PROYECTO LOGIN

DEFINICIÓN PROYECTO

OBJETIVOS

Objetivo General

Desarrollar un sistema de inicio de sesión el cual permita autenticación segura de los usuarios, garantizando el acceso controlado al sistema mediante la validación de credenciales almacenadas en una base de datos.

Objetivos Específicos

- Diseñar e implementar una interfaz de usuario intuitiva y funcional con el objetivo de que facilite el ingreso por parte de los usuarios.
- Permitir la autenticación de usuarios a través de correo electrónico y contraseña, asegurándose de que los datos sean correctos.
- Crear una base de datos que almacene la información de los usuarios de forma organizada y segura.
- Establecer la conexión entre la aplicación y la base de datos.
- Verificar que cuente con seguridad garantizando la confidencialidad de las contraseñas mediante técnicas de cifrado o encriptación.
- Mostrar errores que orienten al usuario durante el proceso de autenticación. Implementar un control de sesiones que mantenga la autenticación activa mientras el usuario navega por el sistema.
- Incorporar la funcionalidad de cierre de sesión, asegurando que el usuario pueda finalizar su sesión de forma segura.
- Restringir el acceso al sistema a todos los usuarios que no se encuentren autenticados. Que la arquitectura sea escalable, para que permita a nuevos usuarios registrarse en un futuro, así como también realizar modificaciones al sistema. Realizar pruebas de validación para garantizar la fiabilidad del sistema.
- Optimizar los tiempos de respuesta del sistema, garantizando un proceso de autenticación ágil y eficiente para el usuario.
- Asegurar que el sistema cuente con la compatibilidad con distintos navegadores y dispositivos.

DESCRIPCIÓN

El proyecto consiste en el desarrollo de un sistema de inicio de sesión (login) que permita a los usuarios autenticarse de manera segura dentro de una aplicación web. Este sistema validará las credenciales ingresadas (correo electrónico y contraseña) con los datos almacenados en una base de datos, garantizando el acceso únicamente a usuarios registrados y autorizados.

El login contará con una interfaz amigable e intuitiva, diseñada para facilitar la interacción del usuario. Además, incluirá funciones de cifrado de contraseñas, manejo de sesiones activas y cierre de sesión seguro, todo bajo buenas prácticas de desarrollo web.

JUSTIFICACIÓN

El desarrollo de un sistema de inicio de sesión es fundamental para cualquier aplicación que requiera control de acceso y protección de información. A través de este proyecto se busca garantizar la seguridad, confidencialidad e integridad de los datos de los usuarios, evitando accesos no autorizados y vulnerabilidades comunes.

Asimismo, la implementación de este login permitirá adquirir conocimientos prácticos sobre conexión a bases de datos, validación de usuarios, encriptación de contraseñas y control de sesiones. Con el fin de brindar al usuario una experiencia segura y fluida al momento de ingresar a una plataforma digital.

FUNCIONALIDADES PRINCIPALES

El sistema de login incluirá las siguientes funcionalidades clave:

1. **Registro de usuarios:** Permite almacenar nuevos usuarios en la base de datos.
2. **Inicio de sesión:** Autenticación mediante correo electrónico y contraseña.
3. **Validación de credenciales:** Verificación de los datos ingresados frente a los almacenados en la base de datos sean correctos.
4. **Cifrado de contraseñas:** Protección de las contraseñas mediante algoritmos de encriptación (por ejemplo, bcrypt o hash).
5. **Gestión de sesiones:** Mantiene al usuario autenticado durante su navegación por el sistema.
6. **Cierre de sesión seguro:** Permite finalizar la sesión y eliminar los datos de autenticación temporal.
7. **Mensajes de error y validación:** Informa al usuario sobre credenciales incorrectas o campos incompletos.
8. **Compatibilidad multiplataforma:** Asegura el correcto funcionamiento en distintos navegadores y dispositivos.
9. **Arquitectura escalable:** Facilita la futura expansión del sistema (nuevos usuarios, roles o módulos).

ESPECIFICACIÓN DE REQUISITOS (ANÁLISIS)

REQUISITOS FUNCIONALES

Registro de usuarios	El sistema debe permitir el registro de nuevos usuarios mediante un formulario que solicite nombre, correo electrónico, fecha de nacimiento y contraseña. El sistema debe validar que el correo no esté previamente registrado, la contraseña sea lo suficientemente segura, y la fecha de nacimiento sea acorde al tiempo actual. La contraseña debe almacenarse cifrada en la base de datos.
Inicio de sesión	El sistema debe permitir que los usuarios registrados inicien sesión ingresando su correo y contraseña. El sistema debe verificar que datos, como correo, estén registrados previamente, de lo contrario, el usuario deberá registrarse.
Validación de credenciales	El sistema debe verificar que las credenciales ingresadas coincidan con las almacenadas en la base de datos. Si las credenciales son incorrectas, el sistema debe mostrar un mensaje de error informativo.
Cifrado de contraseñas	El sistema debe tener un proceso de cifrado al momento de almacenar las contraseñas en la base de datos, de modo que no se podrán visualizar a simple vista desde una consulta directa a la base de datos.
Gestión de sesiones	El sistema debe crear una sesión activa al iniciar sesión correctamente. El sistema debe mantener la sesión activa mientras el usuario navegue por

	la aplicación. El sistema debe cerrar la sesión automáticamente al presionar el botón “Cerrar sesión” o después de un tiempo de inactividad.
Cierre de sesión seguro	El sistema debe permitir al usuario cerrar su sesión de forma segura. Al cerrar sesión, debe eliminarse toda la información temporal relacionada con el usuario.
Mensajes de error y validación	Si las credenciales ingresadas por el usuario son incorrectas a las almacenadas en la base de datos, o no existen, el sistema deberá notificar al usuario por medio de un mensaje de alerta según sea el caso. Si las credenciales son correctas y coinciden con los parámetros requeridos, el sistema validará el acceso y mostrará un mensaje de validación, permitiendo acceder al usuario.
Compatibilidad multiplataforma	El sistema deberá adaptarse según la plataforma de donde sea accedida, de modo que no afecte su funcionamiento y mantenga su atractivo visual original.
Arquitectura escalable	El sistema deberá ser adaptable, con dinamismo, de modo que pueda aceptar fácilmente y sin problemas mayores, la adición de contenido futuro o la modificación de contenido previamente agregado.