguen siendo el método más común, han demostrado ser vulnerables debido a las malas prácticas de los usuarios, como la reutilización o la creación de contraseñas débiles. A pesar de los esfuerzos por concienciar a los usuarios sobre la importancia de crear contraseñas seguras, muchas personas continúan utilizando combinaciones simples, lo que facilita los ataques cibernéticos (Townsend, 2020).

El uso de contraseñas por sí solo presenta vulnerabilidades inherentes, como los ataques de fuerza bruta, en los que un atacante intenta todas las combinaciones posibles hasta encontrar la correcta. Para mitigar estos riesgos, una clave debe ser lo suficientemente grande para que un ataque de fuerza bruta sea prácticamente imposible (Townsend, 2020). No obstante, la autenticación basada en contraseñas sigue siendo una medida insuficiente para garantizar la seguridad digital en muchos escenarios, lo que ha llevado a la adopción de soluciones más sofisticadas.

3.5.1. Métodos de autenticación

La autenticación puede llevarse a cabo de diversas maneras. El método más básico es el de "algo que el usuario sabe", generalmente una contraseña o un PIN. A pesar de su uso extendido, este método tiene debilidades bien documentadas, como la facilidad con la que los atacantes pueden adivinar o robar credenciales. En este sentido, la autenticación multifactor

(MFA) ha surgido como una solución más segura. El MFA combina varios factores de autenticación, como algo que el usuario sabe (contraseña), algo que el usuario tiene (un token o dispositivo) y algo que el usuario es (datos biométricos, como huellas dactilares o reconocimiento facial). Este enfoque aumenta significativamente la seguridad al requerir múltiples capas de verificación para acceder a un sistema o cuenta (Microsoft, s. f.).

Figura 10

Autenticación por Token

Nota. Adaptada de Tipos de Autenticación: Contraseña, Token, JWT, Dos Factores y Más, por Bessa, D, 2023 (https://www.aluracursos.com/blog/assets/tipos-de-autenticacion/img7.png).

Otro enfoque es la autenticación biométrica, que utiliza características físicas o de comportamiento de un individuo, como la huella dactilar, el reconocimiento facial o la geometría de la mano, para verificar su identidad. Estos métodos son difíciles de falsificar, ya que dependen de atributos únicos e inherentes a cada persona. Sin embargo, la autenticación biométrica también tiene sus desventajas, como los problemas relacionados con la privacidad y la dificultad para cambiar credenciales biométricas en caso de que sean comprometidas (Bessa, 2023).

En el panorama actual de ciberseguridad, la autenticación basada en riesgos también está cobrando relevancia. Este método evalúa el contexto en el que se realiza el intento de autenticación, como la ubicación del usuario, la hora del día y el dispositivo utilizado, para determinar si se trata de una solicitud legítima. Si el sistema detecta una anomalía, puede requerir una verificación adicional para garantizar la autenticidad del usuario. Este enfoque permite un equilibrio entre seguridad y usabilidad, ofreciendo una capa adicional de protección sin añadir fricciones innecesarias para el usuario (Bessa, 2023).

La evolución de los métodos de autenticación ha sido impulsada por la creciente necesidad de proteger datos sensibles y evitar filtraciones. La autenticación de dos factores (2FA) y la autenticación multifactor han ganado popularidad debido a su capacidad para reforzar la seguridad al exigir más de un método de verificación. Además, el uso de tecnologías emergentes, como la autenticación sin contraseñas, está ganando terreno, lo que sugiere que las contraseñas podrían quedar obsoletas en un futuro cercano (Townsend, 2020).

La autenticación es un componente esencial en la ciberseguridad y sigue evolucionando para hacer frente a las amenazas cambiantes del entorno digital. A medida que los métodos de autenticación se vuelven más sofisticados, las organizaciones y los individuos deben mantenerse al día con las mejores prácticas para garantizar la protección de sus activos más valiosos. Aunque las contraseñas han sido el método predominante durante décadas, su vulnerabilidad ha dado paso a soluciones más seguras, como la autenticación multifactor y la biometría. Sin embargo, ninguna solución es completamente infalible, lo que resalta la importancia de seguir desarrollando e implementando nuevas tecnologías de autenticación para garantizar la seguridad en un mundo cada vez más interconectado (Microsoft, s. f.).

4. Marco Metodológico

4.1. Metodología de Investigación

“La metodología de la investigación es la disciplina que se encarga de definir, clasificar y sistematizar al conjunto de técnicas y sistemas que se utilizan en una investigación científica determinada” (Raffino, 2024). En otras palabras, es el enfoque organizado que guía el proceso de recolección y análisis de información en una investigación, asegurando que se apliquen técnicas adecuadas y se mantenga un orden lógico en cada etapa.

4.1.1. Diseño de Investigación

Dado que se busca analizar cómo influye el uso de un generador de contraseñas en la reducción de prácticas inseguras, así como los objetivos trazados, se recurrió a un enfoque exploratorio para descubrir comportamientos y prácticas actuales, complementado con un análisis descriptivo que permita establecer una base sólida para el desarrollo del prototipo.

De acuerdo con Ortiz (2020) la investigación exploratoria “corresponde al primer acercamiento a un tema específico antes de abordarlo en un trabajo investigativo más profundo. Se trata de un proceso para tener información básica relacionada con el problema de investigación”. Así mismo Kiss (2024) señala que una investigación descriptiva “es aquella que tiene como objetivo especificar las propiedades del fenómeno que se estudia. En este tipo de investigaciones, se describen situaciones, eventos o fenómenos para ofrecer un panorama claro y completo del tema, que puede servir de base para otras investigaciones posteriores”.

4.1.2. Enfoque de la investigación

El presente trabajo será diseñado bajo el planteamiento metodológico con un enfoque mixto (cuantitativo y cualitativo), puesto que se adapta a las características y necesidades de la investigación para identificar y contextualizar las prácticas inseguras de los usuarios.

Figura 11

Investigación Mixta

Nota. Adaptada de Investigación mixta. Qué es y tipos que existen, por Ortega, C, 2021 (https://www.questionpro.com/blog/wp-content/uploads/2021/04/Portada-investigacion-mixta.jpg).

El enfoque mixto utiliza la recolección, el análisis e integración tanto de la investigación cuantitativa como cualitativa. Los datos cuantitativos “incluyen información cerrada como la que se utiliza para medir actitudes, por ejemplo, escalas de puntuación.” (Ortega, 2021). Así mismo

Ortega (2021) nos indica que los datos cualitativos “son información abierta que el investigador suele recopilar mediante entrevistas, grupos de discusión y observaciones”.

Para la obtención de datos relevantes en el marco de este proyecto, se emplearán dos técnicas principales de recolección de información, que será la encuesta y la revisión documental. Ambas técnicas permitirán reunir datos cualitativos y cuantitativos, proporcionando una visión integral de las prácticas actuales de los usuarios en cuanto a la seguridad de contraseñas y la importancia de utilizar contraseñas fuertes.

4.1.3. Recolección de Datos

La encuesta consistirá en un cuestionario estructurado que se aplicará a un grupo aleatorio de usuarios entre los 18 y 60 años. Este cuestionario tiene como objetivo principal recopilar información sobre las prácticas actuales y el nivel de conocimiento de los usuarios respecto a la seguridad de contraseñas.

El enfoque de la encuesta será explorar aspectos como: la frecuencia de reutilización de contraseñas entre diferentes plataformas, la adopción de prácticas seguras (por ejemplo, el uso de combinaciones de caracteres complejas), la percepción de los usuarios sobre la importancia de contar con contraseñas robustas, la frecuencia con la que los usuarios cambian o actualizan sus contraseñas y el conocimiento de herramientas de gestión de contraseñas y la percepción de su utilidad.

Los resultados de la encuesta permitirán identificar comportamientos y prácticas comunes en el manejo de contraseñas, así como las áreas donde los usuarios pueden tener deficiencias o falta de conocimiento. Esta información servirá de base para el desarrollo del

prototipo del generador de contraseñas, enfocándose en aquellas funcionalidades que puedan mejorar la seguridad y usabilidad para los usuarios.

