



INSTITUTO TECNOLÓGICO BELTRÁN
Centro de Tecnología e Innovación

Instituto Superior De Formacion Técnica N°197

Alumno: Luis Toncic

Profesor: Diego Klehr



RISUN
TECHNOLOGY
Control de Acceso QR

**Tecnicatura Superior en Análisis de Sistemas
Prácticas Profesionalizantes III**

Índice

| | |
|--|----|
| Acta de constitución del proyecto | 3 |
| Introducción | |
| 1.1 Propósito | 7 |
| 1.2 Ámbito | 7 |
| 1.3 Definiciones y Abreviaturas | 7 |
| 1.4 Referencias | 7 |
| Infografía | 8 |
| Descripción General del Proyecto | |
| 2.1 Perspectiva del Producto | 9 |
| 2.2 Usuarios del Sistema | 9 |
| 2.3 Restricciones | 9 |
| Especificación de Requerimientos | |
| 3.1 Requerimientos Funcionales | 10 |
| 3.2 Requerimientos No Funcionales | 23 |
| Diseño del Sistema | |
| 4.1 Interfaces de usuario | 25 |
| 4.2 Modelo de Datos (DER) | 35 |
| 4.3 Diagrama de Casos de Uso | 36 |
| 4.4 Especificación de Casos de Uso | 37 |
| 4.5 Diagrama de Secuencia | 42 |
| 4.6 Diagrama de Clases | 48 |
| 4.7 Diagrama de Componentes | 49 |
| 4.8 Diagrama de Despliegue | 50 |
| Pruebas | 51 |
| Anexos | |
| 5.1 Manual de Usuario (Acceso) | 56 |
| 5.2 Manual de Usuario (Gestión) | 61 |
| 5.3 Historias de Usuario | 68 |
| Apéndices | |
| 6 Glosario de Términos | 73 |

Acta de Constitución del proyecto

Título del Proyecto

Sistema Integral de Control de Accesos y Gestión con Auditoría

1. Propósito del Proyecto

El proyecto busca desarrollar un sistema que permita gestionar el acceso de personas mediante el uso de códigos QR, con un enfoque en la seguridad, trazabilidad y usabilidad. Este sistema incluirá módulos para la gestión de usuarios y personas, generación y validación de tokens QR, y auditoría detallada de eventos administrativos.

2. Descripción del Proyecto

El sistema tendrá tres módulos principales:

- Módulo de Acceso QR: Generación, validación y control de tokens QR para gestionar el ingreso y egreso de usuarios.
- Módulo de Gestión de Personas y Usuarios: Operaciones CRUD con soporte para borrado lógico y validaciones de consistencia entre datos.
- Módulo de Auditoría y Reportes: Registro detallado de eventos administrativos y funcionalidad de exportación a CSV para análisis.

3. Objetivos del Proyecto

- Proveer un sistema seguro y eficiente para gestionar accesos basados en códigos QR.
- Implementar un control estricto sobre las acciones administrativas con auditoría y trazabilidad.
- Ofrecer una interfaz intuitiva y accesible adaptada a diferentes roles (directivo, usuario general).
- Garantizar la integridad y disponibilidad de la información mediante borrados lógicos y validaciones.

4. Alcance del Proyecto

El proyecto abarcará las siguientes áreas:

- Desarrollo de módulos: Accesos QR, ABM de personas y usuarios, auditoría.
- Base de datos relacional: Diseño e implementación para soportar todas las funcionalidades del sistema.
- Pruebas y despliegue: Validaciones funcionales, integrales y de sistema para garantizar la calidad del producto final.
- Entrega de documentación: Manuales de usuario, especificaciones técnicas y reporte de pruebas realizadas.

5. Criterios de Éxito

- El sistema debe gestionar accesos basados en QR con menos de un 1% de errores reportados.
- La funcionalidad de auditoría debe registrar el 100% de los eventos administrativos.
- Cumplimiento con los requisitos funcionales y no funcionales definidos según la norma IEEE 830.
- Documentación completa y aprobada para soporte y mantenimiento.

6. Requerimientos Iniciales

- Servidor con soporte para PHP 8.2+, MySQL 8+, y acceso a bibliotecas necesarias para generación de códigos QR.
- Navegadores modernos (Chrome, Firefox) para la interfaz web.
- Equipo de trabajo:
 - Desarrollador: Responsable del diseño, desarrollo e implementación.
 - Tester: A cargo de validar la calidad y funcionalidad del sistema.
 - Supervisor: Aprobación del cumplimiento de los requisitos.

7. Restricciones y Suposiciones

Restricciones:

- Cumplir con los plazos establecidos para cada entrega parcial y final.
- Ajustarse a la tecnología especificada (PHP, MySQL, HTML, CSS, JavaScript).
- Presupuesto limitado para adquisición de librerías o servicios externos.

Suposiciones:

- Los usuarios tendrán conocimientos básicos de uso de sistemas web.
- El servidor tendrá disponibilidad 24/7 y backups diarios para garantizar la seguridad.

8. Cronograma de Entregas

| | Labores | Duración | Comienzo | T.E.E |
|----|--|-----------|------------|------------|
| 1 | Análisis | 3 semanas | 11/03/2024 | 03/04/2024 |
| 2 | Perfiles de Usuario | 2 semanas | 11/03/2024 | 27/03/2024 |
| 3 | Project Charter | 2 semanas | 11/03/2024 | 27/03/2024 |
| 4 | Infografía | 2 semanas | 03/04/2024 | 15/04/2024 |
| 5 | Especificación de Requerimientos de Software | 4 semanas | 17/04/2024 | 13/05/2024 |
| 6 | Diagrama de Clases | 4 semanas | 15/05/2024 | 10/06/2024 |
| 7 | Casos de Usos | 4 semanas | 15/05/2024 | 10/06/2024 |
| 8 | Diagrama de Secuencia | 4 semanas | 15/05/2024 | 10/06/2024 |
| 9 | Diagrama de Componentes | 4 semanas | 15/05/2024 | 10/06/2024 |
| 10 | Prototipos | 1 semana | 12/06/2024 | 19/06/2024 |
| 11 | Prueba de Concepto | 1 dia | 24/06/2024 | 24/06/2024 |
| 12 | Desarrollo: Modulo QR | 2 semanas | 12/08/2024 | 21/08/2024 |
| 13 | Desarrollo: Modulo Gestión | 3 semanas | 26/08/2024 | 16/09/2024 |
| 14 | Desarrollo: Modulo Auditoría | 4 semanas | 18/09/2024 | 16/10/2024 |
| 15 | Testing | 1 semana | 21/10/2024 | 28/10/2024 |
| 16 | Presentación | 1 semana | 30/10/2024 | 06/11/2024 |

9. Riesgos Identificados

| Riesgo | Impacto | Probabilidad | Plan de mitigación |
|----------------------------------|---------|--------------|---|
| Fallo en la Generación del token | Alto | Medio | Implementar pruebas unitarias para la funcionalidad |
| Errores en la Auditoria | Medio | Bajo | Revisar integridad en la parte de pruebas |
| Retraso en el Desarrollo | Alto | Medio | Usar herramientas de Gestión |

10. Entregables

- Sistema completo desplegado y funcional.
- Documentación técnica (especificación de requisitos, manuales, diagramas UML).
- Manual de usuario detallado.
- Reporte de pruebas realizadas y validaciones exitosas.

Introducción

1.1 Propósito del documento

Este documento define todos los aspectos relacionados con el desarrollo, diseño, implementación, y pruebas del Sistema de Control de Acceso por Tokens QR, incluyendo la gestión de usuarios, auditoría de actividades y generación de reportes. Se presenta en conformidad con los estándares establecidos por la Norma IEEE 830, ofreciendo un detalle completo de los requisitos funcionales, no funcionales, y todos los artefactos técnicos necesarios para su desarrollo.

1.2 Alcance del sistema

El sistema abarca las siguientes funcionalidades clave:

- Gestión de Usuarios: Alta, Baja y Modificación con roles y permisos específicos.
- Gestión de Personas: Registro de datos personales asociados a usuarios.
- Generación de Tokens QR: Emisión de tokens únicos con validación temporal.
- Control de Accesos: Ingreso y egreso con estado actualizado en tiempo real.
- Auditoría de Actividades: Registro detallado de todas las acciones realizadas por los usuarios administrativos.
- Generación de Reportes: Informes personalizables exportados en formato CSV.

El sistema está diseñado para optimizar la administración de accesos en instituciones educativas, garantizando seguridad, eficiencia y trazabilidad en todos los procesos.

1.3 Definiciones, acrónimos y abreviaturas

- Token QR: Código generado que permite el control de accesos.
- ABM: Alta, Baja y Modificación, referente a la gestión de registros.
- Auditoría: Proceso de registrar acciones administrativas realizadas en el sistema.
- CSV: Formato de archivo para exportación de datos tabulares.

1.4 Referencias

- Norma IEEE 830: Especificación de Requisitos de Software.
- Manuales del Usuario y de Gestión proporcionados en el proyecto.
- Guía de estilos para aplicaciones de control de acceso.

Infografía



Descripción General

2.1 Perspectiva del producto

El sistema opera en un entorno cliente-servidor, con una interfaz accesible desde navegadores modernos. Está diseñado para adaptarse a dispositivos móviles, garantizando accesibilidad desde cualquier lugar.

Módulos Principales:

- Login y Seguridad: Validación de usuarios mediante reCAPTCHA y verificación de credenciales.
- Gestión de Personas y Usuarios: Interfaz para registrar datos personales y asignar roles.
- Generación y Validación de Tokens QR: Funcionalidad central para control de accesos.
- Auditoría y Reportes: Registro y exportación de actividades realizadas en el sistema.

2.2 Usuarios del sistema

- Directivo: Acceso completo al sistema, generación de reportes.
- Administrativo: Gestión de personas y usuarios.
- Alumno/Docente/Invitado: Uso de tokens para accesos.

2.3 Restricciones

- Conexión a internet requerida.
- Uso exclusivo en navegadores modernos.

Requisitos del sistema

3.1 Requisitos Funcionales

Módulo de Login:

- RF01: Validar credenciales ingresadas por el usuario.
- RF02: Permitir acceso solo a usuarios no eliminados lógicamente.
- RF03: Implementar reCAPTCHA para prevenir bots.

Gestión de Personas y Usuarios:

- RF04: Registrar nuevos usuarios y personas.
- RF05: Asociar cada usuario a un rol predefinido (directivo, docente, alumno, etc.).
- RF06: Implementar borrado lógico para usuarios y personas.

Tokens QR:

- RF07: Generar tokens únicos asociados a usuarios.
- RF08: Validar el estado de un token (usado/no usado).
- RF09: Controlar el tiempo de expiración del token.

Auditoría y Reportes:

- RF10: Registrar todas las acciones administrativas realizadas por los usuarios.
- RF11: Permitir filtros avanzados por fecha, acción y usuario.
- RF12: Exportar reportes en formato CSV.

IDENTIFICADOR: RF01

NOMBRE: Validar credenciales ingresadas por el usuario

| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
|-----------|-----------------------|----------|--------------------------|
| Necesario | | Sí | Alta |

Entrada

Usuario y contraseña válidos

Salida

Acceso permitido o mensaje de error

DESCRIPCIÓN:

| Proceso | Detalle |
|----------------|---|
| Pre Condición | El usuario debe estar registrado y activo. |
| Descripción | Validar las credenciales ingresadas por el usuario. |
| Post Condición | Acceso permitido según las credenciales correctas. |

MANEJO DE SITUACIONES ANORMALES:

Credenciales incorrectas o usuario eliminado (mensaje de error).

CRITERIOS DE ACEPTACIÓN:

- Las credenciales deben ser verificadas con precisión.
- El sistema debe notificar en caso de error.

IDENTIFICADOR: RF02

NOMBRE: Permitir acceso solo a usuarios no eliminados lógicamente

| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
|-----------|-----------------------|----------|--------------------------|
| Necesario | | Sí | Alta |

Entrada

Usuario activo en la base de datos

Salida

Acceso permitido o mensaje de error

DESCRIPCIÓN:

| Proceso | Detalle |
|----------------|---|
| Pre Condición | Usuario no debe estar eliminado lógicamente. |
| Descripción | Controlar que solo usuarios activos puedan acceder. |
| Post Condición | Acceso denegado para usuarios eliminados. |

MANEJO DE SITUACIONES ANORMALES:

Intento de acceso con usuario eliminado (mensaje de error).

CRITERIOS DE ACEPTACIÓN:

- Usuarios eliminados lógicamente no deben poder autenticarse.
- El sistema debe dar retroalimentación clara.

IDENTIFICADOR: RF03

NOMBRE: Implementar reCAPTCHA para prevenir bots

| | | | |
|----------|-----------------------|----------|--------------------------|
| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
| Deseable | | No | Media |

Entrada

Validación de reCAPTCHA

Salida

Autenticación exitosa o denegada

DESCRIPCIÓN:

| Proceso | Detalle |
|----------------|---|
| Pre Condición | El formulario debe incluir el reCAPTCHA. |
| Descripción | Evitar accesos automatizados con bots mediante reCAPTCHA. |
| Post Condición | Solo accesos legítimos permitidos. |

MANEJO DE SITUACIONES ANORMALES:

Fallo en la validación del reCAPTCHA.

CRITERIOS DE ACEPTACIÓN:

- El reCAPTCHA debe ser visible y funcional.
- El sistema debe denegar accesos sospechosos.

IDENTIFICADOR: RF04

NOMBRE: Registrar nuevos usuarios y personas

| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
|-----------|-----------------------|----------|--------------------------|
| Necesario | | Sí | Alta |

Entrada

Datos personales y rol asignado

Salida

Nuevo registro en la base de datos

DESCRIPCIÓN:

| | |
|----------------|---|
| Proceso | Detalle |
| Pre Condición | Los datos del usuario o persona deben ser completos y válidos. |
| Descripción | Permitir el registro de nuevos usuarios y personas en el sistema. |
| Post Condición | El usuario o persona es registrado exitosamente en el sistema. |

MANEJO DE SITUACIONES ANORMALES:

Error en la validación de datos o usuario duplicado.

