ELEMENTOS
ISSN-L: 2248-5252 / E-ISSN: 2027-923X

IMPLEMENTACIÓN DE UN GENERADOR DE CONTRASEÑAS SEGURAS BASADO EN EXPRESIONES REGULARES EN JAVA

IMPLEMENTING A SECURE PASSWORD GENERATOR BASED ON REGULAR EXPRESSIONS IN JAVA

Daniela Patricia Camargo Martínez
dpcamargo@poligran.edu.co
Institución Universitaria Politécnico Grancolombiano

Colombia

Juan David Roncancio Josa
jdaroncancio@poligran.edu.co
Institución Universitaria Politécnico Grancolombiano

Colombia

Víctor Danilo Vitola Cali
vvitola@poligran.edu.co
Institución Universitaria Politécnico Grancolombiano

Colombia

Recepción: *22/ 03/ 2024*
Aceptación: *01/07/2025*

DOI: https://doi.org/10.15765/jtshzb78

RESUMEN

El presente trabajo implementa un generador de contraseñas seguras y personalizables que resuelve el problema de vulnerabilidad en la protección de cuentas digitales. La

ELEMENTOS
ISSN-L: 2248-5252 / E-ISSN: 2027-923X

herramienta implementada en Java permite crear contraseñas altamente seguras mediante un sistema intuitivo que garantiza la máxima protección contra ciberataques, y al mismo ofrece una experiencia simplificada al usuario para garantizar su adaptación general. Los resultados demuestran la efectividad del sistema para generar contraseñas robustas que cumplen con los estándares de seguridad, protegiendo tanto a usuarios individuales como a pequeñas o grandes empresas contra el robo de datos y la suplantación de identidad.

PALABRAS CLAVES

Seguridad de la información, ciberseguridad, generador de contraseñas seguras, personalización, usabilidad, expresiones regulares.

INTRODUCCIÓN

Las contraseñas débiles son una de las principales vulnerabilidades en la seguridad digital, facilitando ataques cibernéticos. El 80% de las brechas de datos están relacionadas con contraseñas inseguras, y el 88% de los ataques exitosos usan claves de 12 caracteres o menos. A pesar de la información disponible, muchos usuarios siguen usando combinaciones predecibles debido a la falta de personalización y facilidad de uso. Si estos siguen usando contraseñas inseguras, estas mismas estarán expuestas a hackeos, robos de datos, filtración de información, pérdidas de acceso a cuentas importantes, ya sean laborales o personales, y suplantación de identidad.

Esto plantea la pregunta: ¿De qué forma se puede implementar un generador de contraseñas que sea tanto seguro como fácil de usar y que, a su vez, sea lo más

personalizable posible para el usuario, para así poder satisfacer las necesidades de diversos usuarios?

Este proyecto es clave para la seguridad digital, ya que protege tanto a usuarios individuales como a empresas de ciberataques. Como señala Arango (2024), "una contraseña débil es como una puerta mal cerrada", lo que resalta la necesidad de herramientas eficientes para generar contraseñas seguras.

MÉTODO

Para el desarrollo del proyecto se empleó un enfoque cuantitativo y aplicado, orientado al diseño e implementación de un sistema funcional capaz de generar contraseñas seguras mediante el uso de expresiones regulares.

1. Enfoque metodológico:

Se adoptó un enfoque de desarrollo incremental, basado en etapas de análisis, diseño, pruebas y validación. Esta estructura permitió construir el sistema de manera progresiva, asegurando la integración de funciones clave en cada fase.

2. Estrategia para la consecución de datos y fuentes:

La recopilación de información se centró en el análisis de requisitos funcionales necesarios para la construcción del sistema, así como la consulta de bibliografía y documentación técnica relacionada con expresiones regulares y validación de contraseñas. Todo esto fue coherente con los objetivos del proyecto: construir un generador de contraseñas seguras y funcionales.

3. Descripción de variables y relaciones a verificar:

ELEMENTOS
ISSN-L: 2248-5252 / E-ISSN: 2027-923X

Se definieron variables relacionadas con la longitud, complejidad y seguridad de las contraseñas. Además, se incluyeron condiciones que permiten detectar errores en tiempo real y ofrecer sugerencias de corrección. Si bien no se planteó una hipótesis tradicional, se asumió que el sistema sería capaz de generar contraseñas que cumplan con criterios de seguridad preestablecidos.

4. Herramientas y procedimientos para procesar la información:

Se empleó un entorno de desarrollo (por ejemplo, Java con interfaz gráfica), y herramientas de depuración y prueba de código. El sistema fue construido en módulos: manejo de expresiones regulares, lógica del generador, validación en tiempo real y gestión de contraseñas. Los procedimientos incluyeron el análisis sintáctico de entradas, verificación de patrones y gestión de errores en la entrada del usuario.

5. Descripción de experimentos o pruebas:

Se realizaron pruebas unitarias sobre cada clase del sistema para verificar su correcto funcionamiento. Posteriormente, se llevaron a cabo pruebas de usuario enfocadas en la interfaz gráfica y la experiencia general, obteniendo retroalimentación sobre usabilidad, comprensión de mensajes de error y eficacia en la generación de contraseñas.

6. Mecanismos y criterios de validación:

La validación del sistema se realizó mediante ajustes iterativos basados en los resultados de las pruebas. Se verificó que las contraseñas generadas cumplieran con los estándares de seguridad definidos (longitud, combinación de caracteres, ausencia de patrones

ELEMENTOS
ISSN-L: 2248-5252 / E-ISSN: 2027-923X

predecibles), y que la interfaz permitiera al usuario corregir errores de forma clara y en tiempo real.