Además de la encuesta, se llevará a cabo una revisión documental con el fin de contextualizar y profundizar con la información. La revisión se centrará en el análisis de fuentes secundarias, tales como estudios, informes y artículos académicos que traten sobre la seguridad de contraseñas, generación de contraseñas fuertes y las mejores prácticas en el manejo de contraseñas.

Los principales objetivos de esta revisión documental son: identificar las técnicas recomendadas por expertos para la generación de contraseñas seguras, analizar las estrategias que se consideran efectivas para fomentar el uso de contraseñas robustas, examinar estudios previos sobre la efectividad de los generadores de contraseñas y su influencia en la mejora de la seguridad de los usuarios, y recopilar recomendaciones sobre las características que debería tener un generador de contraseñas efectivo y accesible para los usuarios comunes.

Esta revisión permitirá alinear las funcionalidades del prototipo con las recomendaciones y tendencias actuales en cuanto a seguridad de contraseñas, asegurando que el diseño del generador no solo satisfaga las necesidades de los usuarios, sino que también esté fundamentado en prácticas comprobadas y respaldadas por la investigación.

4.1.4. Instrumentos de Recolección de Datos

Para llevar a cabo las técnicas de recolección descritas, se utilizarán dos instrumentos principales: un cuestionario estructurado y fuentes documentales relevantes.

El cuestionario estructurado será el instrumento empleado para la encuesta. Este documento estará compuesto por una serie de preguntas cerradas, diseñadas para obtener información detallada sobre las prácticas y percepciones de los usuarios en cuanto a la seguridad de contraseñas. Se incluirán preguntas de opción múltiple y escala de Likert que permitan obtener los datos necesarios. La estructura del cuestionario asegurará que se aborden todos los aspectos relevantes de la seguridad de contraseñas, proporcionando una base sólida para el análisis y el desarrollo del prototipo.

Como complemento al cuestionario, se realizará una búsqueda de fuentes documentales y artículos especializados que aborden la temática de seguridad de contraseñas. Entre las fuentes a considerar se incluyen estudios académicos, informes de organismos de seguridad informática, libros y artículos publicados en revistas científicas. Estas fuentes permitirán contextualizar los datos obtenidos en la encuesta y aportar una base teórica sólida sobre la importancia de las contraseñas seguras y las prácticas recomendadas para su creación y uso. La combinación de estos instrumentos garantizará que el prototipo esté diseñado no solo en función de las necesidades y prácticas actuales de los usuarios, sino también con base en recomendaciones y estándares reconocidos en la industria.

4.1.5. Análisis de Datos y Procesamiento de Datos

Para llevar a cabo la recolección de los datos que se obtendrán de la encuesta se utilizará la herramienta Google Forms, mientras que la revisión documental se gestionará y recopilará mediante Zotero.

La encuesta permitirá un análisis cuantitativo enfocado en identificar patrones de comportamiento y percepciones de los usuarios con relación a la seguridad de sus contraseñas. La elección de preguntas cerradas facilita la recopilación de datos estructurados y claros, permitiendo identificar rápidamente tendencias en las prácticas de los usuarios.

Los datos cuantitativos se analizarán mediante gráficos generados automáticamente por Google Forms, tales como gráficos de barras y gráficos de torta. Estos gráficos ofrecerán una representación visual de la información, lo cual ayudará a:

1. Identificar la frecuencia con la que los usuarios reutilizan contraseñas.

2. Medir el nivel de acuerdo de los usuarios sobre sus propias prácticas de seguridad, a través de la escala de Likert.

Complementariamente la revisión documental será gestionada a través de Zotero, una herramienta que permite almacenar y categorizar documentos relevantes de manera organizada y eficiente. Este análisis cualitativo proporcionará:

1. Información sobre las mejores prácticas en la creación de contraseñas seguras.

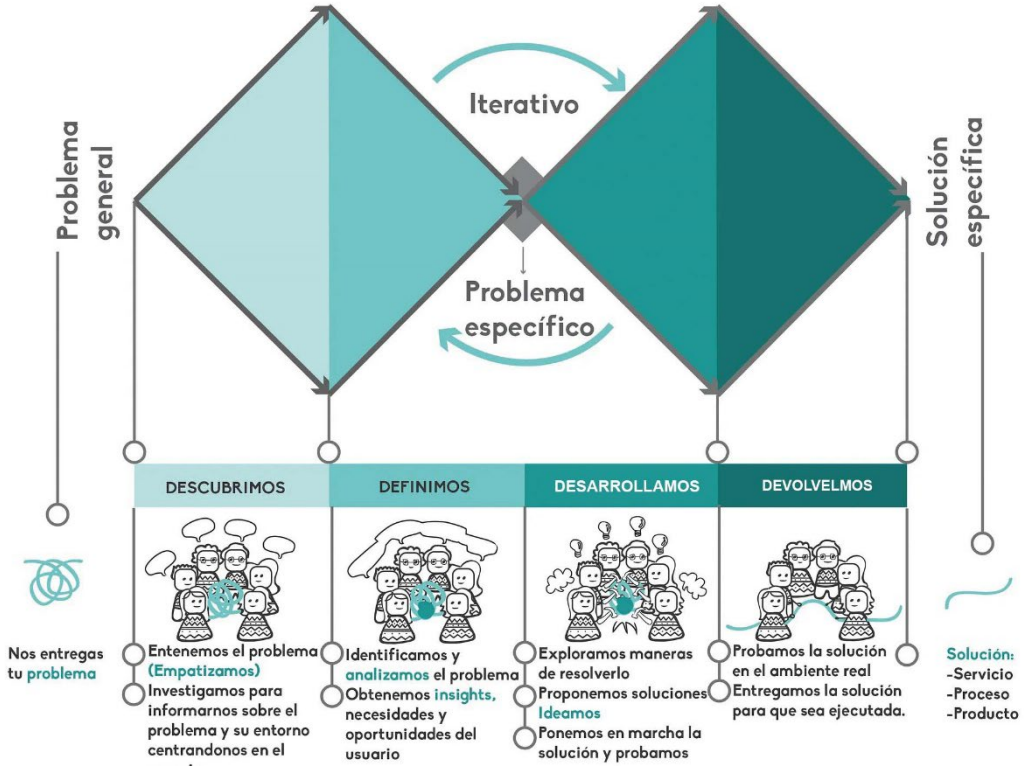
2. Análisis de problemas comunes en la gestión de contraseñas.

El uso de Zotero facilitará el acceso a fuentes documentales, permitiendo la comparación de estas prácticas recomendadas con los datos obtenidos de la encuesta, y contribuyendo a la identificación de requisitos específicos para el desarrollo del prototipo.

4.2. Metodología de Desarrollo (Metodología Doble Diamante)

Figura 12

Diamante Doble



Nota. Adaptada de Design Thinking EMT Madrid, por Echávarri, B, 2018 (https://miro.medium.com/v2/resize:fit:2000/format:webp/1*dFOn9b0OuAPSYVjTQY0AtA.jpeg).

La metodología doble diamante es una metodología de diseño e innovación, que pueden seguir tanto diseñadores como no diseñadores para encontrar soluciones a problemas complejos que respondan a las necesidades de las personas (GammaUX, 2020). Es un método estructurado en cuatro fases: Descubrimiento, Definición, Desarrollo y Entrega. Este método permite un enfoque iterativo y cíclico, asegurando que el prototipo cumpla con los objetivos de mejorar las prácticas de los usuarios en cuanto a la seguridad de sus contraseñas.

4.2.1. Fase de Descubrimiento

Es un proceso de búsqueda ampliada en la que el emprendedor (dueño de la idea), indaga o investiga acerca de un determinado tema que lo motiva (Castillo, 2019). En este proyecto esta fase tiene como propósito identificar las prácticas inseguras comunes en la creación y gestión de contraseñas entre los usuarios y a partir de esto, definir los requisitos que debe cumplir el generador de contraseñas.

- Se llevarán a cabo encuestas para recopilar información sobre los hábitos y conocimientos de los usuarios respecto a la seguridad de contraseñas, enfocándose en prácticas inseguras, como la reutilización de contraseñas.

- Se realizará una revisión documental de estudios previos sobre la seguridad de contraseñas, empleando Zotero para la organización de estas fuentes.

