Centro educativo

Código	Centro	Concello	Ano académico
15005397	I.E.S. Fernando Wirtz Suárez	A Coruña	2024-2025

Ciclo formativo

	Familia Profesional	Código do Ciclo Formativo	Ciclo Formativo	Grao	Réxime
	Informática e comunicacións	CSIFC02	Desenvolvemento de Aplicacións Web	Superior	Dual

Módulo profesional e unidades formativas de menor duración (*)

Código MP / UF	Nome
MP0492	Proxecto de Desenvolvemento de Aplicacións Web

Profesorado responsable

Titora	Cristina Martínez Pérez

Alumno

Alumno/Alumna	Javier Vázquez Pardo

Datos do Proxecto

Título	KeyBastion

<fecha no formato “dd / mm / aa ”>

<Nome Alumno/a>

CONTROL DE VERSIÓNS:

Versión	Data	Observacións

Índice / Táboa de Contidos:

1. Obxectivo
2. Descrición
3. Alcance
4. Planificación
5. Medios a utilizar4
6. Presuposto
7. Titulo
8. Execución / Demostración4

1. Obxectivo

El objetivo principal de este proyecto es desarrollar una aplicación llamada KeyBastion, que permite crear, almacenar, gestionar y compartir contraseñas de forma segura. La aplicación emplea tecnologías avanzadas de cifrado (AES-256) y autenticación (JWT y BCrypt) para garantizar la seguridad de las credenciales de los usuarios y protegerlas contra accesos no autorizados.

- Objetivos específicos:
  - Permitir a los usuarios almacenar y recuperar contraseñas cifradas.
  - Ofrecer un generador de contraseñas seguras.
  - Facilitar el compartimiento seguro de contraseñas mediante enlaces temporales.
  - Registrar un historial de accesos y modificaciones para garantizar la trazabilidad.

2. Descripción

KeyBastion es una aplicación diseñada para gestionar contraseñas de forma segura y eficiente. La aplicación ofrece funcionalidades clave como:

- **Cifrado AES-256** para almacenar contraseñas de manera segura.
- **Hash de contraseñas** de los usuarios mediante BCrypt.
- **Autenticación** basada en JWT para evitar accesos no autorizados.
- **Historial de accesos y auditoría** para garantizar la trazabilidad de las acciones realizadas.
- **Generador de contraseñas seguras** integrado.

Puntos destacables:

- La implementación del cifrado AES-256 y la autenticación JWT fueron los aspectos técnicos más complejos, ya que requirieron un conocimiento profundo de seguridad y criptografía.
- La integración del generador de contraseñas seguras y el sistema de compartimiento mediante enlaces temporales también supusieron un desafío técnico significativo.

Modelo Relacional en Diagramas

Entidades y Relaciones:

- Usuario (1) —— (N) Credencial
- Usuario (1) —— (N) Compartición —— (N) Usuario
- Credencial (1) —— (N) Compartición
- Credencial (N) —— (1) Categoría
- Usuario (1) —— (N) Registro_Acceso
- Usuario (1) —— (1) Configuración

3. Alcance

El alcance del proyecto incluye las siguientes funcionalidades:

- **Registro e inicio de sesión seguro** mediante JWT.
- **Gestión de credenciales:** creación, modificación, eliminación y clasificación por categorías.
- **Cifrado avanzado** para almacenar contraseñas de manera segura.
- **Compartimiento seguro** de contraseñas mediante enlaces temporales.
- **Historial de actividades y auditoría** de accesos.

4. Planificación

Análisis y diseño (14 de marzo - 22 de marzo):

Definición de requisitos.

Diseño de modelos y arquitectura.

Planificación inicial.

Desarrollo del back-end (23 de marzo - 19 de abril):

Implementación del sistema de usuarios y autenticación.

Creación de la API REST para gestión de credenciales y compartimiento.

Integración del cifrado de datos.

Implementación del generador de contraseñas.

Desarrollo del front-end (20 de abril - 17 de mayo):

Creación de interfaces y flujo del usuario.

Integración con la API del back-end.

Implementación de validaciones y seguridad en el front-end.

Pruebas y despliegue (18 de mayo - 21 de mayo):

Pruebas de seguridad y usabilidad.

Despliegue en un entorno de pruebas.

Implementación en producción.

5. Medios a utilizar

Back-end: Java, Spring Boot, mySQL, JPA/Hibernate.

Front-end: React.js, Bootstrap, Axios.

Seguridad: BCrypt, AES-256, JWT.

Herramientas de desarrollo: IntelliJ IDEA, Postman, Git/GitHub, Podman.

Infraestructura: AWS EC2/S3, Heroku (opcional para despliegue en pruebas).

6. Presuposto

<

Opcional

CA 3.7. Fíxose a valoración económica que dea resposta ás condicións da execución.

CA 2.6. Realizouse o orzamento correspondente.

>

- **Servidor AWS EC2:** 10€/mes.
- **Base de datos PostgreSQL en AWS RDS:** 15€/mes.
- **Certificado SSL:** 5€/mes.
- **Dominio (porkbun.com, por ejemplo):** 9€/año.
- **Equipo:** 1200€.

7. Titulo

KeyBastion

8. Execución / Demostración

O/A alumno/a realizará finalmente, unha demostración do funcionamento do proxecto.