Carrera: Ingeniería en Ciberseguridad

Fecha de entrega: 10/11/2024

Nombre: Andrés Guerrero

Tema: Selección del Programa a desarrollar/ Generación de Diagramas funcionales y Arquitectura de Software

Software: Desarrollar un generador seguro de contraseñas

1. **Identificar el problema**

La mayoría de las personas de todo el mundo tienen dificultades para gestionar sus contraseñas. Una investigación reciente con respecto a violaciones de datos de Verizon informó que más del 70 % de los empleados repiten sus contraseñas mientras están en el trabajo. Según el estudio, el 81 % de las violaciones relacionadas con la piratería informática utilizaron contraseñas robadas o poco seguras. A pesar que muchas personas saben que reutilizar contraseñas es una mala práctica, existe un alto porcentaje que lo sigue haciendo.

La mayor parte de las personas tienen miedo de olvidar las contraseñas difíciles, por lo que para reducir el riesgo del acceso no autorizado a la información sensible es imprescindible utilizar contraseñas seguras, ya que el 80 % de todas las violaciones de datos en 2019 correspondían a la vulnerabilidad de contraseñas, provocando grandes pérdidas financieras. Además, existen diferentes tipos de ataque, que se focalizan en la contraseña débil y en el caso de la actividad empresarial, los ciberdelincuentes pueden usarlo para difundir información falsa, compartir datos con sus competidores o solicitar un rescate. (Security & Security, 2024)

2. **Comprender el problema**

   Para mejorar la seguridad de la contraseña necesitamos 20 caracteres aleatorios con letras mayúsculas y minúsculas, números y símbolos ya que tardan desde unos minutos hasta tres mil millones de años en descubrirse.

   También es importante que la contraseña tenga una longitud larga ya que genera más seguridad

3. **Identificar soluciones alternas**

- No reutilizar contraseñas
- Utilizar una contraseña única para cada sitio web
- No utilizar información personal en contraseñas
- Generar una contraseña aleatoria de caracteres utilizando python

4. **Seleccionar una mejor solución**

   La mejor solución es generar una contraseña aleatoria de caracteres utilizando python. Porque crea una contraseña de longitud específica mezclando letras, números y símbolos. Permitiendo dar seguridad contra ataques bruscos cuando utilizan combinaciones criptográficamente aleatorias.

5. **Listar los pasos de la solución seleccionada**

   1. Definir tipos de caracteres necesarios para construir la contraseña
   2. Incluir al menos un carácter de cada tipo
   3. Completar la longitud con caracteres aleatorios
   4. Evaluar la seguridad de la contraseña

