Proyecto final: Guardianpass: La bodega digital más segura.

Roles:

1. Juan Gutiérrez Scrum máster
2. Diego Castro product owner
3. Juan Castañeda developer
4. David Quiroga developer

Definición del problema o necesidad:

El proyecto tiene como objetivo resolver el problema de la gestión segura y eficiente de contraseñas en entornos digitales. Con el crecimiento del uso de servicios en línea y aplicaciones, los usuarios enfrentan el desafío de recordar y mantener seguras múltiples contraseñas. Esto conlleva al a riesgo de utilizar contraseñas débiles o repetidas, lo que puede resultar en vulnerabilidades de seguridad y posibles ataques cibernéticos.

La necesidad principal es desarrollar un gestor de contraseñas robusto que permitía a los usuarios almacenar, generar y gestionar contraseñas de manera mas segura y conveniente. El proyecto abordara los siguientes aspectos:

1. Almacenamiento seguro de contraseñas: Utilizar técnicas de cifrado avanzado para almacenar las contraseñas de los usuarios de forma segura, protegiéndolas de accesos no autorizados.
2. Generador de contraseñas: Ofrecer una herramienta para generar contraseñas aleatorias y seguras que cumplan con los estándares de seguridad modernos.
3. Interfaz intuitiva: Desarrollar una interfaz de usuario intuitiva y fácil de usar que permita a los usuarios acceder y gestionar sus contraseñas de manera eficiente, incluso para aquellos con poca experiencia técnica.
4. Sincronización y respaldo: Implementar funciones que permitan sincronizar y respaldar las contraseñas aun la nube o en dispositivos locales, asegurando que los dataos estén disponibles y protegidos en todo momento.
5. Seguridad adicional: Incorporar características adicionales de seguridad, como autenticación de dos factores y bloqueo automático, para proteger aun mas las cuentas de los usuarios.

**Tecnologías a utilizar:**

1. Flujo de usuario: Registro/Inicio de sesión, Almacenamiento/Recuperación de contraseñas, Generación de contraseñas, Organización/Categorización de contraseñas, Sincronización/Respaldo de datos.
2. Funciones principales: Cifrado/Descifrado de contraseñas, Generación de contraseñas aleatorias, Autenticación de usuario, Gestión de sesiones.
3. Entradas: Nombres de usuario, contraseñas maestras, contraseñas para servicios en línea, categorías/etiquetas.
4. Datos: Contraseñas, configuraciones de usuario.
5. Salidas: Contraseñas recuperadas, mensajes de confirmación/error interfaz de usuario actualizada.

**Planificación:**

Definición de alcance:

1. El alcance del proyecto incluirá el desarrollo de un gestor de contraseñas seguro y fácil de usar que permita a los usuarios almacenar, generar y gestionar sus contraseñas de manera eficiente.
2. Las características clave incluirán almacenamiento seguro de contraseñas, generador de contraseñas, autenticación de usuario, organización y categorización, respaldo y seguridad.

Cronograma:

|  |  |  |  |
| --- | --- | --- | --- |
| Actividad | Duración estimada | Inicio | Fin |
| Planificación del proyecto | 1 semana | 4/04/2024 | 6/04/2024 |
| Análisis de requisitos | 1 semana | 7/04/2024 | 13/04/2024 |
| Diseño de la interfaz de usuario | 1 semana | 14/04/2024 | 20/04/2024 |
| Desarrollo del Backend | 10 días | 21/04/2024 | 30/04/2024 |
| Desarrollo del Frontend | 1 semana | 1/05/2024 | 8/05/2024 |
| Pruebas y depuración | 1 semana | 8/05/2024 | 11/05/2024 |
| Implementación de sincronización | 1 semana | 12/05/2024 | 18/05/2024 |
| Implementación de seguridad final | 1 semana | 19/05/2024 | 25/05/2024 |
| Pruebas finales y ajustes | 1 semana | 26/05/2024 | 29/05/2024 |
| Entrega del proyecto |  | 31//05/2024 |  |