CRITERIOS DE ACEPTACIÓN:

- Todos los campos obligatorios deben completarse correctamente.
- El registro debe reflejarse en la base de datos.

IDENTIFICADOR: RF05

NOMBRE: Asociar cada usuario a un rol predefinido

| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
|-----------|-----------------------|----------|--------------------------|
| Necesario | | Sí | Alta |

Entrada

Rol seleccionado

Salida

Usuario asociado al rol correcto

DESCRIPCIÓN:

| Proceso | Detalle |
|----------------|---|
| Pre Condición | El rol debe existir en el sistema. |
| Descripción | Asociar automáticamente a cada usuario un rol como directivo, docente, etc. |
| Post Condición | El usuario cuenta con permisos según el rol asignado. |

MANEJO DE SITUACIONES ANORMALES:

Intento de asignar un rol no existente.

CRITERIOS DE ACEPTACIÓN:

- Los roles deben reflejarse correctamente en el perfil del usuario.
- Solo roles válidos pueden ser asignados.

IDENTIFICADOR: RF06

NOMBRE: Implementar borrado lógico para usuarios y personas

| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
|-----------|-----------------------|----------|--------------------------|
| Necesario | | Sí | Alta |

Entrada

ID del usuario o persona a eliminar

Salida

Usuario o persona marcado como eliminado

DESCRIPCIÓN:

| | |
|----------------|---|
| Proceso | Detalle |
| Pre Condición | El usuario o persona debe existir en el sistema. |
| Descripción | Evitar eliminar registros físicamente mediante un estado de eliminado lógico. |
| Post Condición | El registro permanece en la base de datos con estado 'eliminado'. |

MANEJO DE SITUACIONES ANORMALES:

Error al cambiar el estado del registro.

CRITERIOS DE ACEPTACIÓN:

- Los registros eliminados no deben aparecer en búsquedas activas.
- El sistema debe garantizar la integridad de los datos restantes.

IDENTIFICADOR: RF07

NOMBRE: Generar tokens únicos asociados a usuarios

| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
|-----------|-----------------------|----------|--------------------------|
| Necesario | | Sí | Alta |

Entrada

ID del usuario

Salida

Token único generado

DESCRIPCIÓN:

| | |
|----------------|--|
| Proceso | Detalle |
| Pre Condición | El usuario debe estar registrado y activo. |
| Descripción | Generar un token único vinculado a un usuario para el control de acceso. |
| Post Condición | El token está disponible para su uso. |

MANEJO DE SITUACIONES ANORMALES:

Generación fallida o token duplicado.

CRITERIOS DE ACEPTACIÓN:

- El token debe ser único y no reutilizable.
- El sistema debe validar la asociación correcta con el usuario.

IDENTIFICADOR: RF08

**NOMBRE: Validar el estado de un token
 (usado/no usado)**

| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
|-----------|-----------------------|----------|--------------------------|
| Necesario | | Sí | Alta |

Entrada

Token ingresado por el usuario

Salida

Validación exitosa o denegada

DESCRIPCIÓN:

| Proceso | Detalle |
|----------------|--|
| Pre Condición | El token debe existir y no estar expirado. |
| Descripción | Verificar que el token ingresado esté activo y no haya sido usado. |
| Post Condición | Acceso otorgado o denegado según el estado del token. |

MANEJO DE SITUACIONES ANORMALES:

Token inválido, usado o expirado.

CRITERIOS DE ACEPTACIÓN:

- Tokens usados o expirados no deben permitir acceso.
- El sistema debe registrar el estado del token correctamente.

IDENTIFICADOR: RF09

NOMBRE: Controlar el tiempo de expiración del token

| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
|-----------|-----------------------|----------|--------------------------|
| Necesario | | Sí | Alta |

Entrada

Token generado

Salida

Token válido o expirado

DESCRIPCIÓN:

| Proceso | Detalle |
|----------------|--|
| Pre Condición | El token debe tener una fecha de expiración válida. |
| Descripción | Garantizar que cada token tenga un límite de tiempo establecido. |
| Post Condición | Tokens expirados no pueden ser utilizados. |

MANEJO DE SITUACIONES ANORMALES:

Token utilizado después de su expiración.

CRITERIOS DE ACEPTACIÓN:

- El tiempo de expiración debe configurarse correctamente.
- Tokens expirados deben invalidarse automáticamente.

IDENTIFICADOR: RF10

NOMBRE: Registrar todas las acciones administrativas realizadas

| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
|-----------|-----------------------|----------|--------------------------|
| Necesario | | Sí | Alta |

Entrada

Acción realizada por el administrador

Salida

Registro en la tabla de auditoría

DESCRIPCIÓN:

| | |
|----------------|---|
| Proceso | Detalle |
| Pre Condición | El usuario debe tener permisos administrativos. |
| Descripción | Registrar todas las acciones relevantes para auditoría. |
| Post Condición | Las acciones quedan documentadas en la base de datos. |

MANEJO DE SITUACIONES ANORMALES:

Error al registrar una acción administrativa.

CRITERIOS DE ACEPTACIÓN:

- El sistema debe registrar todas las acciones de manera automática.
- La auditoría debe incluir detalles completos de cada acción.

IDENTIFICADOR: RF11

NOMBRE: Permitir filtros avanzados por fecha, acción y usuario

| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
|----------|-----------------------|----------|--------------------------|
| Deseable | | No | Media |

Entrada

Fecha inicial y final

Acción seleccionada

Usuario

Salida

Listado filtrado de registros

DESCRIPCIÓN:

| Proceso | Detalle |
|----------------|--|
| Pre Condición | Debe existir al menos un registro que cumpla los criterios. |
| Descripción | El sistema permitirá filtrar registros de auditoría por parámetros avanzados como fechas, acciones específicas realizadas y usuarios involucrados. |
| Post Condición | Se muestra el listado filtrado según los parámetros especificados. |

MANEJO DE SITUACIONES ANORMALES:

No se encuentran registros que coincidan con los filtros (mostrar mensaje de 'Sin resultados').

CRITERIOS DE ACEPTACIÓN:

- Los filtros deben devolver resultados precisos basados en los parámetros seleccionados.
- El tiempo de respuesta del filtrado debe ser inferior a 5 segundos.

IDENTIFICADOR: RF12

NOMBRE: Exportar reportes en formato CSV

| Tipo: | (Necesario/Deseable) | CRÍTICO? | Prioridad de Desarrollo: |
|-----------|-----------------------|----------|--------------------------|
| Necesario | | Sí | Alta |

Entrada

Criterios de filtrado establecidos

Salida

Archivo CSV descargable

DESCRIPCIÓN:

| Proceso | Detalle |
|----------------|--|
| Pre Condición | Debe existir al menos un registro que coincida con los filtros aplicados. |
| Descripción | Permitir que los directivos exporten registros de auditoría en formato CSV para su análisis externo. |
| Post Condición | El archivo CSV se genera correctamente y se descarga en el equipo del usuario. |

MANEJO DE SITUACIONES ANORMALES:

Error al generar el archivo CSV (mostrar mensaje de error y registrar el incidente en la auditoría).

CRITERIOS DE ACEPTACIÓN:

- El archivo CSV debe incluir todas las columnas y datos relevantes.
- La descarga debe completarse en menos de 5 segundos para un conjunto de hasta 1000 registros.

3.2 Requisitos No Funcionales

RNF01: Rendimiento:

El sistema debe procesar hasta 100 solicitudes de generación de tokens por minuto sin afectar el rendimiento.

RNF02: Seguridad:

Todas las contraseñas deben almacenarse encriptadas usando bcrypt.

RNF03: Compatibilidad:

El sistema debe ser accesible desde Google Chrome, Firefox y Microsoft Edge.

RNF04: Disponibilidad:

Garantizar un uptime del 99.5% mediante hosting confiable.

RNF05: Usabilidad:

Todas las funcionalidades deben estar documentadas en un manual de usuario interactivo.

ID: RNF01

Descripción: El sistema debe procesar hasta 100 solicitudes de generación de tokens por minuto sin afectar el rendimiento.

Prioridad: Alta

Criterios:

- El sistema debe mantenerse estable bajo esta carga.

ID: RNF02

Descripción: Todas las contraseñas deben almacenarse encriptadas usando bcrypt.

Prioridad: Alta

Criterios:

- Los datos de las contraseñas deben ser irrecuperables por medios directos.

ID: RNF03

Descripción: El sistema debe ser accesible desde Google Chrome, Firefox y Microsoft Edge.

Prioridad: Media

Criterios:

- El diseño debe ser responsive y compatible con múltiples navegadores.

ID: RNF04

Descripción: Garantizar un uptime del 99.5% mediante hosting confiable.

Prioridad: Alta

Criterios:

- El servicio debe garantizar alta disponibilidad según SLA.

ID: RNF05

Descripción: Todas las funcionalidades deben estar documentadas en un manual de usuario interactivo.

Prioridad: Media

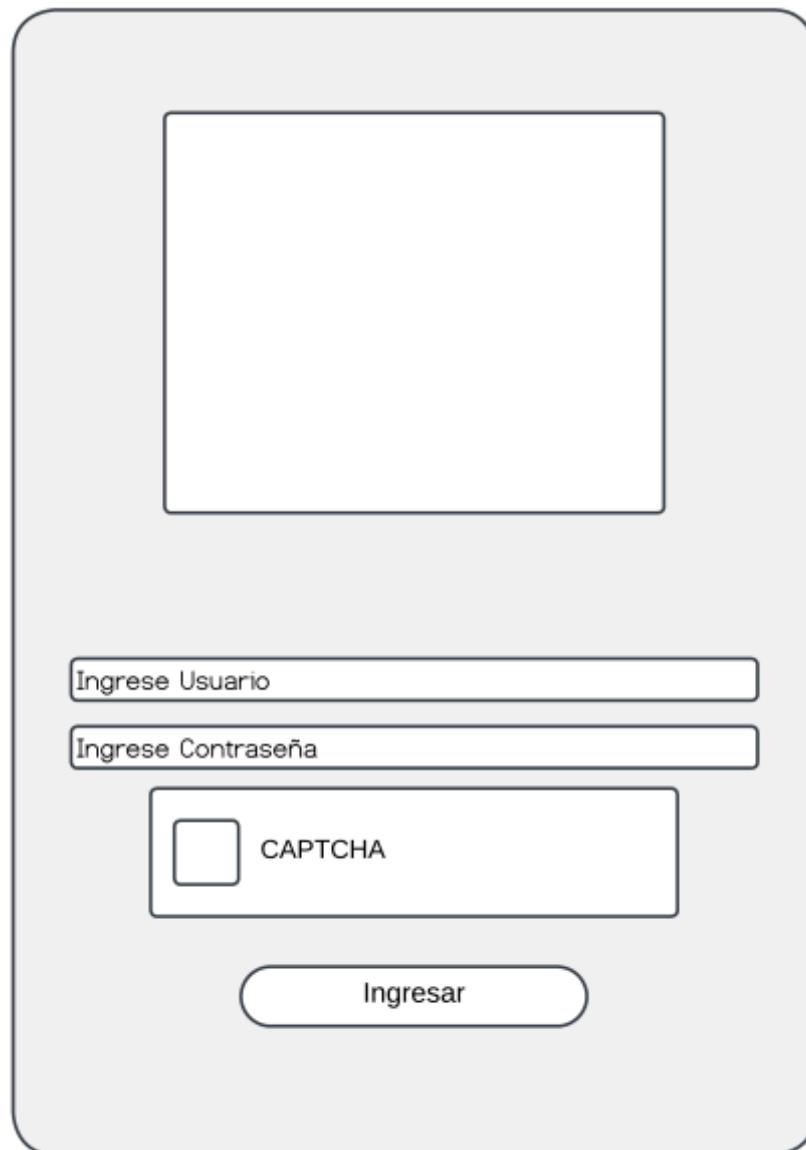
Criterios:

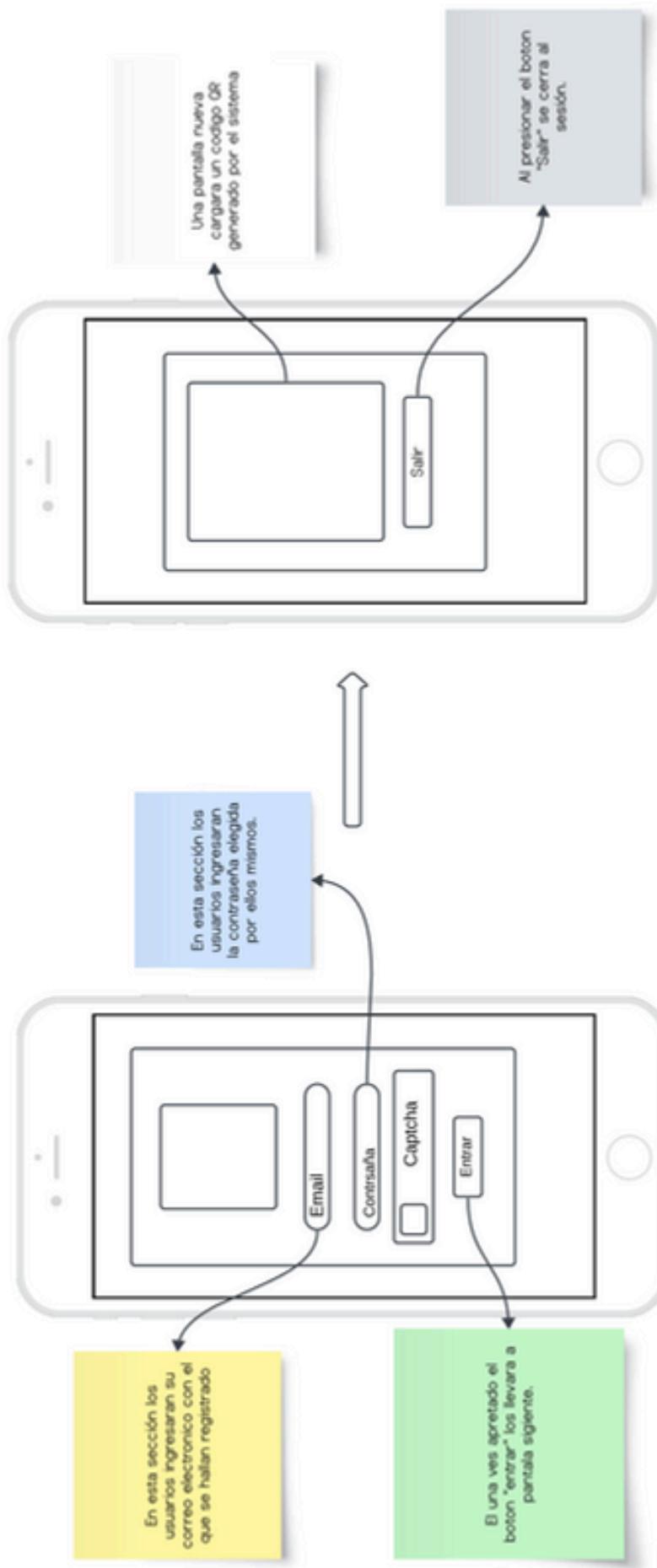
- El manual debe cubrir casos de uso comunes y escenarios de error.