Diagrama Caso de Uso

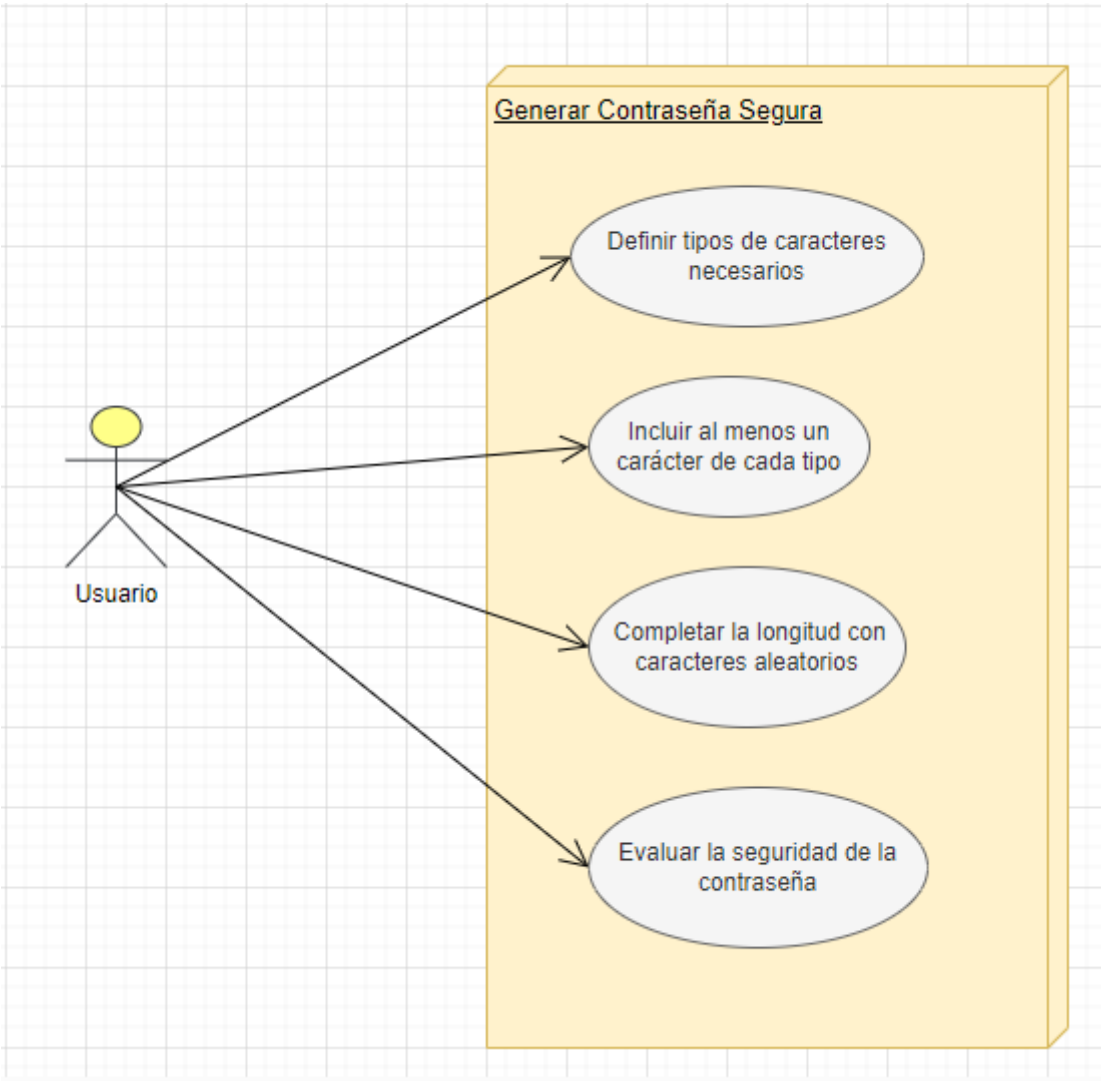
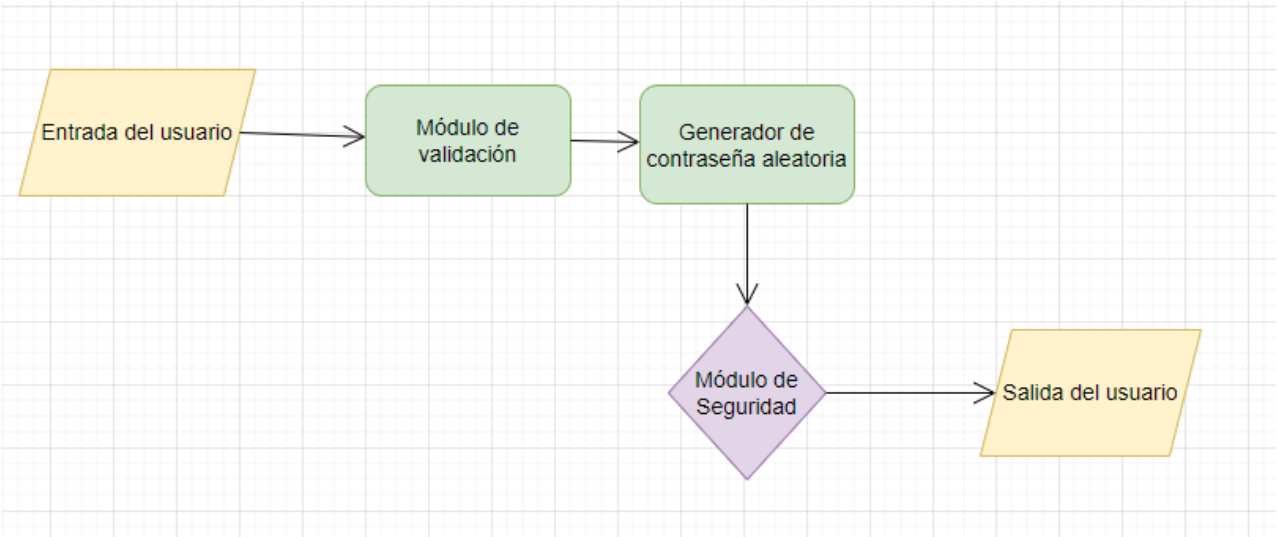


Diagrama de Arquitectura del Software



Fuente bibliográfica:

Security, K., & Security, K. (2024, 12 enero). ¿Por qué es importante la seguridad de contraseñas? Keeper Security Blog - Cybersecurity News & Product Updates. https://www.keepersecurity.com/blog/es/2022/09/14/why-is-password-security-important/