Proyecto LOGIN

Requisitos no funcionales

Seguridad

- El login debe implementar un mecanismo de bloqueo de cuenta después de 5 intentos fallidos.
- Autenticación segura y confidencialidad de contraseñas con encriptación.
- Control de sesiones para mantener la autenticación activa de forma segura.
- Cierre de sesión seguro.
- Restricción de acceso a usuarios no autenticados.

Usabilidad

- Interfaz intuitiva y funcional que facilite el ingreso.
- Mensajes de error orientativos durante la autenticación.
- La contraseña debe tener una opción para mostrar/ocultar la contraseña.
- El mensaje de error para un login fallido debe mostrar "nombre de usuario o contraseña incorrecta".
- El botón de "iniciar sesión" se debe deshabilitar después del primer clic para prevenir envíos múltiples.

Rendimiento

- Optimización de tiempos de respuesta para un proceso ágil y eficiente.
- El sistema debe verificar al usuario y cargar la página principal en menos de 3 segundos.
- El servidor durante el proceso de login no debe exceder los 200 milisegundos.

Compatibilidad

- Soporte multi-navegador y multi-dispositivo.
- Fiabilidad / Calidad.
- Pruebas de validación para garantizar la fiabilidad del sistema.

Escalabilidad y Mantenibilidad

- Arquitectura escalable para admitir nuevos registros y permitir modificaciones futuras al sistema.

DIAGRAMA DE CASOS DE USOS Y DESCRIPCIÓN DEL LOGIN

Diagrama de Casos de Uso:

El diagrama muestra el actor principal, Usuario, y los casos de uso asociados con el proceso de inicio de sesión.

Descripción de Casos de Uso

· Caso de Uso: Iniciar Sesión (Login)

CAMPO	DESCRIPCIÓN
Identificador	CU-001
Nombre	Iniciar sesión (login)
Objetivo	Permitir que el usuario acceda a una página o aplicación privada mediante su cuenta.
Precondición	El usuario debe tener una cuenta registrada.
Ruta principal	El usuario ha iniciado sesión con éxito.
Ruta alternativa	El usuario

Ruta principal (Éxito)

1. El sistema muestra la interfaz de inicio de sesión (login).

2. El usuario introduce su nombre de usuario/contraseña.

3. El usuario presiona el botón Iniciar Sesión.

4. El sistema toma la información y la compara con la almacenada en la base de datos.

5. Si la información es válidas, el Sistema crea una sesión activa para el Usuario.

6. El Sistema redirige al usuario a la página principal.

7. El caso de uso finaliza.

Ruta Alternativa

· A1: Credenciales Inválidas:

1. Si la verificación del Sistema (paso 4 de la ruta principal) determina que el nombre de usuario o la contraseña no coinciden con ningún registro.

2. El Sistema muestra un mensaje de error (correo / contraseña incorrecta . Por favor, inténtelo de nuevo.) en la interfaz de inicio de sesión.

3. El Usuario vuelve al paso 2 de la ruta principal.

· A2: Campos Vacíos:

1. Si el usuario presiona “Iniciar Sesión” (paso 3) con uno o ambos campos (usuario/contraseña) vacíos.

2. El sistema muestra un mensaje de advertencia (Ambos campos son obligatorios.)

3. El usuario vuelve al paso 2 de la ruta principal.

· A3: Olvidó Contraseña:

1. El usuario selecciona la opción “Olvidé mi contraseña” en la interfaz de login.

2. El sistema inicia el caso de uso relacionado con la recuperación de contraseña.

IDENTIFICACION Y DEFINICION DE ENTIDADES Y ATRIBUTOS

Identificación de entidades.

Usuario	Sesión	IntentoLogin
Representa a las personas que pueden registrarse e iniciar sesión en el sistema	Representa el registro de las sesiones activas que los usuarios inician.	Registra los intentos fallidos de inicio de sesión, útil para el bloqueo tras varios errores.

Definición de Atributos de cada Entidad
Entidad Usuario.
Atributos:
id_usuario: Identificador único del usuario.
Nombre: Nombre completo del usuario.
Correo: Correo electrónico del usuario (usado como usuario de login).
Fecha_nacimiento: Fecha de nacimiento del usuario.
Contraseña: Contraseña cifrada.
Fecha_registro: Fecha en que se registró el usuario.
Estado_cuenta: Estado de la cuenta (por intentos fallidos o baja).