Este análisis permitirá guiar el diseño del generador, alineándolo con las necesidades de los usuarios y recomendaciones de buenas prácticas en seguridad de contraseñas.

4.2.2. Fase de Definición

Es un proceso de elección o selección de los resultados de la búsqueda ampliada, tratando de escribir y reescribir la forma en que los resultados de la búsqueda se enlazan. El resultado de estas dos fases dará por resultado la idea específica de negocio o solución creativa (Castillo, 2019). En el enfoque del proyecto este consiste en especificar las funcionalidades clave del generador de contraseñas, orientadas a facilitar la creación de contraseñas seguras de manera sencilla y accesible.

Con base en los datos recopilados en la Fase de Descubrimiento, se definirán:

- Las características principales del generador, tales como la posibilidad de generar contraseñas con distintas combinaciones de caracteres y permitir al usuario copiar la contraseña generada.

- La aplicación además de la generación de contraseñas, podría permitir copiarlas en el portapapeles del usuario.

Este establecerá los elementos clave que la aplicación debe incluir para responder eficazmente a los problemas identificados, como la personalización de la longitud y complejidad de las contraseñas.

4.2.3. Fase de Desarrollo

Esta fase se trata de convertir la idea específica en algo realizable (Castillo, 2019). Bajo esta definición en este proyecto se implementará la aplicación utilizando HTML, CSS y JavaScript, asegurando que cumpla con los principios básicos de usabilidad y seguridad para la generación de contraseñas.

- Se construirá una interfaz intuitiva mediante HTML y CSS.

- La funcionalidad de generación de contraseñas se desarrollará con JavaScript, enfocada en las necesidades descubiertas para los usuarios.

Durante esta fase, se realizarán pruebas de usabilidad para verificar que la aplicación cumple con los requisitos definidos y que la generación de contraseñas es eficiente y segura.

4.2.4. Fase de Entrega

Es ver cómo responde el diseño a pequeña escala, sin grandes gastos, lo mínimo posible. Ese será el producto o resultado de la metodología propuesta. Si este prototipo funciona, se harán los ajustes que se crean convenientes, y se procederá a escalar (Castillo, 2019). Esta fase en el proyecto se aplicará y se enfocará en la validación final de la aplicación y en asegurar que responde efectivamente a las necesidades de los usuarios detectadas en la Fase de Descubrimiento.

- Se realizarán pruebas de validación para confirmar que el generador cumple con los objetivos trazados.

- La documentación final del proyecto incluirá los detalles del proceso de desarrollo, los beneficios del generador en cuanto a la mejora de prácticas de seguridad de contraseñas, y cómo su simplicidad facilita el uso de contraseñas más seguras.

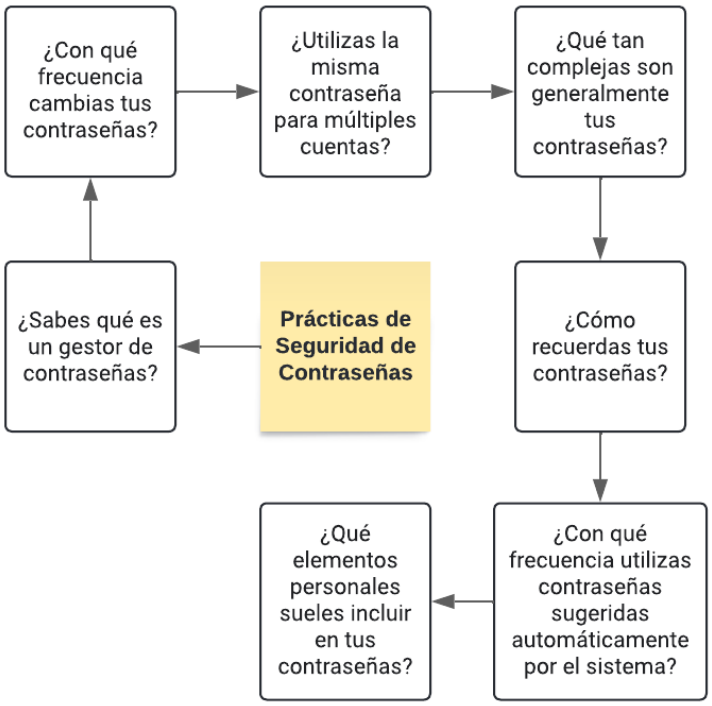
5. Resultados

5.1. Fase de Descubrimiento

En esta fase se exploran y entienden en profundidad las prácticas de seguridad de contraseñas entre los usuarios, incluyendo el uso de gestores de contraseñas, el conocimiento general sobre contraseñas seguras y los comportamientos de riesgo en la gestión de contraseñas. A partir de la encuesta realizada, y con un análisis documental, se identifican problemas y oportunidades de mejora en la seguridad de las contraseñas que guiarán el desarrollo del prototipo de un generador de contraseñas fuertes.

Figura 13

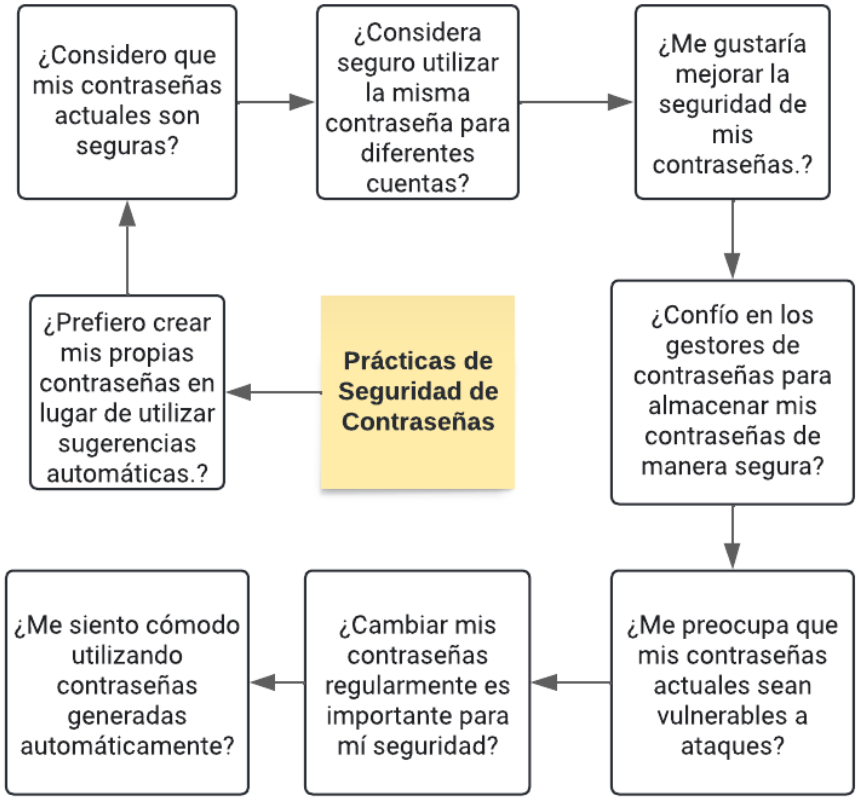
Encuesta



Nota. Fuente: El autor.

Figura 14

Escala Likert



Nota. Fuente: El autor.