Diseño del sistema

4.1 Interfaces de usuario

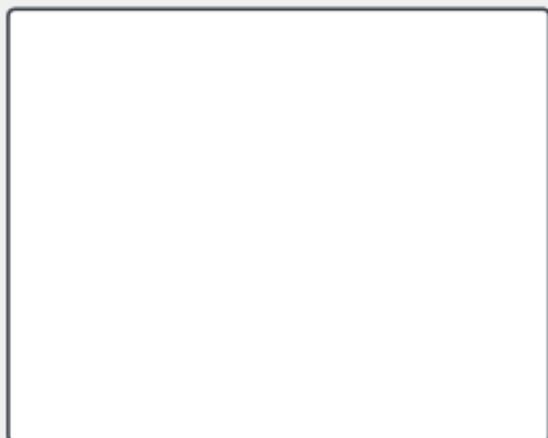
Modulo de Acceso







Modulo de Gestión



CAPTCHA

Gestión de Personas y Usuarios

| | |
|---------------------------------|-----------------------------------|
| Agregar Persona | Tabla de Personas |
|---------------------------------|-----------------------------------|

TABLA PERSONAS

Mostrar registros

Buscar:

| ID | Nombre | Apellido | Edad | DNI | Mail | Teléfono | Dirección | Localidad | Legajo | Carrera | Turno | Acciones |
|----|--------|----------|------|-----|------|----------|-----------|-----------|--------|---------|-------|----------|
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

Mostrando registro del 1 al 5 de un total de 5 registros

[Anterior](#) [Siguiente](#)

Gestión de Personas y Usuarios

TABLA USUARIOS

Mostrar registros

Buscar:

| ID | Usuario | Contraseña | Rol | Legajo | Acciones |
|----|---------|------------|-----|--------|----------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Mostrando registro del 1 al 5 de un total de 5 registros

Salir

Reportes

Edad

Teléfono

Legajo

Rol

Personal

Apellido

Mail

Localidad

Turno

Mañana

Agregar Persona

Nombre

DNI

Dirección

Carrera

Agregar

Modulo de Auditoría

[Atrás](#)
[Salir](#)

[Bitácora de Tokens](#)

[Bitácora de Accesos](#)

[Bitácora de Auditoría](#)

[Bitácora de Auditoría](#)

[Bitácora de Accesos](#)

[Bitácora de Tokens](#)

Apellido

Buscar por apellido

Rol

Todos

Show

Acción

Todas

Fecha Inicio

dd/mm/aaaa

Search

Usuario

Buscar por DNI

Fecha Fin

dd/mm/aaaa

Filtrar

Buscar por Usuario

Restablecer

| Nombre | Apellido | DNI | Usuario | Rol | Acción | Descripción | Fecha |
|--------|----------|-----|---------|-----|--------|-------------|-------|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Show entries
Showing 1 to 8 of 8 entries
[Exportar CSV](#)

[Previous](#)
[Next](#)

Bitácora

Accesos

Bitácora de Auditoria

Bitácora de Accesos

Control de Acceso QR

Atrás

Sair

| | | | | | | | |
|----------|---------------------|--------|----------------|---------------|--------------------|--------------|--------------------------|
| Apellido | Buscar por apellido | DNI | Buscar por DNI | Usuario | Buscar por Usuario | Role | Todas |
| Turno | Todos | Estado | Todos | Fecha Ingreso | dd/mm/aaaa | Fecha Egreso | <input type="checkbox"/> |
| | | | | ▼ | | | |
| | | | | | | | |
| | | | | | | | |

Filtrar

Show entries

Search

| Nombre | Apellido | DNI | Usuario | Role | Turno | Fecha Ingreso | Fecha Egreso | Estado |
|--------|----------|-----|---------|------|-------|---------------|--------------|--------|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Showing 1 to 8 of 8 entries

Exportar CSV

Previous

Next

Bitácora

Tokens

[Bitácora de Auditoría](#)

[Bitácora de Acceso](#)

[Bitácora de Tokens](#)

Apellido

DNI

Buscar por apellido

Rol

Buscar por DNI

Usuario

Todas

Buscar por Usuario

Turno

Token

Todos

Buscar por Token

Estado de Acceso

Todos

Buscar por Estado de Acceso

Fecha Creación Token

dd/mm/aaaa

Fecha Expiración Token

dd/mm/aaaa

Filtrar

Restablecer

Show entries

Search

| Nombre | Apellido | DNI | Usuario | Rol | Turno | Token | Fecha Creación | Fecha Expiración | Estado Acceso |
|--------|----------|-----|---------|-----|-------|-------|----------------|------------------|---------------|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

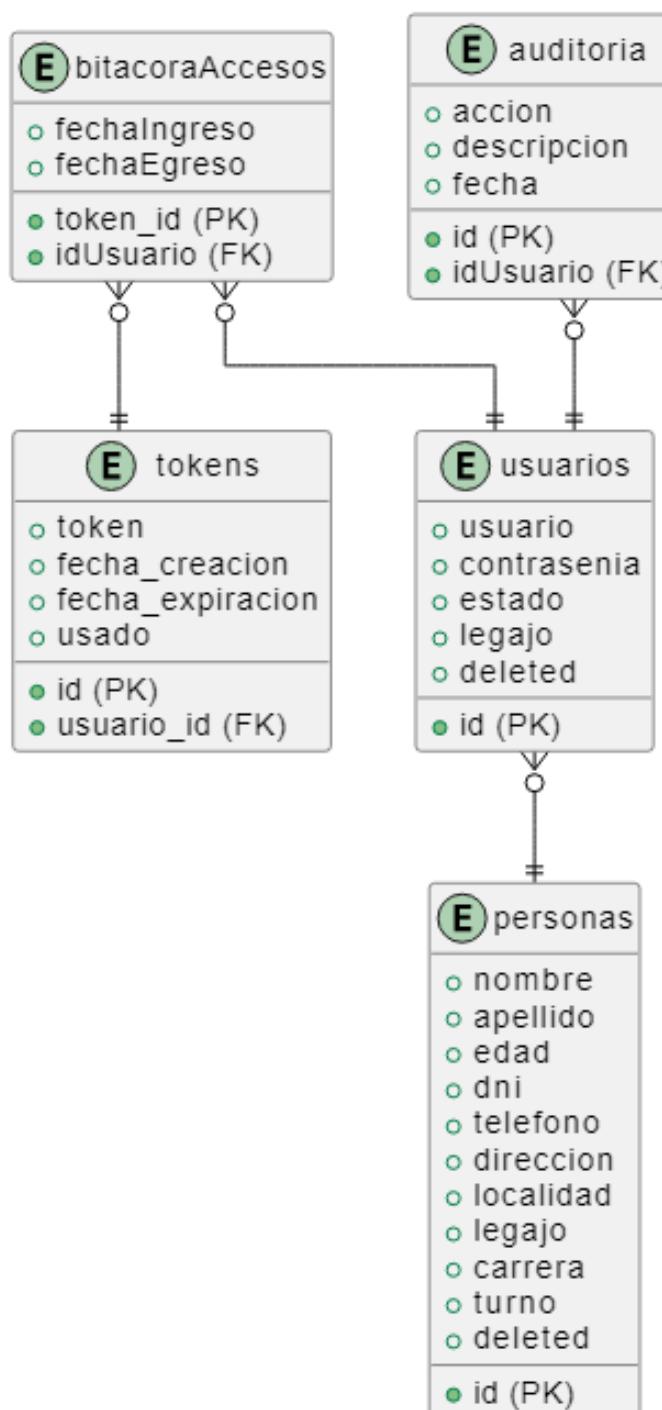
Showing 1 to 8 of 8 entries

[Exportar CSV](#)

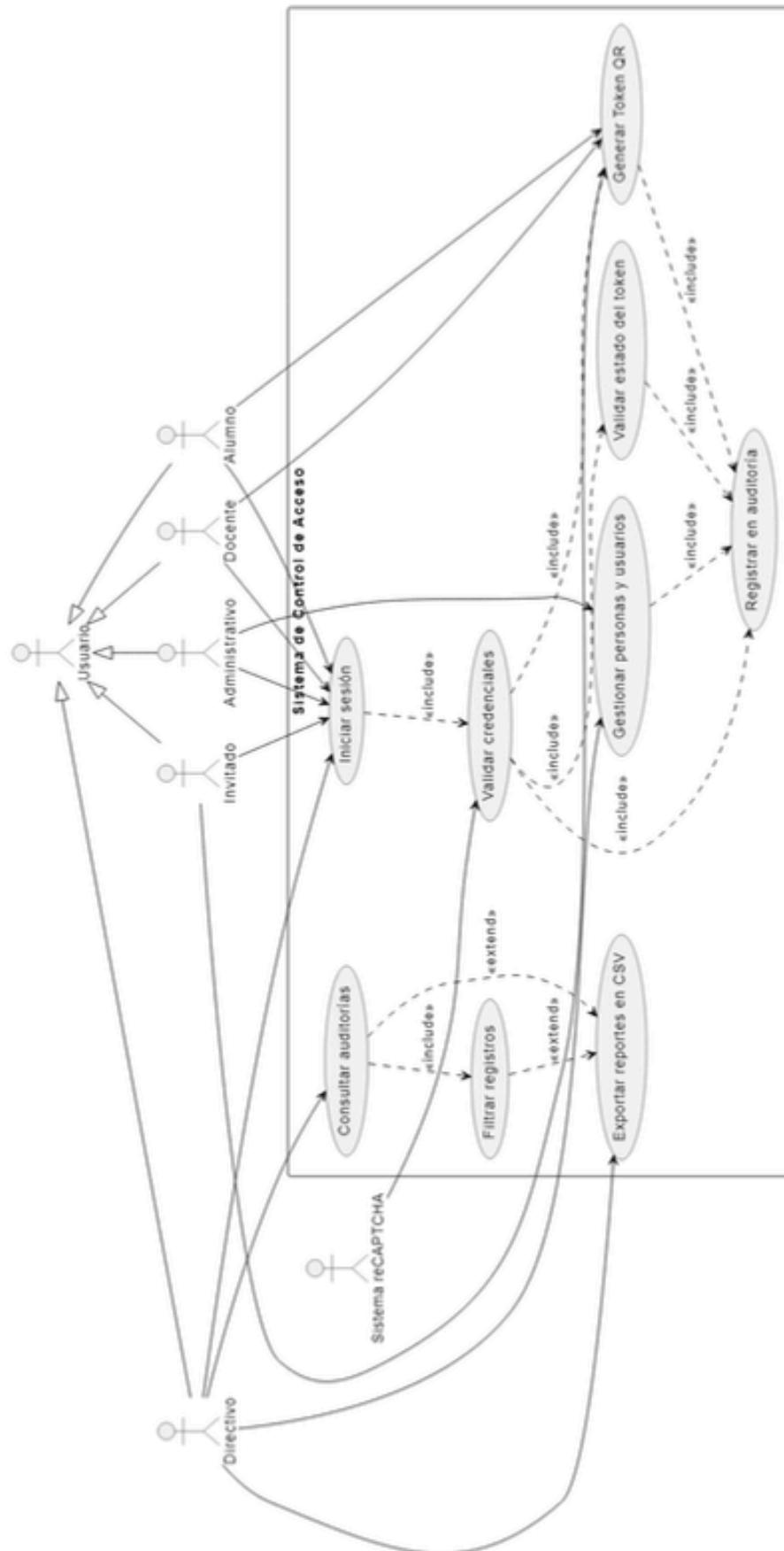
[Previous](#) [Next](#)

4.2 Modelo de Datos (DER)

- bitacoraAccesos: Almacena los registros de acceso de los usuarios, relacionados con los tokens y usuarios.
- tokens: Guarda la información de los tokens de autenticación de los usuarios.
- auditoria: Registra las acciones realizadas por los usuarios.
- usuarios: Contiene la información de los usuarios del sistema.
- personas: Almacena los datos personales de los usuarios.



4.2 Diagrama de Casos de Uso



4.3 Especificación de Casos de Uso

Caso de Uso 1: Iniciar sesión

ID: CU01

Actor Principal: Usuario (Cualquier rol).

Requisitos Asociados: RF01, RF02, RF03.

Precondiciones:

- El usuario debe tener un nombre de usuario y contraseña válidos.