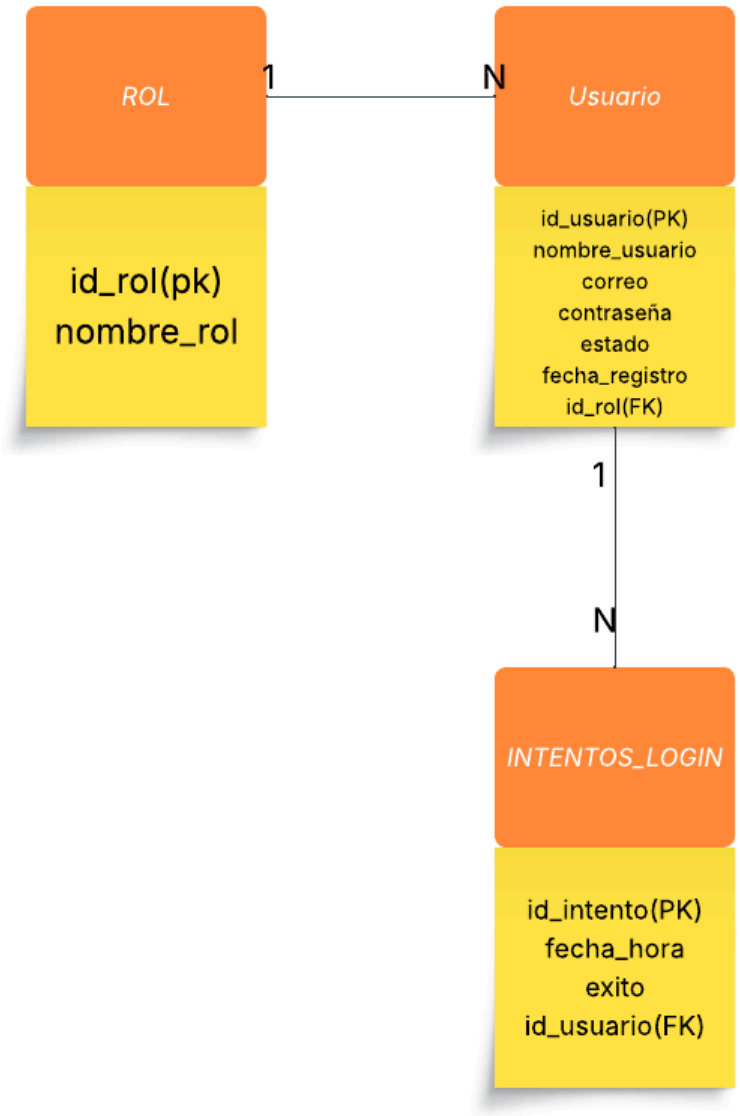
Entidad Sesión.
Atributos:
Id_sesion: Identificador único de la sesión.
Id_usuarin: Usuario asociado a la sesión.
Token_sesion: Token o identificador único de sesión.
Fecha_inicio: Fecha y hora en que inicia la sesión.
Fecha_fin: Fecha y hora en que se cierra la sesión.
Estado: ('activa', 'cerrada', 'expirada') Estado actual de la sesión.

Entidad IntentoLogin.
Atributos:
Id_intento: Identificador único del intento.
Id_usuario: Usuario asociado al intento.
Fecha_intento: Fecha y hora del intento.
Exitoso: Indica si el intento fue exitoso o fallido.

Relaciones entre entidades.

Relación	Tipo	Descripción
Usuario – Sesión	1 a N	Un usuario puede tener varias sesiones activas o cerradas.
Usuario – IntentoLogin	1 a N	Un usuario puede realizar varios intentos de inicio de sesión.

DIAGRAMA ENTIDAD RELACIÓN


ROL
1
N
Usuario
id_rol(pk)
nombre_rol
id_usuario(PK)
nombre_usuario
correo
contraseña
estado
fecha_registro
id_rol(FK)
1
N
INTENTOS_LOGIN
id_intento(PK)
fecha_hora
exito
id_usuario(FK)