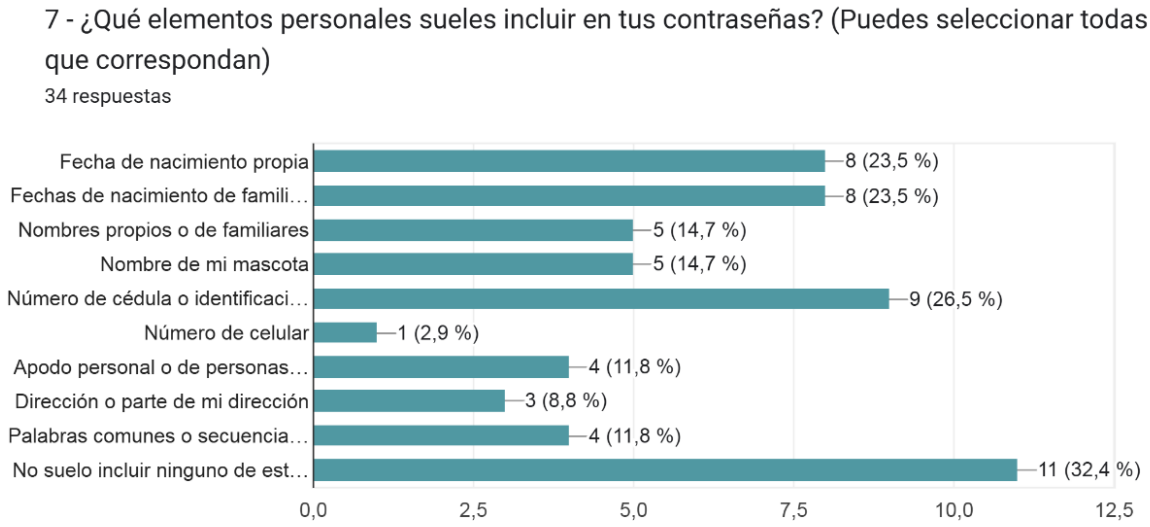
5.1.1. Identificación de prácticas inseguras

Los resultados de la encuesta revelaron que muchos usuarios aún incluyen elementos personales en sus contraseñas, tales como fechas de nacimiento, nombres de mascotas, números de identificación y números de teléfono. Estos datos personales pueden ser fácilmente identificables, lo que incrementa el riesgo de exposición a ataques de fuerza bruta y otras vulnerabilidades. Alrededor de un 30% de los encuestados afirmaron que utilizan elementos relacionados con su vida personal en la creación de contraseñas, lo que demuestra un hábito que va en contra de las buenas prácticas de seguridad. Esta práctica es

problemática, pues los atacantes pueden fácilmente acceder a este tipo de información en redes sociales u otros canales públicos, exponiendo a los usuarios a ataques de fuerza bruta y de diccionario (Kaspersky, 2020). Además, una parte significativa de los participantes indicó que reutiliza contraseñas en múltiples plataformas, lo que incrementa la vulnerabilidad de todas las cuentas del usuario si una de ellas es comprometida.

Figura 15

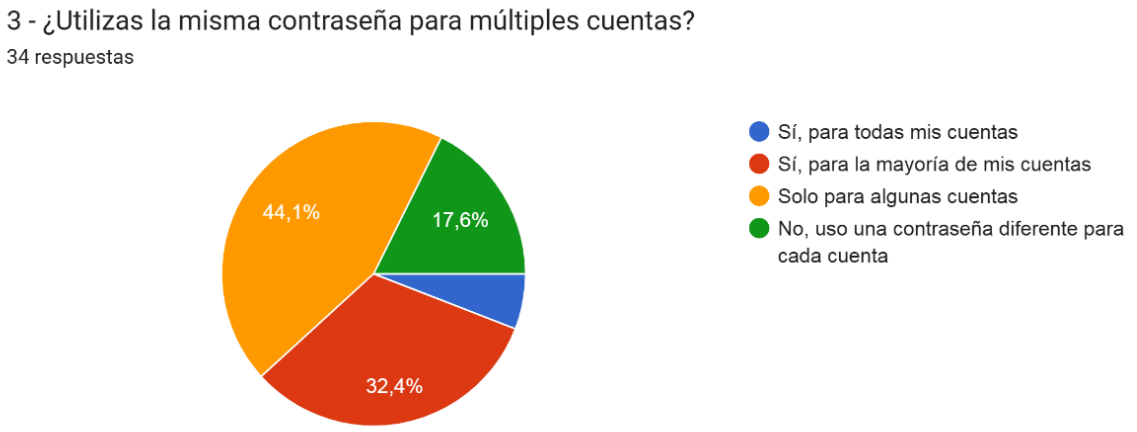
Elementos Personales en Contraseñas



Nota. Fuente: El autor.

Figura 16

Usos Contraseñas



Nota. Fuente: El autor.

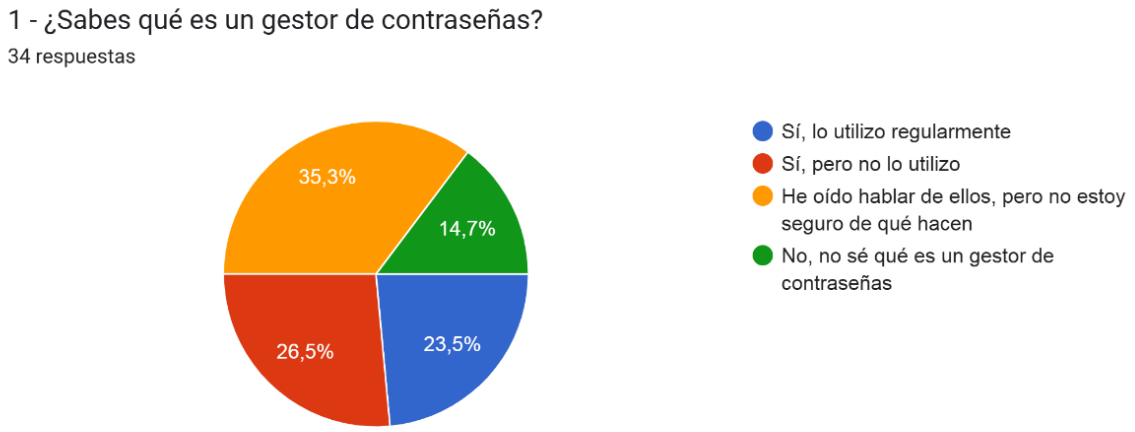
5.1.2. Conocimiento y uso de gestores de contraseñas

En cuanto al conocimiento sobre los gestores de contraseñas, un porcentaje significativo de los participantes indicó que nunca ha utilizado uno. Además, aunque el 26% de los encuestados afirmó conocer lo que es un gestor de contraseñas, expresaron no tener confianza suficiente para utilizarlos. Estos hallazgos sugieren que, aunque algunos usuarios están conscientes de la existencia de herramientas que pueden ayudar a mejorar la seguridad de sus contraseñas, la desconfianza y el desconocimiento limitan su adopción. Este desconocimiento podría explicarse en parte por la falta de recursos educativos accesibles, así como la percepción de que las contraseñas largas y complejas son difíciles de recordar. Sin embargo, estudios de Kaspersky destacan que los gestores de contraseñas no solo generan contraseñas aleatorias y seguras, sino que también simplifican la experiencia del usuario al

guardar y recordar estas contraseñas (Kaspersky, 2020). Esta herramienta podría ser esencial en un proyecto que busque mejorar las prácticas de seguridad entre los usuarios, promoviendo la adopción de contraseñas fuertes y únicas sin la carga de recordarlas.

Figura 17

Gestor Contraseñas



Nota. Fuente: El autor.

Este análisis de la fase evidencia una falta de conocimientos y prácticas seguras entre los usuarios en relación con sus contraseñas. El desconocimiento de los gestores de contraseñas y la preferencia por contraseñas basadas en datos personales resaltan la necesidad de una solución sencilla, que facilite la creación de contraseñas seguras y evite la reutilización. Esta fase concluye con la identificación de una oportunidad para desarrollar una aplicación de generador de contraseñas fuertes, enfocado en promover prácticas de seguridad digital accesibles y eficaces para los usuarios.

5.2. Fase de Definición

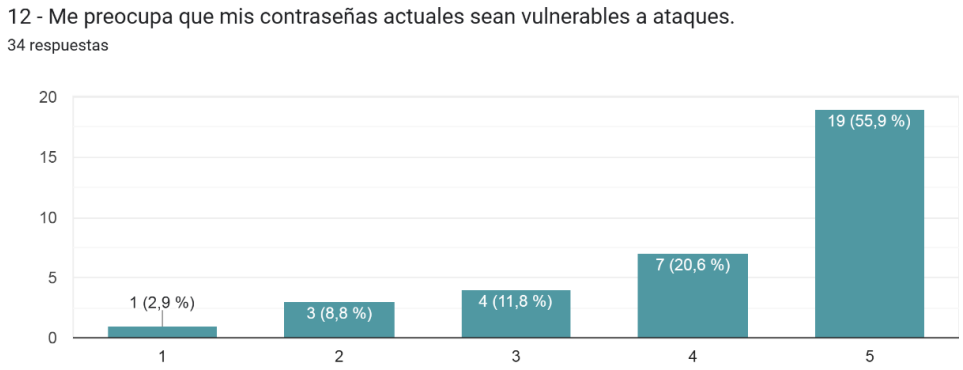
Con base en los hallazgos de la fase de descubrimiento, se delimitó claramente el problema principal a abordar con el desarrollo de un generador de contraseñas. Esta fase permitió definir los retos específicos a enfrentar, centrándose en mejorar la adopción de prácticas seguras y reducir la reutilización de contraseñas inseguras entre los usuarios.