Flujo Principal:

1. El usuario ingresa su nombre de usuario y contraseña.
2. El sistema valida las credenciales.
3. Si las credenciales son válidas, se permite el acceso.
4. Si las credenciales son inválidas, se muestra un mensaje de error.

Postcondiciones:

- El usuario accede al sistema.

Caso de Uso 2: Validar credenciales

ID: CU02

Actor Principal: Sistema.

Requisitos Asociados: RF01.

Precondiciones:

- El usuario ha ingresado sus credenciales.

Flujo Principal:

1. El sistema verifica las credenciales ingresadas.
2. Se registra la acción en la auditoría.

Postcondiciones:

- Se determina si las credenciales son válidas o no.

Caso de Uso 3: Registrar en auditoría

ID: CU03

Actor Principal: Sistema.

Requisitos Asociados: RF10.

Precondiciones:

- Se ha realizado una acción que requiere auditoría.

Flujo Principal:

1. El sistema registra la acción realizada por el usuario en la base de datos de auditoría.

Postcondiciones:

- La acción queda registrada en el sistema.

Caso de Uso 4: Gestionar personas y usuarios

ID: CU04

Actor Principal: Administrativo, Directivo.

Requisitos Asociados: RF04, RF05, RF06.

Precondiciones:

- El usuario debe estar autenticado.

Flujo Principal:

1. El usuario selecciona la opción de gestión de personas y usuarios.
2. El sistema muestra la lista de usuarios.
3. El usuario puede agregar, editar o eliminar usuarios.

Postcondiciones:

- Los cambios se reflejan en la base de datos.

Caso de Uso 5: Generar Token QR

ID: CU05

Actor Principal: Docente, Alumno, Invitado.

Requisitos Asociados: RF07.

Precondiciones:

- El usuario debe estar autenticado.

Flujo Principal:

1. El usuario solicita la generación de un Token QR.
2. El sistema genera el Token QR y lo muestra al usuario.
3. Se registra la acción en la auditoría.

Postcondiciones:

- El Token QR es generado y disponible para el usuario.

Caso de Uso 6: Validar estado del token

ID: CU06

Actor Principal: Sistema.

Requisitos Asociados: RF08.

Precondiciones:

- Se debe tener un Token QR generado.

Flujo Principal:

1. El sistema verifica el estado del Token QR.
2. Se registra la acción en la auditoría.

Postcondiciones:

- Se determina si el Token QR es válido o no.

Caso de Uso 7: Consultar auditorías

ID: CU07

Actor Principal: Directivo.

Requisitos Asociados: RF10, RF11.

Precondiciones:

- El usuario debe estar autenticado.

Flujo Principal:

1. El usuario solicita consultar registros de auditoría.
2. El sistema muestra los registros disponibles.
3. El usuario puede seleccionar filtros para refinar la búsqueda.

Postcondiciones:

- Se muestran los registros de auditoría según los filtros aplicados.

Caso de Uso 8: Filtrar registros

ID: CU08

Actor Principal: Directivo.

Requisitos Asociados: RF11.

Precondiciones:

- Se han consultado registros de auditoría.

Flujo Principal:

1. El usuario aplica filtros a los registros de auditoría.
2. El sistema muestra los registros filtrados.

Postcondiciones:

- Se muestran solo los registros que cumplen con los criterios de filtro.

Caso de Uso 9: Exportar reportes en CSV

ID: CU09

Actor Principal: Directivo.

Requisitos Asociados: RF12.

Precondiciones:

- Se han filtrado registros de auditoría.

Flujo Principal:

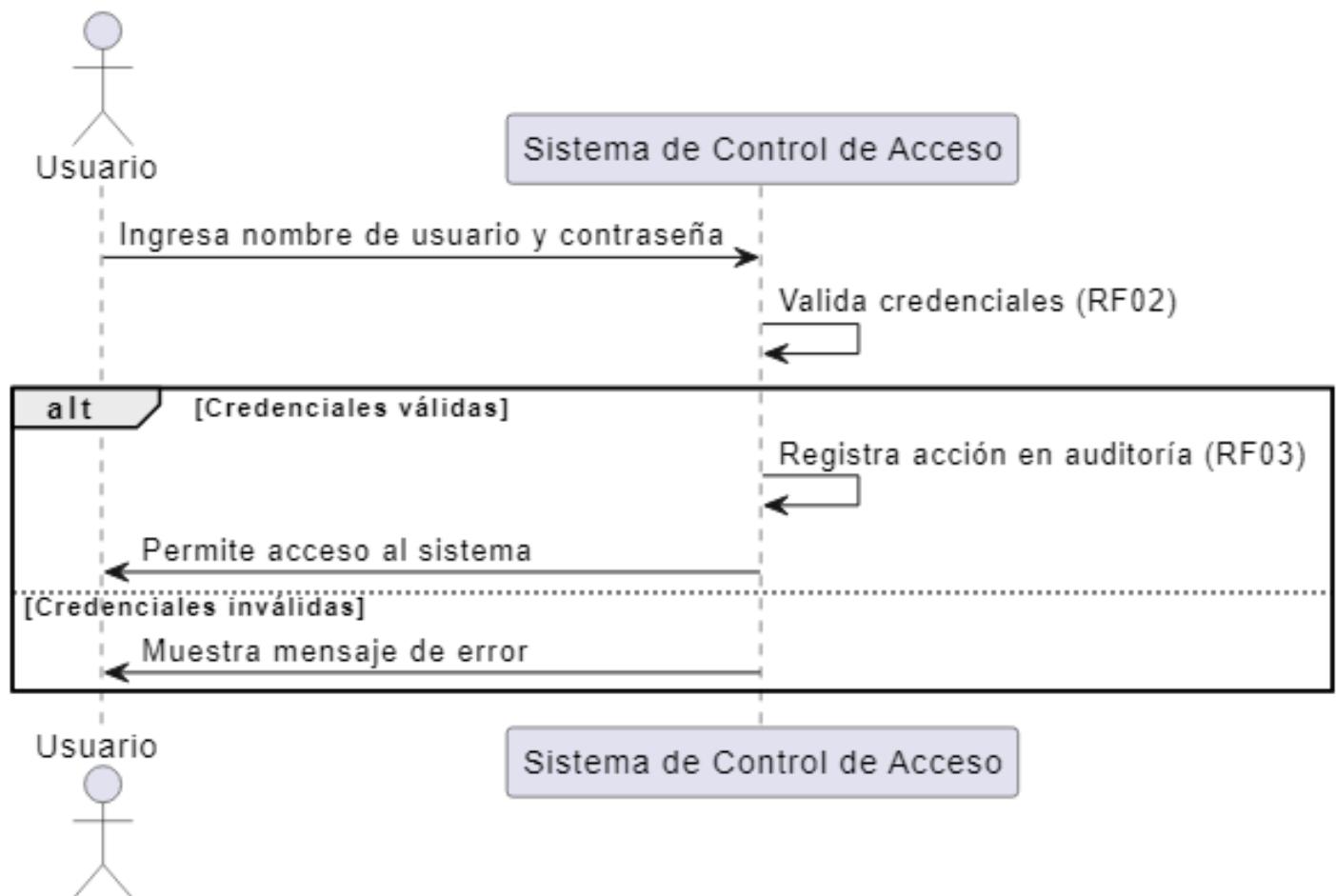
1. El usuario solicita exportar los registros en formato CSV.
2. El sistema genera el archivo CSV.
3. El usuario descarga el archivo.

Postcondiciones:

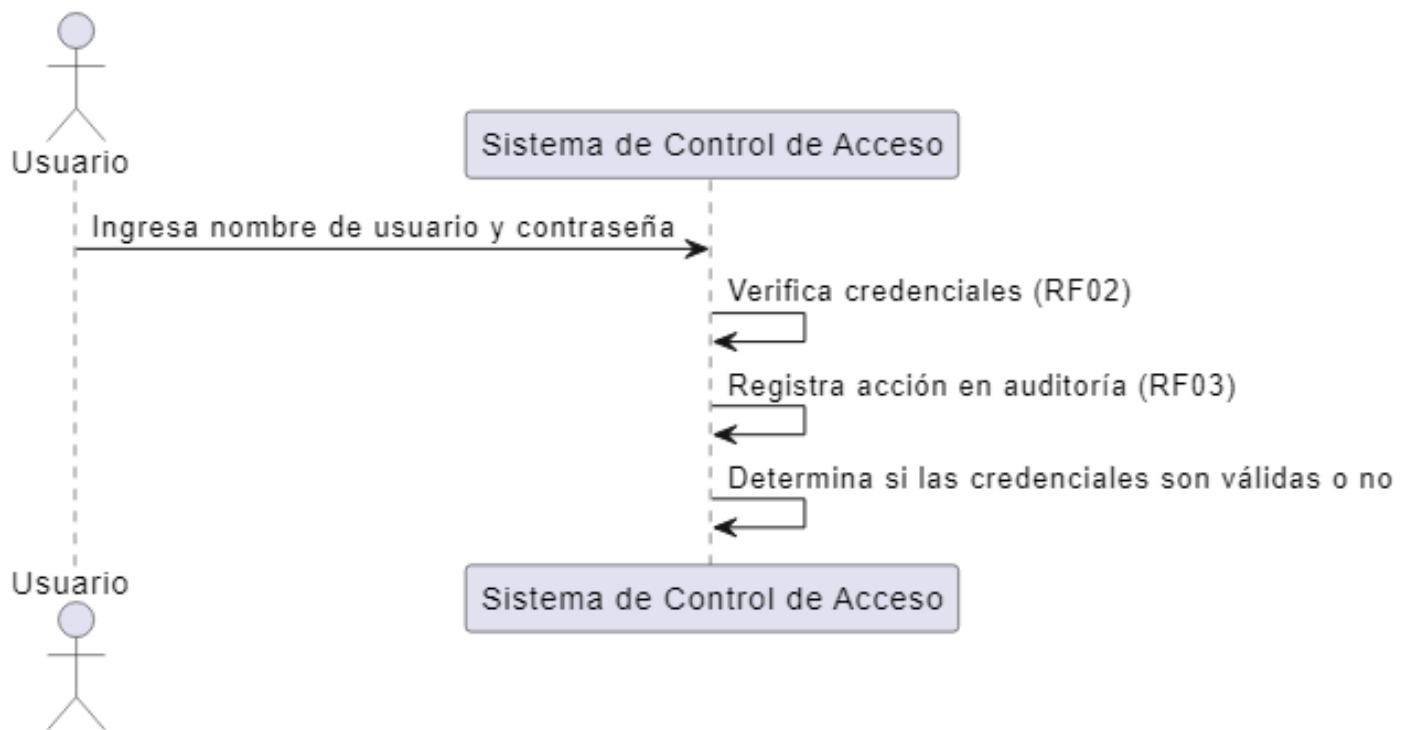
- El archivo CSV es descargado por el usuario.

4.5 Diagramas de Secuencia

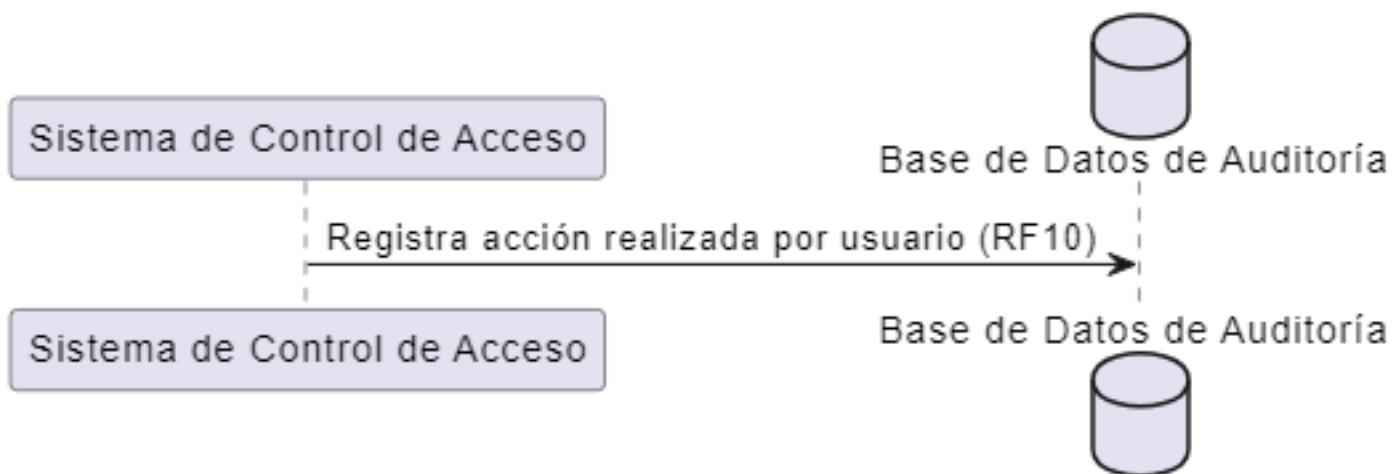
Caso de Uso 1: Iniciar Sesión (CU01)