RESULTADOS

Validación de contraseñas según medidas de seguridad

El análisis de los resultados demostró que el sistema de generación y validación de contraseñas cumple con los estándares de seguridad establecidos. Mediante expresiones regulares, se verificó que las contraseñas generadas automáticamente o ingresadas por el usuario siguen los siguientes criterios:

1. Longitud mínima de 8 caracteres.
2. Inclusión de al menos una letra mayúscula y una minúscula.
3. Presencia de al menos un número y un carácter especial.

En las pruebas realizadas, el sistema rechazó contraseñas que no cumplían con estos requisitos, como "password123" (falta carácter especial y mayúsculas) o "abcDEF@" (falta número), lo que confirma la efectividad del filtro de expresiones regulares implementado.

Efectividad en la generación de contraseñas personalizadas

El generador de contraseñas mostró un alto grado de personalización, permitiendo a los usuarios seleccionar parámetros como:

1. Longitud deseada (entre 8 y 32 caracteres).

2. Inclusión o exclusión de caracteres especiales.
3. Combinación de mayúsculas, minúsculas y números.

En las pruebas, se generaron contraseñas como "JdV1235+" y "Hola380#"*, las cuales fueron validadas como seguras por el sistema. Además, se observó que las sugerencias automáticas cumplían con los estándares de complejidad requeridos, reduciendo el riesgo de contraseñas débiles.

DISCUSIÓN Y CONCLUSIÓN

El presente trabajo demuestra la importancia de contar con herramientas eficaces para la generación de contraseñas seguras, abordando el problema de vulnerabilidad en la seguridad digital. A través de un sistema implementado en Java, se logró desarrollar una solución intuitiva que combina **personalización y robustez**, asegurando la protección contra ciberataques.

El **análisis de resultados** confirma que el generador de contraseñas cumple con los estándares de seguridad exigidos, verificando la inclusión de caracteres especiales, números, mayúsculas y minúsculas, además de una longitud mínima adecuada. La validación mediante expresiones regulares permite detectar errores en tiempo real, fortaleciendo el proceso de seguridad.

Desde una perspectiva práctica, la herramienta no solo beneficia a **usuarios individuales**, sino que también se convierte en un recurso valioso para **empresas y organizaciones**, reduciendo riesgos de **suplantación de identidad y robo de datos**.

Como recomendación para estudios futuros, se sugiere explorar mejoras en **usabilidad y accesibilidad**, así como integrar tecnologías emergentes como **inteligencia artificial** para la generación adaptativa de contraseñas basadas en patrones de seguridad personalizados. Además, la implementación de mecanismos de autenticación multifactor podría fortalecer aún más la seguridad digital.

ANTECEDENTES

En Colombia, la seguridad digital ha cobrado gran relevancia debido al aumento de ciberataques. Según **Páez Cruz (2014)**, la mejor manera de protegerse contra intrusos y evitar el robo de identidad es mediante el uso de contraseñas seguras. La autora enfatiza que la falta de precaución en sitios web y el uso de claves débiles exponen a los usuarios a riesgos innecesarios.

Por otro lado, **Gilarranz Nieto (2019)** desarrolló un gestor de contraseñas seguras en la Universidad de Valladolid, destacando la importancia de contar con herramientas que permitan almacenar y generar claves robustas. Su investigación resalta que la reutilización de contraseñas es un problema recurrente que compromete la seguridad de los usuarios.

LOCAL

En Medellín, la transformación digital ha impulsado la adopción de herramientas de seguridad informática. Según **Arango (2024)**, una contraseña débil es comparable a una puerta mal cerrada, lo que facilita el acceso de ciberdelincuentes. Su estudio enfatiza la

necesidad de generar claves seguras mediante combinaciones de caracteres diversos y evitar el uso de información personal en las contraseñas.

Además, se ha promovido el uso de autenticación multifactor y gestores de contraseñas para mejorar la protección de datos en sectores como la banca y el comercio electrónico.

INTERNACIONAL

A nivel global, el uso de contraseñas seguras ha sido objeto de múltiples estudios. **Secureframe (s.f.)** recopiló más de 80 estadísticas sobre contraseñas, revelando que el **88% de los ataques exitosos** utilizan claves de **12 caracteres o menos**. Además, el **65% de los usuarios** reutilizan contraseñas, lo que aumenta el riesgo de vulnerabilidad.

El estudio de **Gilarranz Nieto (2019)** también destaca la importancia de contar con gestores de contraseñas que permitan generar claves aleatorias y altamente seguras. Estas herramientas han sido fundamentales para reducir el riesgo de filtraciones de datos y mejorar la protección de información personal y empresarial.

REFERENCIAS BIBLIOGRÁFICAS

Arango, S. (2024). La Importancia de una Contraseña Segura. *Julabs.* *https://edu-labs.co/articulos/construyendo-la-fortaleza-digital-la-importancia-de-una-contrasena-segura/* .

Gilarranz Nieto, H. (2019). Gestor de contraseñas seguras. *Uva.* https://uvadoc.uva.es/handle/10324/36497.

Páez Cruz, L. (2014). Tip de TIC–Contraseñas seguras. *Redices.* https://repository.ces.edu.co/items/708afed2-b0c1-4def-aa69-4497504a010f.

Secureframe. (s.f). Más de 80 estadísticas de contraseñas para inspirar mejores prácticas de seguridad. *Secureframe.* https://secureframe.com/es-es/blog/password-statistics?utm_source=chatgpt.com