5.2.1. Detección de preocupaciones y actitudes

Los datos de la escala de Likert reflejaron una gran preocupación por la seguridad de contraseñas entre los usuarios, con una media superior a 4 en el nivel de preocupación por la vulnerabilidad de las contraseñas. Sin embargo, a pesar de este alto nivel de preocupación, también se observó una resistencia hacia la adopción de gestores de contraseñas. La encuesta reveló que los usuarios prefieren crear sus propias contraseñas, sintiéndose más cómodos con contraseñas que consideran personalizadas y fáciles de recordar.

Figura 18

Preocupación de Vulnerabilidad



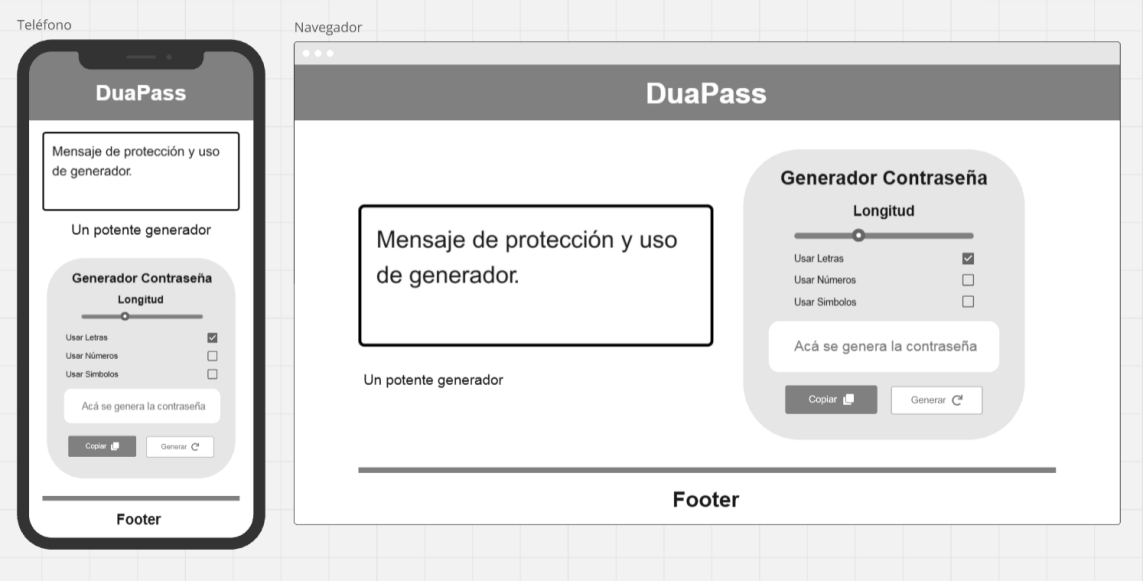
Nota. Este gráfico corresponde a la precesión de los usurarios donde 1 = Muy en desacuerdo, 2 = Desacuerdo, 3 = Indiferente, 4 = De acuerdo y 5 = Muy de acuerdo, Fuente: El autor.

Este análisis identificó una necesidad clave de ofrecer una herramienta que permita a los usuarios generar contraseñas fuertes de forma rápida y personalizada, sin depender de gestores de contraseñas externos que puedan percibir como inseguros. La herramienta propuesta se enfocará en educar a los usuarios sobre la importancia de las prácticas seguras, al mismo tiempo que les facilita la creación de contraseñas que se adapten a sus preferencias y necesidades.

5.2.2. Definición del problema y requisitos del prototipo

Figura 19

Maqueta Diseños



Nota. Fuente: El autor.

La encuesta reveló que muchos usuarios tienen hábitos de creación de contraseñas poco seguros, como el uso de información personal y la reutilización de contraseñas en distintas cuentas. Estos resultados subrayan la importancia de que el generador de

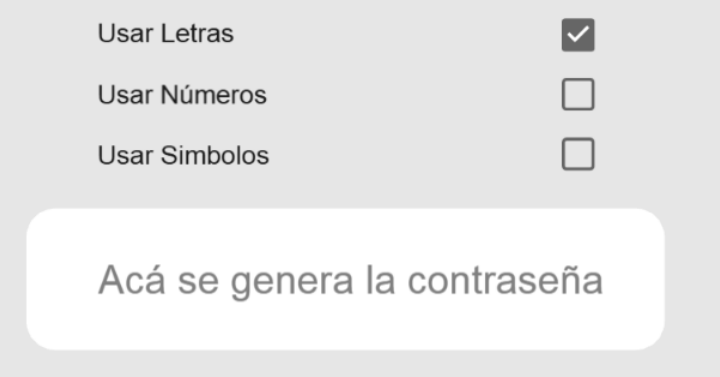
contraseñas incluya una función que permita crear contraseñas aleatorias, con una mezcla de caracteres alfanuméricos y símbolos, tal como lo sugieren las recomendaciones de ciberseguridad (Comillas, 2024; Stackscale, 2022). Además, dado el desconocimiento de los gestores de contraseñas y la desconfianza de los usuarios a usarlos, la aplicación deberá facilitar el copiado rápido de las contraseñas generadas y garantizar una experiencia amigable.

La solución propuesta se enfoca en el desarrollo de un generador que cumpla con las siguientes características:

1. Generación Aleatoria de Contraseñas: Implementar un algoritmo que genere contraseñas robustas, mezclando letras, números y símbolos, para cumplir con las buenas prácticas de seguridad digital.

Figura 20

Parámetros Contraseña

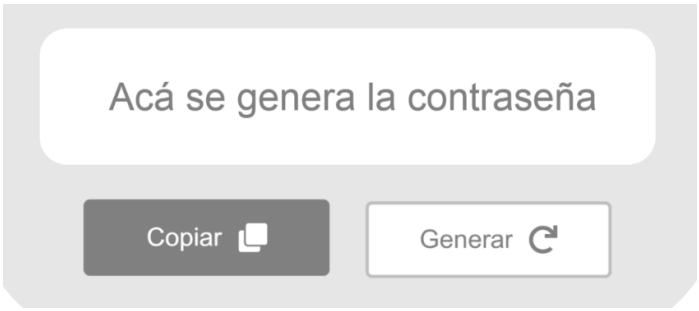


Nota. Fuente: El autor.

2. Simplicidad de Uso: Dado que muchos usuarios desconocen las herramientas de gestión de contraseñas, el prototipo debe ser sencillo de utilizar, permitiendo copiar las contraseñas generadas en un solo clic.

Figura 21

Botón Copiar y Generar



Nota. Fuente: El autor.

3. Flexibilidad en los Parámetros de Generación: Ofrecer opciones para ajustar la longitud y complejidad de la contraseña, adaptándose a las necesidades de seguridad de cada usuario.

Figura 22

Longitud Contraseña

Nota. Fuente: El autor.

El análisis de las prácticas de los usuarios y de las recomendaciones de seguridad en la documentación han permitido definir los requisitos para un prototipo efectivo de generador de contraseñas fuertes. Esta herramienta buscará no solo generar contraseñas seguras, sino

también guiar a los usuarios en la adopción de mejores prácticas de seguridad digital, abordando la problemática de manera práctica y educativa.

5.3. Fase de Desarrollo

En esta fase se concreta el prototipo de un generador de contraseñas seguro, accesible y funcional. El diseño de esta herramienta busca no solo brindar una solución de seguridad, sino también promover una cultura de prácticas seguras entre los usuarios al facilitarles la generación de contraseñas robustas y educarlos sobre su importancia.