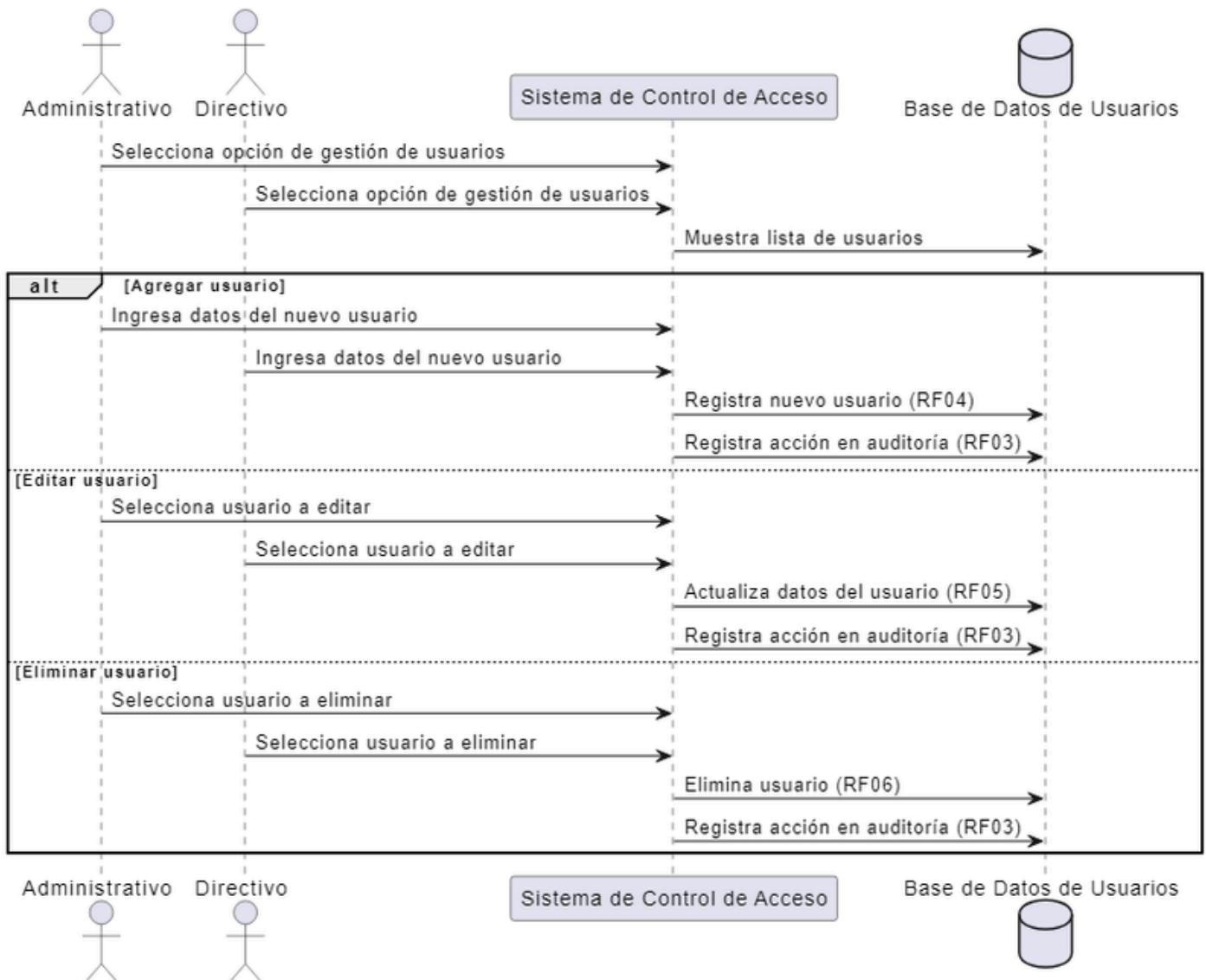
Caso de Uso 2: Validar Credenciales (CU02)



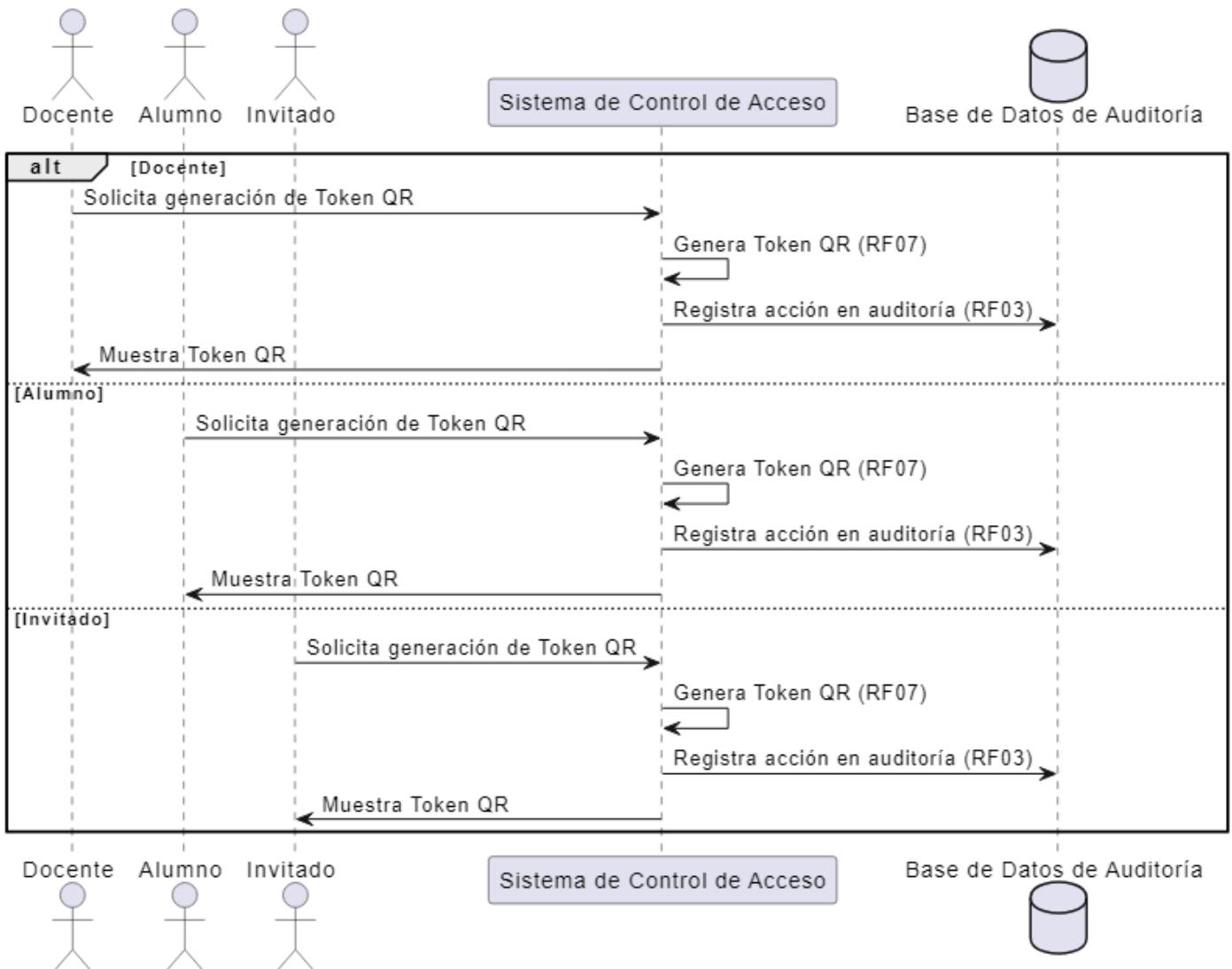
Caso de Uso 3: Registrar en Auditoria (CU03)



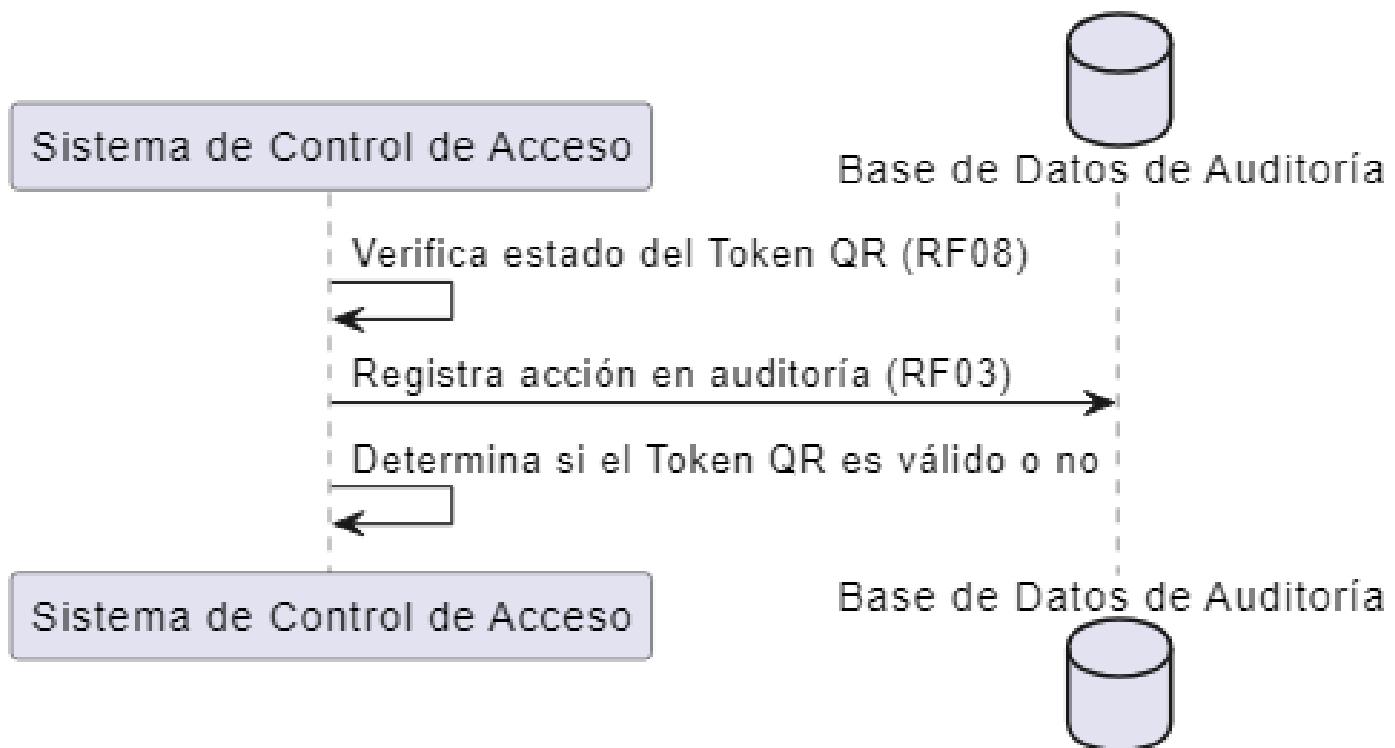
Caso de Uso 4: Gestionar Personas y Usuarios (CU04)



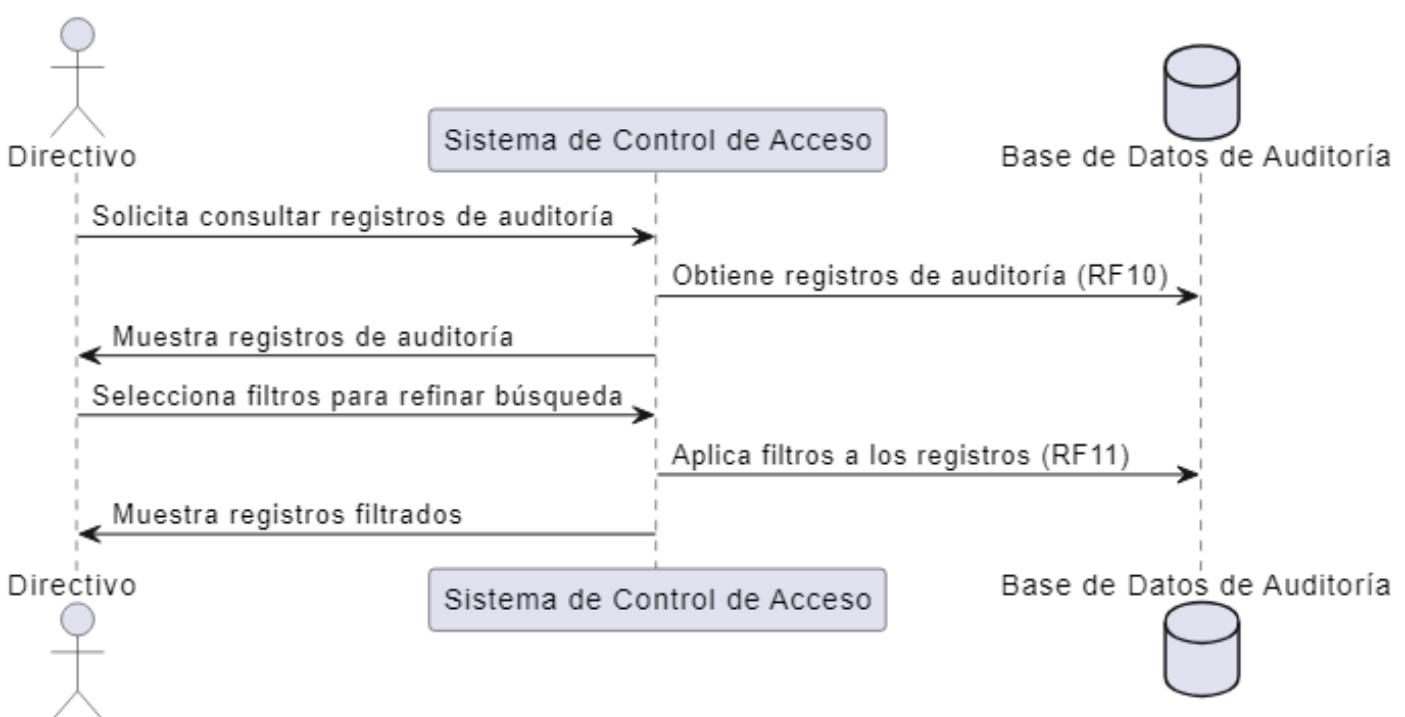
Caso de Uso 5: Generar token QR (CU05)



