# Definición del Proyecto: Sistema de Login Seguro

Autores

Angulo Rivera José Camilo

Borrego Meza Roger

Loera Ochoa Fernando Daniel

Serrano Arellanes Carlos David

Facultad de Informática Culiacán

Universidad Autónoma de Sinaloa

ingeniería de Software

Nombre del docente: Fidel Bojórquez Solis

## Objetivo

El sistema debe permitir a los usuarios autenticarse mediante un nombre de usuario y contraseña, garantizando el acceso seguro a las secciones restringidas de la aplicación.

Se busca establecer un control de acceso confiable, proteger la información de los usuarios y ofrecer una experiencia sencilla y eficiente en el proceso de inicio y cierre de sesión.

## Descripción

El proyecto consiste en el desarrollo de un sistema de login web que valide las credenciales de los usuarios contra una base de datos y gestione sus sesiones activas de forma segura.

El sistema mostrará mensajes de error claros en caso de credenciales incorrectas, permitirá la recuperación de contraseña mediante correo electrónico y ofrecerá una opción de registro para nuevos usuarios.

Además, se implementará la funcionalidad de "recordar usuario" para mantener la sesión iniciada en el dispositivo si el usuario así lo desea.

La aplicación controlará las sesiones activas y evitará la duplicidad en caso de que el mismo usuario intente iniciar sesión desde varios dispositivos simultáneamente.

## Justificación

La implementación de un sistema de login es esencial para garantizar la seguridad, confidencialidad y control de acceso dentro de la aplicación.

Permite identificar a cada usuario, proteger la información almacenada y restringir el uso de funcionalidades solo a quienes tengan autorización.

Asimismo, la gestión de sesiones y la recuperación de contraseñas fortalecen la confianza del usuario y aseguran una experiencia de uso profesional y confiable.

Con este sistema, se evitarán accesos no autorizados, se mantendrá la integridad de los datos y se mejorará la administración de usuarios dentro del sistema.

## Funcionalidades Principales

Autenticación mediante nombre de usuario y contraseña.

Validación de credenciales contra la base de datos.

Mensajes de error claros en caso de credenciales incorrectas.

Recuperación de contraseña mediante correo electrónico.

Registro de nuevos usuarios.

Cierre de sesión seguro.

Control de sesiones activas y prevención de duplicidad.

Opción de “recordar usuario” en el dispositivo.

## Requisitos Funcionales

Los requisitos funcionales describen las acciones específicas que el sistema debe realizar.

- El sistema debe permitir el registro de nuevos usuarios mediante un formulario con validación de datos.
- El sistema debe permitir a los usuarios iniciar sesión utilizando su nombre de usuario y contraseña.

- El sistema debe validar las credenciales contra los datos almacenados en la base de datos.
- El sistema debe mostrar mensajes de error claros cuando las credenciales sean incorrectas o el usuario no exista.
- El sistema debe permitir la recuperación de contraseña mediante un correo electrónico con un enlace o código temporal.
- El sistema debe permitir a los usuarios cerrar sesión de forma segura, destruyendo la sesión activa.
- El sistema debe controlar las sesiones activas, evitando múltiples inicios de sesión simultáneos con el mismo usuario si se requiere.
- El sistema debe ofrecer una opción de "recordar usuario", almacenando la sesión localmente en el dispositivo.
- El sistema debe redirigir automáticamente al usuario autenticado a la página principal o al panel correspondiente según su rol.
- El sistema debe bloquear temporalmente la cuenta tras varios intentos fallidos consecutivos (opcional para mayor seguridad).

Requisitos No Funcionales

Los requisitos no funcionales establecerán las características de calidad y comportamiento general del sistema.

- Seguridad:
  Las contraseñas deben almacenarse de forma encriptada utilizando funciones seguras como password_hash().
  Las sesiones deben gestionarse mediante identificadores únicos y protegidos.
  Se deben implementar medidas contra ataques de fuerza bruta e inyección SQL.
- Usabilidad:
  La interfaz debe ser intuitiva, clara y accesible para cualquier tipo de usuario.
  Los mensajes de error deben ser comprensibles y no revelar información técnica.
- Disponibilidad:
  El sistema debe estar disponible al menos el 99% del tiempo durante su uso normal.
- Rendimiento:
  La validación de credenciales y carga de la interfaz no deben superar los 3 segundos en condiciones normales.

- Compatibilidad:
  El sistema debe funcionar correctamente en los navegadores más comunes (Chrome, Edge, Firefox).
  Debe ser adaptable a dispositivos móviles y computadoras de escritorio.
- Mantenibilidad:
  El código debe estar documentado y estructurado para facilitar futuras modificaciones o ampliaciones.
- Privacidad:
  No se deben mostrar datos sensibles en la interfaz ni en los mensajes de error.
  Debe cumplirse con las normas básicas de protección de datos personales.