Esta fase se orienta a cumplir con los requisitos identificados previamente, que guiarán cada aspecto de la construcción del generador:

Implementar un generador de contraseñas seguro y configurable: Basándonos en las mejores prácticas de ciberseguridad identificadas, el generador permitirá a los usuarios personalizar sus contraseñas según sus necesidades. Incluirá opciones para seleccionar el tipo y número de caracteres, combinando letras, números y símbolos especiales. Este enfoque responde a la necesidad de contraseñas fuertes y únicas, proporcionando una alternativa a las contraseñas débiles o repetidas, que fueron identificadas como prácticas comunes en la fase de Descubrimiento.

Tabla 2

Código HTML Longitud Contraseña

```
<div class="generator__container--length">
  <label>Longitud</label>
  <div class="length">
    <input type="range" value="8" min="1" max="60" class="length__slider"
    oninput="this.nextElementSibling.value = this.value" id="length__slider">
    <output for="length__slider">8</output>
  </div>
</div>
```

Nota. Fuente: El autor.

Tabla 3

Código HTML Opciones Contraseña

```
<div class="options__items">
  <label for="options__items--letters">Usar Letras</label>
  <input type="checkbox" id="options__items--letters">
</div>
<div class="options__items">
  <label for="options__items--numbers">Usar Números</label>
  <input type="checkbox" id="options__items--numbers">
</div>
<div class="options__items">
  <label for="options__items--symbols">Usar Símbolos</label>
  <input type="checkbox" id="options__items--symbols">
</div>
```

Nota. Fuente: El autor.

Tabla 4

Código JavaScript Generar Contraseña

```
function generatePassword() {
  const length = parseInt(lengthSlider.value);
  const letters = useLetters.checked
    ? "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
    : "";
  const numbers = useNumbers.checked ? "0123456789" : "";
  const symbols = useSymbols.checked ? "!@#$%^&*()_+-=[]{}|;:,.<>?/" : "";
```

```
8
9       const allCharacters = letters + numbers + symbols;
10
11      let password = "";
12      for (let i = 0; i < length; i++) {
13        const randomIndex = Math.floor(Math.random() * allCharacters.length);
14        password += allCharacters[randomIndex];
15      }
16
17      viewOutput.textContent = password;
18    }
```

Nota. Fuente: El autor.

Crear una interfaz intuitiva y accesible: La interfaz gráfica será sencilla e intuitiva, asegurando que el generador sea fácil de usar para todo tipo de usuarios. La simplicidad y claridad de la interfaz no solo facilitarán la generación y copia de contraseñas, sino que también eliminarán las barreras de uso comúnmente asociadas con herramientas de seguridad. Este aspecto fue resaltado como crucial en los resultados de la encuesta, ya que muchos usuarios indicaron que una de las razones para no utilizar gestores de contraseñas es la falta de familiaridad o desconfianza hacia tecnologías complejas.

Tabla 5

Código CSS Hoja de Estilos de la Página

```
1       .generator__container--title {
2         display: flex;
3         justify-content: center;
4         align-items: center;
5         width: 70%;
6         height: 6rem;
7         margin: 0 auto;
8         background-color: var(--primary-color);
9         border-top-left-radius: 2rem;
10        border-top-right-radius: 2rem;
11        color: var(--secundary-color);
12      }
13      .generator__container {
```

```
    display: flex;
    flex-direction: column;
    width: 70%;
    height: 45rem;
    padding: 0 3rem;
    margin: 0 auto;
    border-bottom-left-radius: 2rem;
    border-bottom-right-radius: 2rem;
    background-color: white;
    color: var(--secundary-color);
    box-shadow: 0 4px 20px rgba(0, 0, 0, 0.1);
  }
  .generator__container--length,
  .generator__container--view,
  .generator__container--options,
  .generator__container--buttons {
    display: flex;
    justify-content: center;
    align-items: center;
    height: 25%;
  }
  .generator__container--length {
    flex-direction: column;
    border-bottom: .1rem solid var(--secundary-color);
  }
  .length {
    display: flex;
    align-items: center;
    gap: 2rem;
    width: 100%;
    margin-top: 2rem;
  }
  .length__slider {
    -webkit-appearance: none;
    width: 100%;
    height: .5rem;
    border-radius: .5rem;
    background: var(--primary-color);
  }
  .length__slider::-webkit-slider-thumb {
    -webkit-appearance: none;
    width: 2rem;
    height: 2rem;
    border-radius: 50%;
    background-color: var(--secundary-color);
    cursor: pointer;
  }
```

Nota. Fuente: El autor.

Incluir funcionalidad educativa: Para cumplir el propósito educativo del proyecto, se añadirán consejos y explicaciones breves sobre la importancia de las contraseñas fuertes y los peligros de la reutilización de contraseñas. La funcionalidad de recordatorio se mostrará cada vez que el usuario genere una contraseña, subrayando prácticas seguras en ciberseguridad. De este modo, la aplicación no solo generará contraseñas, sino que también fomentará una mentalidad de seguridad en cada uso.

Tabla 6

Código HTML Mensajes

```
<section class="information">
  <div class="info__container">
    <p class="info__container--title">Crea contraseñas seguras y personalizadas en segundos.
    Protege tus cuentas con nuestro generador fácil de usar.</p>
    <p class="info__container--description">Un potente generador de contraseñas robustas para proteger tus cuentas en Internet.</p>
  </div>
</section>
```

Nota. Fuente: El autor.

5.3.1. Tecnologías y Enfoque Técnico

El prototipo será construido en HTML, CSS y JavaScript, aprovechando estas tecnologías para crear una aplicación web ligera, rápida y compatible con múltiples dispositivos. Cada tecnología cumple una función específica:

HTML: Estructura la aplicación y los elementos de la interfaz, garantizando una organización clara y accesible de los componentes principales.

CSS: Da estilo y diseño a la aplicación, asegurando una presentación visual atractiva y una experiencia de usuario coherente con los principios de usabilidad.

JavaScript: Implementa la lógica del generador de contraseñas, permitiendo la creación de contraseñas seguras y la configuración de diferentes opciones según las necesidades de cada usuario.

5.4. Fase de Entrega

En esta fase final, se presenta el generador de contraseñas en su versión completa, basado en los resultados de las fases previas. La fase de entrega tiene como objetivo proporcionar una herramienta funcional y fácil de usar, que responda a las necesidades identificadas en la fase de descubrimiento y cumpla con los requisitos definidos en la fase de definición.

Se ofrece a los usuarios un generador de contraseñas robusto que facilita la creación de contraseñas seguras sin necesidad de conocimientos avanzados en ciberseguridad. La herramienta es intuitiva, confiable y está respaldada por buenas prácticas de seguridad digital. Para asegurar su validez, se realizaron pruebas que comprueban el correcto funcionamiento de todas sus funcionalidades, como la generación de contraseñas, opciones de personalización y el botón de generar y copiar. Asimismo, se verificó que la interfaz cumpla con los estándares de usabilidad y accesibilidad, optimizando la experiencia del usuario en términos de facilidad de uso y efectividad.