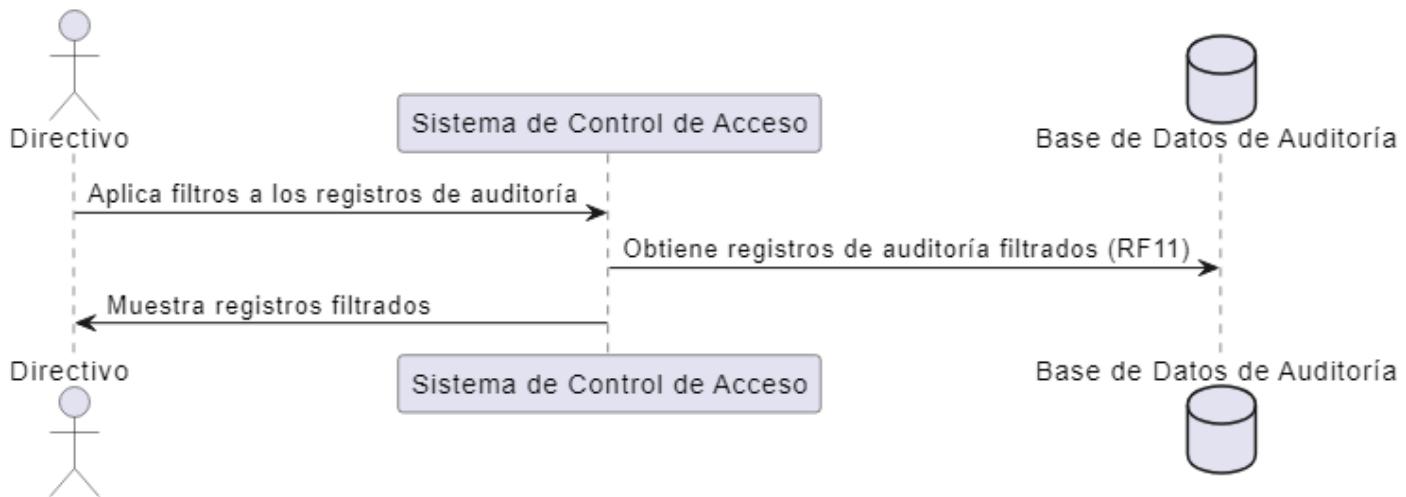
Caso de Uso 6: Validar estado del Token (CU06)



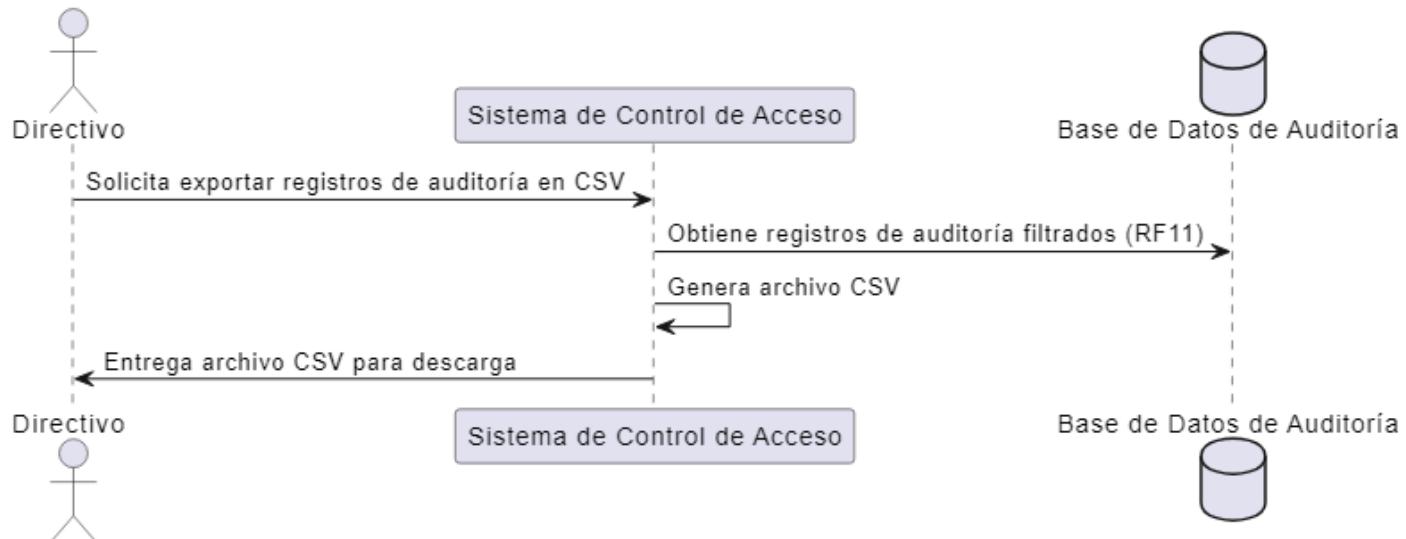
Caso de Uso 7: Consultar Auditorías (CU07)



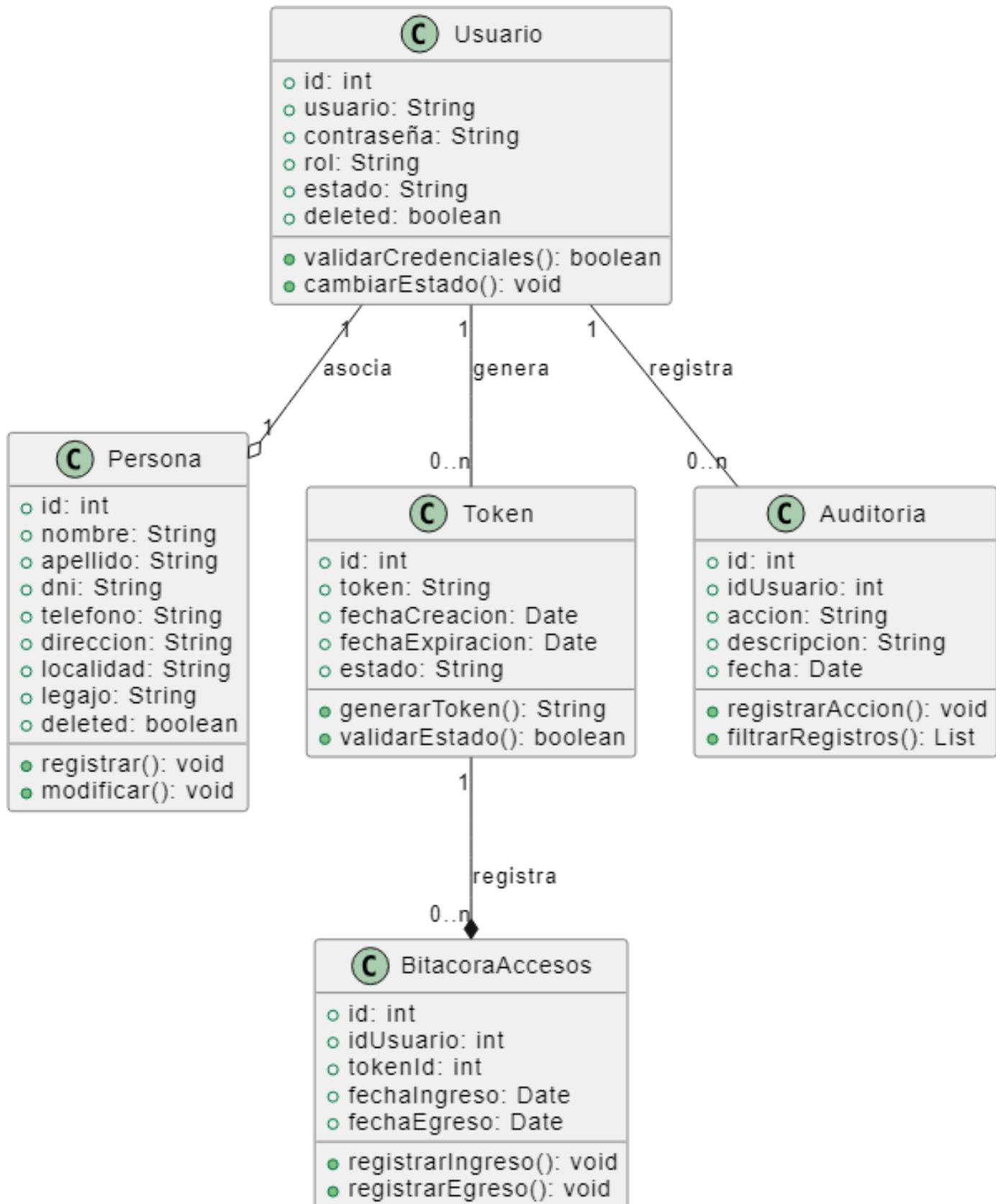
Caso de Uso 8: Filtrar Registros (CU08)



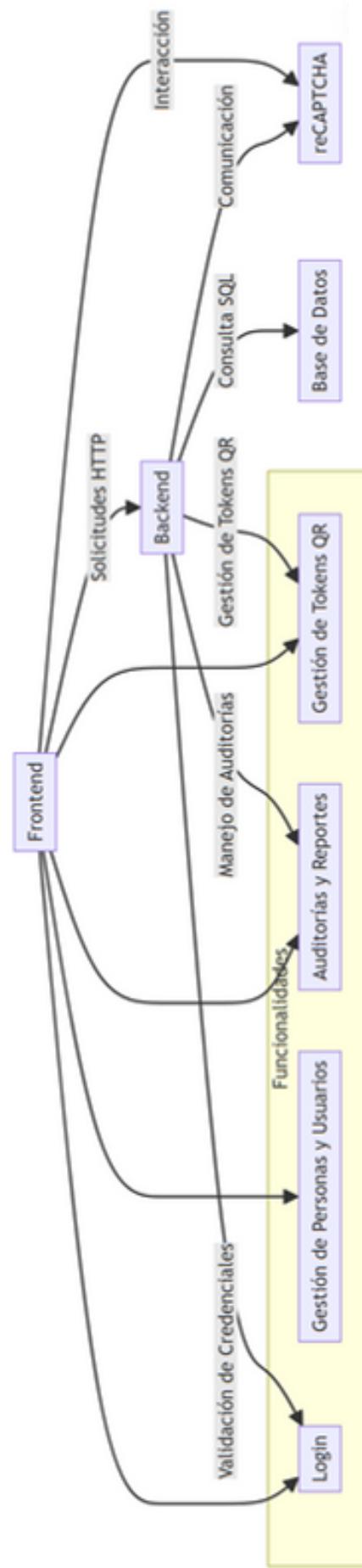
Caso de Uso 9: Exportar reportes en CSV (CU09)



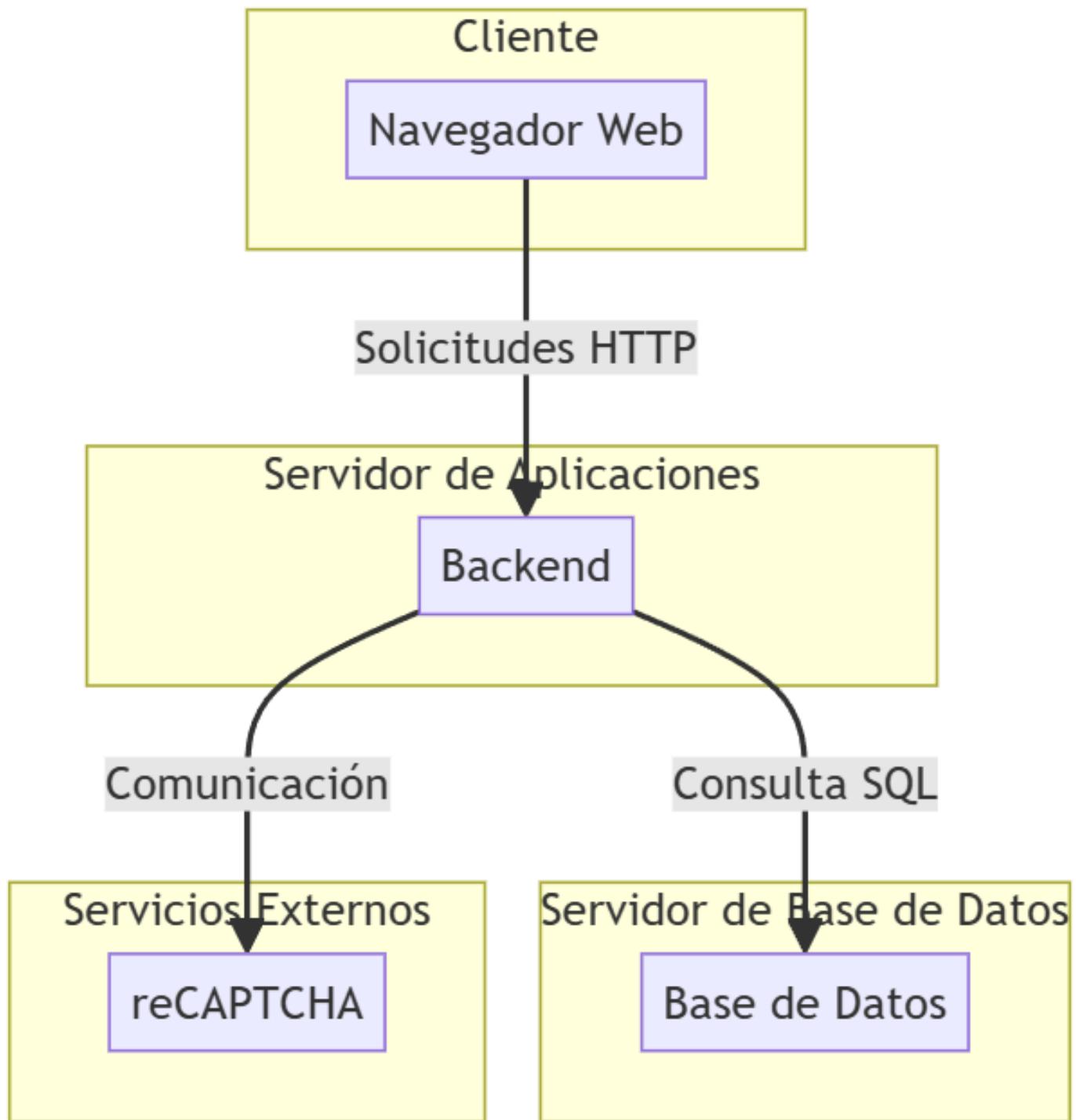
4.6 Diagramas de Clases



4.7 Diagrama de Componentes



4.8 Diagrama de Despliegue



Pruebas

Pruebas Funcionales

| ID Prueba | Descripción | Requisitos Probados | Entrada | Salida Esperada | Criterio de Aceptación | Resultado Obtenido |
|-----------|--|------------------------|---|---|---|---|
| PF01 | Verificar que el sistema valide correctamente las credenciales ingresadas. | RF01, RF02, RF03 | Usuario, contraseña válidos, reCAPTCHA. | Acceso permitido si las credenciales son válidas, mensaje de error si no. | El sistema debe permitir acceso solo a usuarios activos y válidos con reCAPTCHA. | PASSED: Credenciales y reCAPTCHA validados correctamente. |
| PF02 | Verificar creación, edición y eliminación lógica de usuarios/personas. | RF04, RF05, RF06 | Datos completos para altas y bajas. | Datos almacenados/modificados, eliminación lógica aplicada correctamente. | Gestión sin errores y coherencia en los datos registrados. | PASSED: Operaciones realizadas sin errores. |
| PF03 | Verificar generación, validación y expiración de tokens QR. | RF07, RF08, RF09 | Solicitud de generación de token. | Token único generado, validado y expirado según lo configurado. | Tokens deben ser únicos, válidos y expirar correctamente según el tiempo configurado. | PASSED: Tokens generados, validados y expirados correctamente. |
| PF04 | Verificar auditorías, filtros avanzados y exportación en CSV. | RF10, RF11, RF12 | Acciones registradas, solicitud de filtros. | Registros de auditoría reflejados con filtros aplicados correctamente. | Los reportes deben ser precisos y el archivo CSV generarse correctamente. | PASSED: Auditorías y exportaciones funcionan sin problemas. |

