## FASE 2: ANÁLISIS DEL PROYECTO "ENCRIPTACIÓN DE CONTRASEÑA SEGURA"

### INTRODUCCIÓN

El análisis es una de las fases más importantes del ciclo de vida del proyecto, ya que permite identificar y comprender los requisitos, las necesidades del usuario y las posibles amenazas que puedan surgir durante el desarrollo y uso del sistema. En esta etapa, se define cómo debe funcionar la herramienta y qué aspectos críticos deben considerarse para garantizar que cumpla su propósito de manera efectiva y segura.

### OBJETIVO DEL ANÁLISIS

El objetivo principal de esta fase es especificar las funciones, características y restricciones del sistema para garantizar su correcta implementación y seguridad. Este análisis se centra en:

1. **Identificar requisitos funcionales y no funcionales.**
2. **Estudiar las amenazas relacionadas con el uso de contraseñas y la generación de contraseñas seguras.**
3. **Definir los criterios de seguridad y usabilidad para la herramienta.**
4. Establecer las dependencias tecnológicas y los datos que se usarán (como bases de contraseñas comunes o comprometidas).

**Requisitos del sistema**

**1. Requisitos funcionales**

- La herramienta debe permitir al usuario ingresar una contraseña y evaluarla según criterios de seguridad (longitud, complejidad, entropía, etc.).
- Identificar contraseñas vulnerables comparándolas con listas públicas de contraseñas comprometidas.
- Generar y sugerir contraseñas alternativas seguras.
- Proporcionar una explicación clara de por qué una contraseña es débil o fuerte.

**2. Requisitos no funcionales**

- **Rendimiento:** La evaluación y generación de contraseñas debe realizarse en menos de 1 segundo.
- **Usabilidad:** La herramienta debe ser intuitiva y accesible para usuarios con conocimientos básicos en tecnología.
- **Seguridad:** Ninguna contraseña ingresada debe almacenarse ni enviarse a terceros.
- **Compatibilidad:** Debe funcionar en diferentes sistemas operativos y navegadores, si se implementa como una aplicación web.

---

**Análisis de amenazas**

Durante esta fase, es crucial identificar posibles vulnerabilidades y amenazas que puedan surgir en el uso y desarrollo de la herramienta. Estas amenazas incluyen:

**Amenazas en el ingreso de contraseñas**

- **Filtración de contraseñas:** Un atacante podría interceptar las contraseñas ingresadas si no se manejan de forma segura.
- **Validación incorrecta:** Si los criterios de evaluación son inadecuados, una contraseña débil podría considerarse fuerte.

**Amenazas en la generación de contraseñas**

- **Contraseñas predecibles:** Si el algoritmo de generación no es aleatorio, las contraseñas podrían ser susceptibles a ataques.
- **Reutilización de patrones comunes:** Usar patrones repetitivos o basados en datos conocidos (como fechas o nombres) podría debilitar la seguridad.

**Amenazas relacionadas con la base de datos de contraseñas comunes**

- **Falta de actualización:** Si no se mantiene actualizada, la herramienta podría no identificar nuevas contraseñas comprometidas.
- **Filtración de datos:** Un acceso no autorizado a esta base de datos podría comprometer su integridad.

---

**Soluciones a las amenazas**

Para mitigar estas amenazas, se plantean las siguientes soluciones:

**Ingreso de contraseñas**

- Implementar un entorno seguro que garantice la encriptación de las contraseñas ingresadas durante su evaluación (por ejemplo, mediante el uso de HTTPS o TLS).
- Crear un algoritmo robusto basado en estándares de la industria, como las recomendaciones de **NIST** u **OWASP**, para evaluar la fuerza de las contraseñas.

**Generación de contraseñas**

- Utilizar generadores de números aleatorios criptográficamente seguros (por ejemplo, secrets en Python o crypto.randomBytes en JavaScript).
- Evitar patrones predecibles y promover contraseñas únicas para cada usuario.

**Base de datos de contraseñas comprometidas**

- Integrar APIs confiables como Have I Been Pwned para verificar contraseñas contra bases de datos actualizadas.
- Proteger el acceso a estas bases de datos mediante mecanismos de autenticación y encriptación.

---

**Flujo lógico del sistema**

A continuación se detalla cómo se conectan las principales funciones del sistema:

1. **Ingreso de contraseña:** El usuario ingresa su contraseña en la interfaz.
2. **Evaluación:** El sistema evalúa la seguridad de la contraseña en tiempo real, verificando:
    - Longitud mínima requerida (por ejemplo, 12 caracteres).
    - Inclusión de caracteres alfanuméricos y especiales.
    - Ausencia en bases de contraseñas comunes.
3. **Resultado:** Se informa al usuario si la contraseña es segura o necesita ser mejorada.

4. **Generación de una nueva contraseña (si es necesario):** Se genera una contraseña segura basada en criterios personalizados.
5. **Reporte educativo:** Se explica al usuario por qué su contraseña no era segura y cómo puede gestionarlas mejor en el futuro.

---

**Resultados esperados del análisis**

- Definición clara de las funciones que debe cumplir la herramienta.
- Identificación de amenazas y soluciones que se implementarán en las siguientes fases.
- Garantizar que los requisitos definidos sean realistas, alcanzables y se alineen con las necesidades del usuario y las mejores prácticas de seguridad.