Figura 23

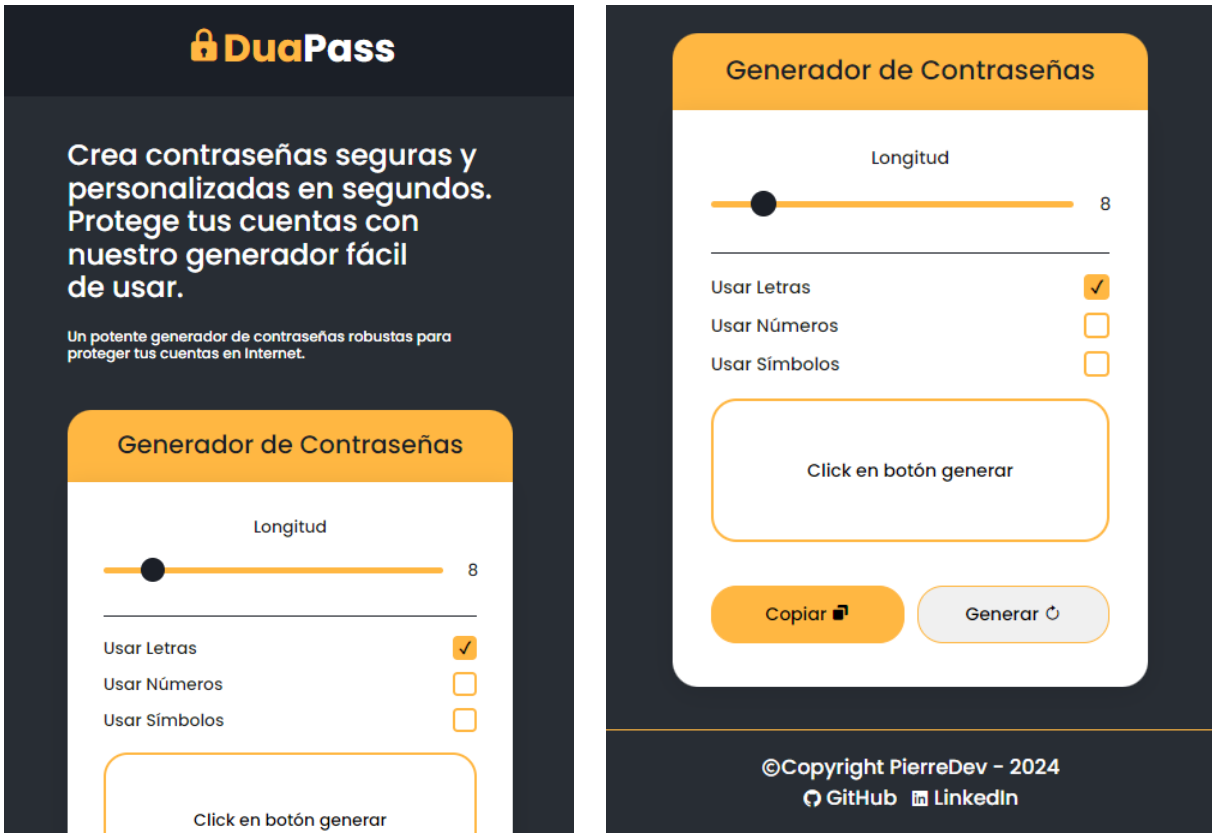
Generador de Contraseñas - Escritorio

Nota. Fuente: El autor.

La versión final del generador fue entregada en un entorno accesible para los usuarios, incorporando todos los ajustes identificados durante las fases de prototipado. Esta versión no solo brinda una experiencia simplificada, sino que también tiene un enfoque educativo, promoviendo prácticas de seguridad. La expectativa es que los usuarios adopten la herramienta para crear contraseñas seguras y personalizadas, disminuyendo la reutilización y el uso de información personal en sus contraseñas. Así, la herramienta no se presenta solo como un generador de contraseñas, sino también como una forma de sensibilizar a los usuarios sobre la importancia de proteger sus cuentas mediante prácticas seguras. Esta fase concluye con la puesta en marcha de la herramienta, alineada con los objetivos planteados y cumpliendo con su propósito de mejorar las prácticas de seguridad digital entre los usuarios.

Figura 24

Generador de Contraseñas - Mobile



Nota. Fuente: El autor.

Finalmente se incluye el enlace directo a la aplicación del generador de contraseñas, esta herramienta ha sido diseñada para que los usuarios puedan acceder de forma rápida y sencilla, asegurando una experiencia de uso intuitiva que fomente la adopción de prácticas seguras.

Puedes acceder al generador de contraseñas y comenzar a crear contraseñas seguras y personalizadas a través del siguiente enlace**: https://jeanpi22.github.io/DuaPass/**

La disponibilidad en línea garantiza que los usuarios puedan utilizar la herramienta en cualquier momento y desde cualquier dispositivo, contribuyendo así a una mayor protección de sus cuentas digitales.

Figura 25

Repositorio

Nota. Fuente: El autor.

Adicional se pone a disposición el enlace al repositorio oficial de la aplicación, donde se encuentran el código fuente y la documentación técnica del generador de contraseñas. Este repositorio permite a los interesados explorar el desarrollo de la herramienta, conocer los detalles de implementación y contribuir con mejoras futuras si así lo desean. Puedes acceder al repositorio a través del siguiente enlace: **https://github.com/JeanPi22/DuaPass**. Esta transparencia en el desarrollo refuerza el compromiso con la calidad, la seguridad y la colaboración en la creación de herramientas útiles y accesibles para mejorar las prácticas de seguridad digital.

6. Conclusiones

Este proyecto se diseñó para abordar el problema de la inseguridad en la gestión de contraseñas entre usuarios, quienes a menudo desconocen las buenas prácticas de seguridad y emplean contraseñas fáciles de adivinar o reutilizan las mismas en diversas plataformas. Las conclusiones reflejan la efectividad de la aplicación y el cumplimiento de los objetivos específicos, los cuales se detallan a continuación:

- A través de la encuesta aplicada, se identificaron prácticas inseguras comunes entre los usuarios, como el uso de datos personales en contraseñas y la reutilización de contraseñas en múltiples plataformas. Estos hallazgos fueron fundamentales para definir los requisitos del generador de contraseñas, y permitieron evidenciar la falta de conciencia en los usuarios sobre los riesgos de estas prácticas. Esta conclusión respalda la necesidad de herramientas accesibles que puedan ayudar a los usuarios a mejorar sus prácticas de seguridad, dado que existe una tendencia generalizada hacia comportamientos que ponen en riesgo la información personal.

- El análisis de los datos recopilados en la fase de descubrimiento permitió establecer los elementos clave para el diseño de una interfaz intuitiva y funcional. Los resultados evidencian que la mayoría de los usuarios prefieren contraseñas que, aunque seguras, sean fáciles de recordar, y muestran una desconfianza hacia el uso de gestores de contraseñas externos. Esta información permitió definir un generador de contraseñas que balancea seguridad y usabilidad, cumpliendo con el objetivo de diseñar una solución que se adapte a las preferencias del usuario sin comprometer la seguridad.

- A través del uso de HTML y CSS, se logró implementar una interfaz sencilla que facilita la generación de contraseñas seguras sin requerir conocimientos avanzados. Este objetivo fue alcanzado exitosamente, y la aplicación permite a los usuarios personalizar la complejidad y longitud de las contraseñas generadas. La estructura clara de la interfaz y la facilidad de acceso a la función de generación responden a los requisitos de usabilidad identificados, destacando el valor de un diseño centrado en el usuario.

- La aplicación cumplió con el objetivo de crear un algoritmo capaz de generar contraseñas seguras mediante la combinación de caracteres alfanuméricos y símbolos especiales. El generador permite a los usuarios personalizar la longitud y configuración de la contraseña, asegurando la generación de claves robustas y únicas para diferentes plataformas. Esta característica cumple con los estándares de seguridad y representa una alternativa accesible para los usuarios que buscan mejorar la seguridad de sus contraseñas sin recurrir a gestores complejos o servicios de terceros.

- Además de cumplir con el objetivo de generar contraseñas, el prototipo incluye una función educativa que ofrece recomendaciones sobre buenas prácticas en seguridad de contraseñas, como evitar la reutilización de contraseñas y la inclusión de información personal. Esta funcionalidad destaca la importancia de sensibilizar a los usuarios sobre los riesgos de sus prácticas actuales y responde a la necesidad de una cultura de seguridad más consciente, fortaleciendo el impacto del proyecto en la mejora de la seguridad digital entre los usuarios.

En resumen, el proyecto "Generador de Contraseñas Seguras" ha logrado cumplir con los objetivos propuestos, proporcionando una herramienta accesible que facilita la generación de contraseñas fuertes y promueve una cultura de seguridad digital entre sus usuarios. La solución planteada aborda efectivamente los problemas identificados en el diagnóstico inicial,

destacando la importancia de herramientas prácticas y educativas en la mejora de las prácticas de ciberseguridad.

7. Recomendaciones

Las recomendaciones se formulan en función de los resultados obtenidos durante la ejecución del proyecto y se orientan a mejorar la utilidad y el alcance de la aplicación, así como a fomentar una mayor concienciación en ciberseguridad.

- Dada la relevancia de la ciberseguridad en el contexto actual, las instituciones educativas, especialmente en carreras relacionadas con tecnologías de la información, promuever el desarrollo de habilidades en seguridad digital. La inclusión de cursos específicos sobre la gestión segura de contraseñas y la concienciación sobre prácticas seguras contribuiría a mejorar la preparación de los estudiantes para enfrentar amenazas cibernéticas y los capacitaría para fomentar una cultura de seguridad en sus entornos laborales futuros.