Pruebas No Funcionales

| ID Prueba | Descripción | Requisitos Probados | Escenario de Prueba | Criterio de Aceptación | Resultado Obtenido |
|-----------|--|---------------------|--|---|--|
| PNF01 | Evaluar desempeño al generar múltiples tokens simultáneamente. | RNF01 | 100 solicitudes de tokens generadas en un minuto. | Procesar las solicitudes sin afectar el rendimiento. | PASSED: Procesadas en 45 segundos sin errores. |
| PNF02 | Verificar almacenamiento encriptado de contraseñas. | RNF02 | Consultar la base de datos directamente. | Ninguna contraseña debe estar en texto plano. | PASSED: Contraseñas encriptadas correctamente con bcrypt. |
| PNF03 | Evaluar accesibilidad desde navegadores principales. | RNF03 | Acceso al sistema desde Google Chrome, Firefox y Edge. | El sistema debe funcionar correctamente en estos navegadores. | PASSED: Comportamiento uniforme en los navegadores. |
| PNF04 | Garantizar disponibilidad del sistema bajo estrés moderado. | RNF04 | Simulación con 100 usuarios concurrentes accediendo. | El sistema debe permanecer funcional con un uptime del 99.5%. | PASSED: Prueba completada sin caídas. |
| PNF05 | Evaluar usabilidad a través del manual interactivo. | RNF05 | Seguimiento del manual para realizar tareas críticas. | Todas las tareas deben completarse con claridad y sin ambigüedad. | PASSED: Manual fue claro y efectivo. |

Pruebas de Integración

| ID Prueba | Descripción | Componentes Probados | Entrada | Salida Esperada | Criterio de Aceptación | Resultado Obtenido |
|-----------|---|----------------------------------|---------------------------------------|---|---|--|
| PI01 | Verificar integración entre login y la validación de usuarios activos. | Login y módulo de usuarios | Usuario activo o eliminado | Permitir acceso solo a usuarios activos. | El sistema debe denegar acceso a usuarios eliminados. | PASSED: Validación correctamente integrada. |
| PI02 | Verificar relación entre gestión de usuarios y auditoría | Gestión de usuarios y auditoría | Agregar, editar o eliminar un usuario | La acción debe quedar registrada en el módulo de auditoría. | Todas las acciones administrativas deben ser registradas correctamente. | PASSED: Auditoría registra acciones correctamente. |
| PI03 | Probar la interacción entre la generación de tokens y el registro en auditoría. | Generación de tokens y auditoría | Solicitud de token QR | La generación de un token debe registrarse en la auditoría. | Cada token generado debe tener su registro asociado en la auditoría. | PASSED: Generación y registro funcionan bien. |
| PI04 | Validar integración de reportes con los filtros y exportación en CSV. | Reportes, filtros y exportación | Filtros aplicados | Generación correcta de reportes filtrados en formato CSV. | El archivo CSV debe reflejar los filtros aplicados en los reportes. | PASSED: Reportes filtrados exportados correctamente. |

Pruebas Unitarias

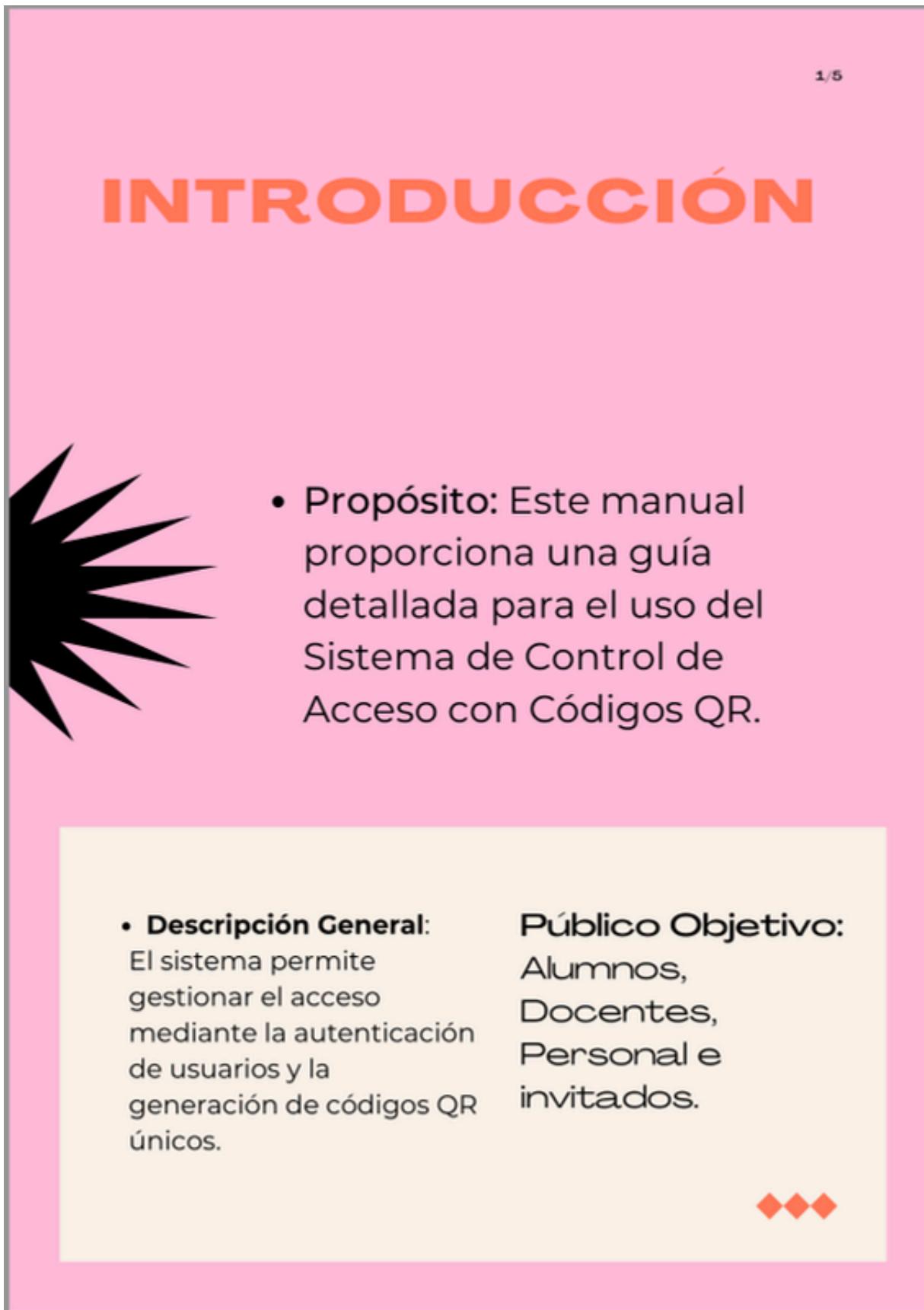
| ID Prueba | Descripción | Unidad Probada | Entrada | Salida Esperada | Criterio de Aceptación | Resultado Obtenido |
|-----------|---|--|---------------------------------------|--|--|--|
| PU01 | Probar la función de validación de credenciales en el login. | Función <code>validarCredenciales()</code> | Usuario y contraseña válidos/erróneos | Retorna <code>true</code> para credenciales válidas y <code>false</code> para inválidas. | La función debe validar correctamente todas las combinaciones posibles. | PASSED: Función validó correctamente. |
| PU02 | Evaluar la función de generación de tokens únicos. | Función <code>generarToken()</code> | Solicitud de token QR | Token único generado correctamente. | Ningún token generado debe repetirse y debe incluir su tiempo de expiración. | PASSED: Tokens únicos generados. |
| PU03 | Probar la función de exportación de reportes en CSV. | Función <code>exportarCSV()</code> | Registros filtrados | Archivo CSV con los datos filtrados. | El archivo debe reflejar exactamente los datos visibles en el reporte. | PASSED: Exportación de CSV sin errores. |
| PU04 | Verificar función de auditoría para registrar acciones administrativas. | Función <code>registrarAuditoria()</code> | Acción realizada por un usuario | Registro correcto de la acción en la tabla de auditoría. | Cada acción debe registrarse con su fecha, descripción y usuario asociado. | PASSED: Auditoría registra correctamente. |

Pruebas del Sistema

| ID Prueba | Descripción | Escenario de Prueba | Entrada | Salida Esperada | Criterio de Aceptación | Resultado Obtenido |
|-----------|---|------------------------------------|---------------------------------|--|---|---|
| PS01 | Evaluar flujo completo de login y acceso al sistema. | Usuario inicia sesión | Usuario y contraseña válidos | Acceso permitido y carga correcta de la interfaz según el rol. | El sistema debe autenticar correctamente y redirigir al módulo correspondiente. | PASSED: Flujo de login funcional. |
| PS02 | Probar flujo de gestión de usuarios desde la creación hasta la auditoría. | Alta, edición y baja de usuarios | Datos de usuario completos | Usuarios creados/editados/eliminados reflejados en auditoría. | Todas las acciones realizadas deben verse reflejadas en los módulos correspondientes. | PASSED: Flujo completo funcional. |
| PS03 | Validar flujo de generación, uso y expiración de tokens QR. | Generación y uso de tokens QR | Solicitud de token QR | Token generado, validado y expirado correctamente. | El sistema debe manejar el ciclo de vida completo de los tokens sin errores. | PASSED: Ciclo de vida de tokens manejado correctamente. |
| PS04 | Evaluar generación de reportes con filtros y exportación en CSV. | Aplicar filtros y exportar reporte | Parámetros de filtros avanzados | Reporte filtrado exportado correctamente en formato CSV. | El archivo generado debe reflejar exactamente los filtros aplicados. | PASSED: Reportes y exportación funcional. |

Anexos

5.1 Manual de usuario (acceso)



INTRODUCCIÓN

1/5

- **Propósito:** Este manual proporciona una guía detallada para el uso del Sistema de Control de Acceso con Códigos QR.

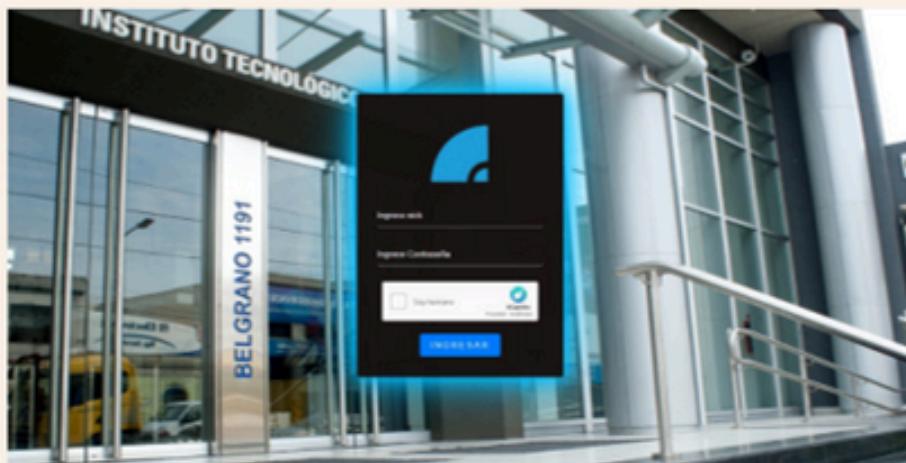
- **Descripción General:**
El sistema permite gestionar el acceso mediante la autenticación de usuarios y la generación de códigos QR únicos.

Público Objetivo:
Alumnos,
Docentes,
Personal e
invitados.

2/5

INICIAR SESIÓN

El Usuario deberá ingresar por medio de la web a la URL:
<http://44.212.37.154/>



Pasos a Seguir:

- **Ingresar nick:** Escribe tu nombre de usuario, tu alias, el que te identifica en este entorno digital.
- **Ingresar Contraseña:** Introduce tu contraseña, esa combinación única que solo tú conoces.
- **Ingresar Captcha:** Resuelve el CAPTCHA que aparece para demostrar que no eres un robot.
- Pulsa el gran botón azul que dice **INGRESAR** y abre las puertas al sistema.