- Realizar campañas de concienciación para fomentar el uso de contraseñas seguras entre usuarios de diversos perfiles, ya que el desconocimiento de buenas prácticas es una de las causas principales de vulnerabilidades en ciberseguridad. Las organizaciones y entidades educativas pueden incluir recursos y talleres prácticos sobre la creación y gestión de contraseñas seguras, así como sobre el uso de gestores de contraseñas y autenticación multifactor, para reducir los riesgos asociados a la reutilización de contraseñas y contraseñas débiles.

- Con el fin de ampliar la funcionalidad del generador de contraseñas, se sugiere considerar la integración de autenticación multifactorial en futuras versiones, así como la posibilidad de almacenar contraseñas de manera segura utilizando cifrado de alto nivel. Además, sería valioso incorporar un sistema de retroalimentación que permita a los usuarios

reportar su nivel de satisfacción y sugerencias sobre el prototipo, facilitando así su mejora continua.

- Gobernaciones y alcaldías implementar campañas de concienciación dirigidas a los ciudadanos sobre la importancia de crear y usar contraseñas seguras para acceder a servicios digitales gubernamentales, como pagos en línea, registros civiles o trámites administrativos. Estas campañas deberían incluir talleres prácticos gratuitos y el uso de herramientas como el generador de contraseñas del proyecto para fomentar prácticas de ciberseguridad. Además, se sugiere que estas entidades desarrollen o adopten plataformas que incorporen autenticación multifactorial para proteger los datos sensibles de los ciudadanos, reduciendo el riesgo de acceso no autorizado y ataques cibernéticos que puedan comprometer los servicios públicos.

- Instituciones de salud, públicas y privadas, promover el uso de contraseñas robustas y personalizadas para proteger el acceso a las historias médicas de los pacientes, garantizando la privacidad de sus datos sensibles. Como medida complementaria, sería ideal que estas instituciones integren soluciones de autenticación más avanzadas, como autenticación multifactorial, para prevenir accesos no autorizados a los sistemas de información de salud. Adicionalmente, pueden incorporar herramientas como generadores de contraseñas seguras para los sistemas internos, capacitando al personal sobre la importancia de la gestión adecuada de credenciales y asegurando la integridad y confidencialidad de los datos médicos en todo momento.

Estas recomendaciones buscan no solo mejorar la efectividad y alcance del proyecto "Generador de Contraseñas Seguras", sino también promover una cultura de ciberseguridad y una adopción generalizada de prácticas seguras en el manejo de información digital.

8. Referencias

AWS. (s. f.-a). *¿Qué es la ciberseguridad? - Explicación de la ciberseguridad - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/cybersecurity/

AWS. (s. f.-b). *¿Qué es la criptografía? - Explicación sobre la criptografía - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/cryptography/

Axity. (2024, mayo 27). *El ABC de las contraseñas seguras para mantener tus datos a salvo | Axity | Servicios de TI y Comunicaciones*. https://axity.com/comunidad-axity/el-abc-de-las-contrasenas-seguras-para-mantener-tus-datos-a-salvo/

Beltrán, M. (2023, abril 29). *Gestores de contraseñas: Qué son y por qué se deben usar*. https://www.eltiempo.com/tecnosfera/apps/gestores-de-contrasenas-que-son-y-por-que-se-deben-usar-763867

Bessa, A. (2023, abril 21). *Tipos de Autenticación: Contraseña, Token, JWT, Dos Factores y Más. | Alura Cursos Online*. Alura. https://www.aluracursos.com/blog/tipos-de-autenticacion

Cano Martínez, J. J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova*, *20*(40), 814-832. https://doi.org/10.21830/19006586.866

Castillo, O. J. (2019). Designthinking y el Método del Doble Diamante para el desarrollo de prototipos de Emprendimientos o StartUps. *Perspectivas: Revista Científica de la Universidad de Belgrano*, *2*(2), Article 2.

Comillas. (2024, marzo 18). *La Importancia de Contraseñas Robustas: Buenas Practicas*. Ciberseguridad. https://ciberseguridad.comillas.edu/la-importancia-de-contrasenas-fuertes-seguridad-y-buenas-practicas/

GammaUX. (2020, julio 31). Cómo usar el modelo del doble diamante para impulsar innovación en diseño. *GammaUX*. https://www.gammaux.com/blog/como-usar-el-modelo-del-doble-diamante-para-impulsar-innovacion-en-diseno/

Giannandrea, L. (2021, julio 21). Recomendaciones para la gestión de la custodia de claves. *eSoft Colombia*. https://esoft.com.co/blog/2021/07/21/recomendaciones-para-la-gestion-de-la-custodia-de-claves/

Goujon, A. (2013). *¿El fin de las contraseñas?* https://www.eset-la.com/pdf/prensa/informe/doble_autenticacion%20_el_fin_de_las_contrasenas.pdf

IBM. (2023, noviembre 14). *¿Qué es la criptografía?* | *IBM*. https://www.ibm.com/mx-es/topics/cryptography

IBM. (2024, agosto 12). *¿Qué es la ciberseguridad?* | *IBM*. https://www.ibm.com/es-es/topics/cybersecurity

Infante Montero, M. (2013). Criptografía y psicología de la contraseña: Generando una contraseña fuerte para diferentes servicios. *Apuntes de Ciencia & Sociedad*, *3*(1), Article 1. https://doi.org/10.18259/acs.2013008

Kaspersky. (2020, octubre 21). *Contraseñas seguras – Cómo crearlas y los beneficios que tienen*. /. https://latam.kaspersky.com/resource-center/threats/how-to-create-a-strong-password

Kiss, T. (2024, septiembre 30). Investigación descriptiva: Qué es, características, ejemplos. *https://concepto.de/*. https://concepto.de/investigacion-descriptiva/

López, M. J. L. (2022). *CRIPTOGRAFÍA Y SEGURIDAD EN COMPUTADORES*.

Microsoft. (s. f.). *¿Qué es la autenticación? Definición y métodos* | *Seguridad de Microsoft*. https://www.microsoft.com/es-co/security/business/security-101/what-is-authentication

Nu. (2023, marzo 3). *Qué es un gestor de contraseñas: ¿por qué usarlo?* | *Blog Nu*. Humanos, simples y transparentes. https://blog.nu.com.co/gestor-de-contrasenas-que-es-y-por-que-usarlo/

ODoherty, C. (2022, junio 14). *Por qué necesita un gestor de contraseñas* | *MetaCompliance*. https://www.metacompliance.com/es/blog/cyber-security-awareness/why-you-need-a-password-manager

Ortega, C. (2021, abril 14). Investigación mixta. Qué es y tipos que existen. *QuestionPro*. https://www.questionpro.com/blog/es/investigacion-mixta/

Ortiz, J. (2020, febrero 28). *Investigación exploratoria: Tipos, metodología y ejemplos*. Lifeder. https://www.lifeder.com/investigacion-exploratoria/

Paredes, G. G. (2006). INTRODUCCIÓN A LA CRIPTOGRAFÍA. *Revista Digital Universitaria*, *7*(7), 17.

Raffino, E. editorial. (2024, septiembre 26). *Metodología*. https://concepto.de/metodologia/

Rodríguez, M. P. (2021). Ciberseguridad en la justicia digital: Recomendaciones para el caso colombiano. *Revista UIS Ingenierías*, *20*(3). https://doi.org/10.18273/revuin.v20n3-2021002

Solutions, G. (2023a, marzo 20). ¿Qué es la norma ISO 27001 y para qué sirve? *GlobalSuite Solutions*. https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

Solutions, G. (2023b, octubre 11). ¿Qué es la norma ISO 27002 y para qué sirve? *GlobalSuite Solutions*. https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27002-y-para-que-sirve/

Stackscale. (2022, mayo 3). *Buenas prácticas para proteger contraseñas en 2022*. https://www.stackscale.com/es/blog/buenas-practicas-contrasenas-seguras/

Townsend, K. (2020, julio 7). *La importancia de la autenticación*. https://blog.avast.com/es/la-importancia-de-la-autenticación-avast