Nota: Si tus credenciales son correctas, accederás al sistema. De lo contrario, revisa tus datos e inténtalo de nuevo.

3/5

BIENVENIDO

Al ingresar correctamente, serás recibido con la siguiente pantalla:



ACCIONES A REALIZAR

- Escanear el Código:** Utiliza tu dispositivo móvil para escanear el código QR que aparece en la pantalla.
- Continuar con la Validación:** Una vez escaneado el código, el sistema procederá a validar tu acceso.

BOTÓN DE SALIDA

- Si deseas salir de la sesión actual, puedes presionar el botón Salir para regresar a la pantalla de inicio de sesión.

Nota: Este paso es crucial para garantizar la seguridad y control del acceso, asegurando que solo personas autorizadas puedan ingresar al sistema.

4/5

LECTURA DE QR/TOKEN

O1

Después de escanear el código QR, serás redirigido a una pantalla, donde se valida el token.

CAMPO DE TOKEN

O2

Verás el token generado en el campo correspondiente.

ENVIAR EL TOKEN

O3

Haz clic en el botón verde "**ENVIAR**" para continuar con la validación del código.



CANCELAR

O4

Si decides no continuar, puedes presionar "**CANCELAR**" para regresar a la pantalla anterior.

Estos pasos te guiarán a través del proceso de inicio de sesión y validación en el sistema. Recuerda siempre verificar que la información ingresada sea correcta para un acceso exitoso.



PANTALLA DE RESULTADO

CASO DE ÉXITO:

Mensaje de Bienvenida

- Si tu acceso es exitoso, verás una pantalla de bienvenida que te da acceso al sistema.



CASO DE ERROR:

Mensaje de Error

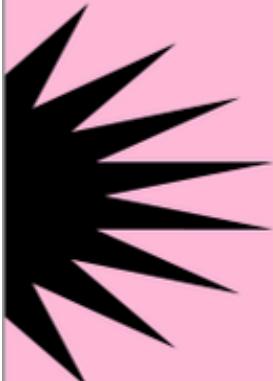
- Si hay un problema con tu acceso, verás una pantalla indicando "ACCESO DENEGADO".
- **Nota:** Revisa tus credenciales o contacta al administrador para asistencia.



5.2 Manual de usuario (Gestión)

1/7

INTRODUCCIÓN



- **Propósito:** Este manual proporciona una guía detallada para el uso de la Gestión de personas y usuarios, del control de acceso.

- **Descripción General:**
El sistema permite gestionar la alta, baja o modificación de registros; mediante la autenticación de usuarios.

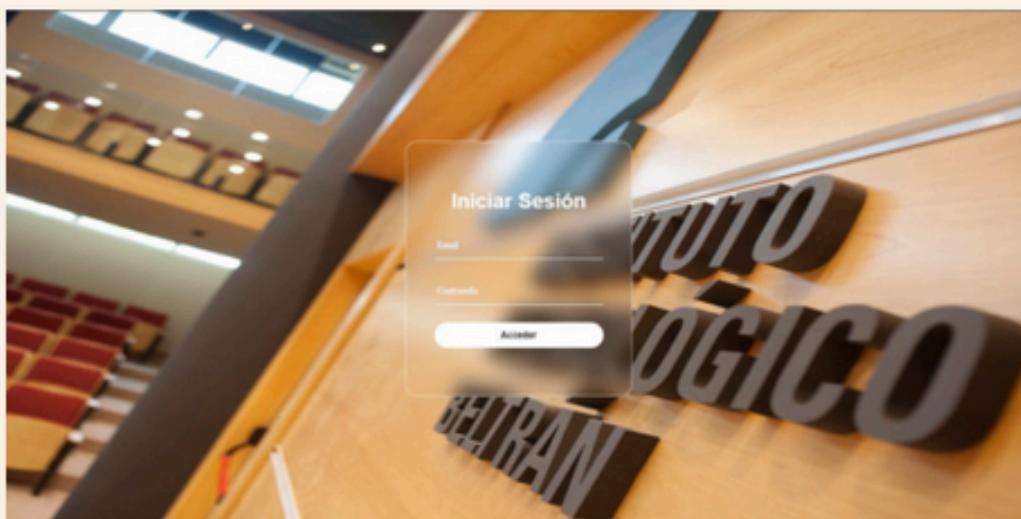
Público Objetivo:
Administrativos
y Directivos



2/7

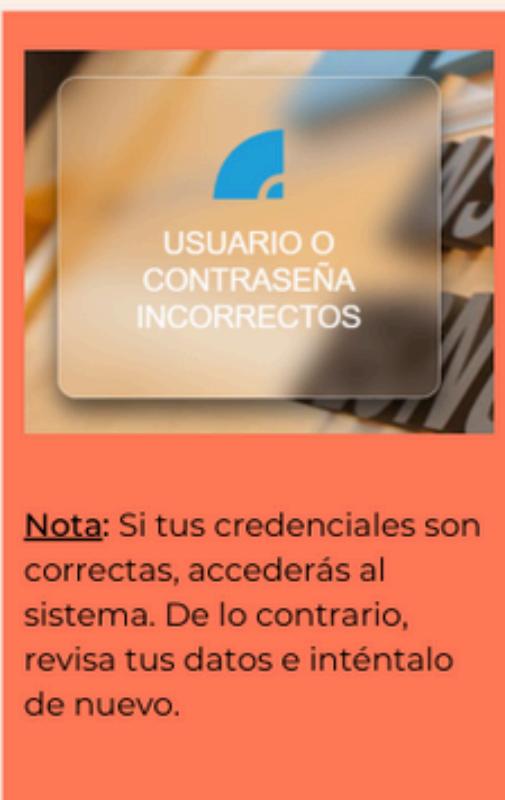
INICIAR SESIÓN

El Usuario deberá ingresar por medio de la web a la URL:
<http://44.212.37.154/gestion.php>



Pasos a Seguir:

- **Ingrese Usuario:**
Escribe tu nombre de usuario, tu alias, el que te identifica en este entorno digital.
- **Ingrese Contraseña:**
Introduce tu contraseña, esa combinación única que solo tú conoces.
- **Pulsa el gran botón azul que dice INGRESAR y abre las puertas al sistema.**



Nota: Si tus credenciales son correctas, accederás al sistema. De lo contrario, revisa tus datos e inténtalo de nuevo.

BIENVENIDO

Al ingresar correctamente, serás recibido con la siguiente pantalla:

Gestión de Personas y Usuarios

[Reportes](#) [Salir](#)

[Agregar Persona](#) [Tabla de Personas](#) [Tabla de Usuarios](#)

TABLA PERSONAS

Mostrar 10 de 6 registros

| ID | Nombre | Apellido | Edad | DNI | Mail | Teléfono | Dirección | Localidad | Lugaro | Carrera | Término | Acciones |
|----|---------|----------|------|----------|--------------------------------|-------------|---------------------|----------------------------|--------|---------|-------------------------------------|-------------------------------------|
| 1 | Luis | Toncic | 36 | 12345678 | ltoncic@gmail.com | 11234567890 | Calle Principal 123 | Avellaneda | L001 | TSAS | Mañana | A B |
| 2 | Diego | Beltrán | 45 | 23456789 | diego@example.com | 1198765432 | Avenida Central 456 | Bernal | L002 | TSAS | Noche | A B |
| 3 | Ricardo | Soriano | 55 | 34567890 | ricardo@example.com | 1145678901 | Plaza Mayor 789 | Guadalupe | L003 | TSAS | Noche | A B |
| 4 | Lucas | González | 30 | 12987654 | lucasgonz@outlook.com | 01123456789 | Avellaneda | L004 | TSAS | Noche | A B | |
| 5 | Lautaro | Jiménez | 24 | 43658123 | lautaro.jimenez@beltran.com.ar | 20531550 | Calle falsa 1234 | Avellaneda, Villa domínico | L001 | TSAS | Tarde | A B |
| 6 | Ivan | Leccina | 26 | 43212345 | ivaleccina@gmail.com | 1123456789 | Av. Costa 123 | Buenaco | L005 | TSAS | Noche | A B |

Mostrando registros del 1 al 6 de un total de 6 registros

[Anterior](#) [Siguiente](#)

ACCIONES A REALIZAR

- Agregar Persona:** ingrese uno a uno los datos de la persona y Presione **Agregar**.

Nota: Si los datos son válidos y el DNI no existe previamente en el sistema, se agregará la nueva persona y se creará un usuario automáticamente con un nombre de usuario basado en el nombre y apellido, y una contraseña predeterminada **Beltran***.

4/7

BAJA Y MODIFICACION PERSONAS

TABLA PERSONAS

Mostrar 10 de 10 registros

Buscar:

| ID | Nombre | Apellido | Edad | DNI | Mail | Teléfono | Dirección | Localidad | Legajo | Carrera | Turno | Acciones |
|----|---------|----------|------|----------|----------------------------------|-------------|---------------------|----------------------------|--------|---------|---|---|
| 1 | Luis | Toncic | 36 | 12345670 | luis.toncic@gmail.com | 1124989099 | Calle Principal 123 | Avellaneda | 1001 | TSAS | Mañana |   |
| 2 | Diego | Klehr | 45 | 23456789 | diego@example.com | 1198765432 | Avenida Central 456 | Bernal | 1002 | TSAS | Noche |   |
| 3 | Ricardo | Soriano | 55 | 34567890 | ricardo@example.com | 1145678901 | Plaza Mayor 789 | Ciudadela | 1003 | TSAS | Noche |   |
| 4 | Lucas | Gonzalez | 30 | 37953754 | lucas.gonzalez@udelar.edu.uy | 01123456789 | Avellaneda 1234 | 1004 | TSAS | Noche |   | |
| 5 | Lautaro | Gómez | 24 | 43658139 | lautaro.jimenez@ibelltron.com.ar | 29531550 | Calle Juana 1234 | Avellaneda, Villa domínico | 1005 | TSAS | Tarde |   |
| 10 | Ivan | Lencina | 26 | 43212345 | ivan.lencina@gmail.com | 1123456789 | Av. Costa Rica 123 | Burzaco | 10015 | TSAS | Noche |   |

01

Presione el botón "Tabla de Personas" y visualizara una tabla con las personas existentes

ELIMINACIÓN

02

Pulse el icono de eliminación  si desea dar de baja un registro

MODIFICACION

03

Si desea modificar algun dato presione el icono de edición  y vera la siguiente pantalla:

ACTUALIZAR PERSONA

04

Haz clic en el botón "Actualizar" una vez que ha modificado el dato deseado.

CANCELAR

05

Si decides no continuar, puedes presionar "Volver" para regresar a la pantalla anterior.

Actualizar Personas

| | |
|---|---------------------|
| Id: | Nombre: |
| 1 | Luis |
| Edad: | DNI: |
| 36 | 12345670 |
| Telefono: | Dirección: |
| 1124989099 | Calle Principal 123 |
| Legajo: | Carrera: |
| L001 | TSAS |
| <input type="button" value="Actualizar"/> | |
| <input type="button" value="Volver"/> | |

5/7

BAJA Y MODIFICACION USUARIOS

TABLA USUARIOS

| ID | Usuario | Contraseña | Rol | Legajo | Acciones |
|----|-----------------|-------------|-----------|--------|---|
| 1 | elpan4s | 1234 | directivo | L001 |   |
| 2 | batataloco | 1234 | docente | L002 |   |
| 3 | r.soriano | beltran2024 | directivo | L003 |   |
| 6 | lautaro.jimenez | holamun | alumno | LJ001 |   |
| 10 | ivan | 1234 | directivo | L0015 |   |

01

Presione el botón "Tabla de Usuarios y visualizara una tabla con los Usuarios existentes

ELIMINACIÓN

02

Pulse el icono de eliminación  si desea dar de baja un registro

MODIFICACION

03

Si desea modificar algun dato presione el icono de edición  y vera la siguiente pantalla:

ACTUALIZAR USUARIO

04

Haz clic en el botón "Actualizar" una vez que ha modificado el dato deseado.

Actualizar Usuarios

| | | | |
|-------------------|-----------|---------------|---------|
| Id: | 1 | Usuario: | elpan4s |
| Role: | Directivo | Estado: | dentro |
| Actualizar | | Volver | |

CANCELAR

05

Si decides no continuar, puedes presionar "Volver" para regresar a la pantalla anterior.



6/7

MODULO AUDITORIA

COMO ACCEDER?

- En la pantalla de inicio, por la parte de arriba a la derecha veras un boton llamado **reportes** (como indica la flecha en la imagen).

| ID | DNI | Mail | Teléfono | Dirección | Localidad | Legajo | Camara | Status | Acciones |
|----|-----------|--------------------------------|-------------|---------------------|-------------------------|--------|--------|--------|----------|
| 36 | 12345678 | luis729@gmail.com | 11234567899 | Calle Principal 123 | Avenida | 1001 | TSAS | Mañana | |
| 45 | 23456789 | diego@example.com | 1198765432 | Avenida Central 456 | Bernal | 1002 | TSAS | Noche | |
| 55 | 34567890 | ricardo@example.com | 1145678901 | Plaza Mayor 789 | Ciudadela | 1003 | TSAS | Noche | |
| 30 | 378956784 | luis.gonzalez@beltran.com.ar | 01123456789 | avenida 1234 | 1004 | TSAS | Noche | | |
| 24 | 456789012 | lautaro.jimenez@beltran.com.ar | 205011550 | Calle Mita 1234 | Avenida, Villa dominico | 1001 | TSAS | Tarde | |
| 26 | 43212345 | luisito@gmail.com | 1123456789 | mi calle 123 | Burzaco | 10015 | TSAS | Noche | |

un total de 6 registros

Anterior Siguiente

Nota: Este botón solo les aparecerá a los usuarios con rol de directivo

QUE PUEDO HACER?

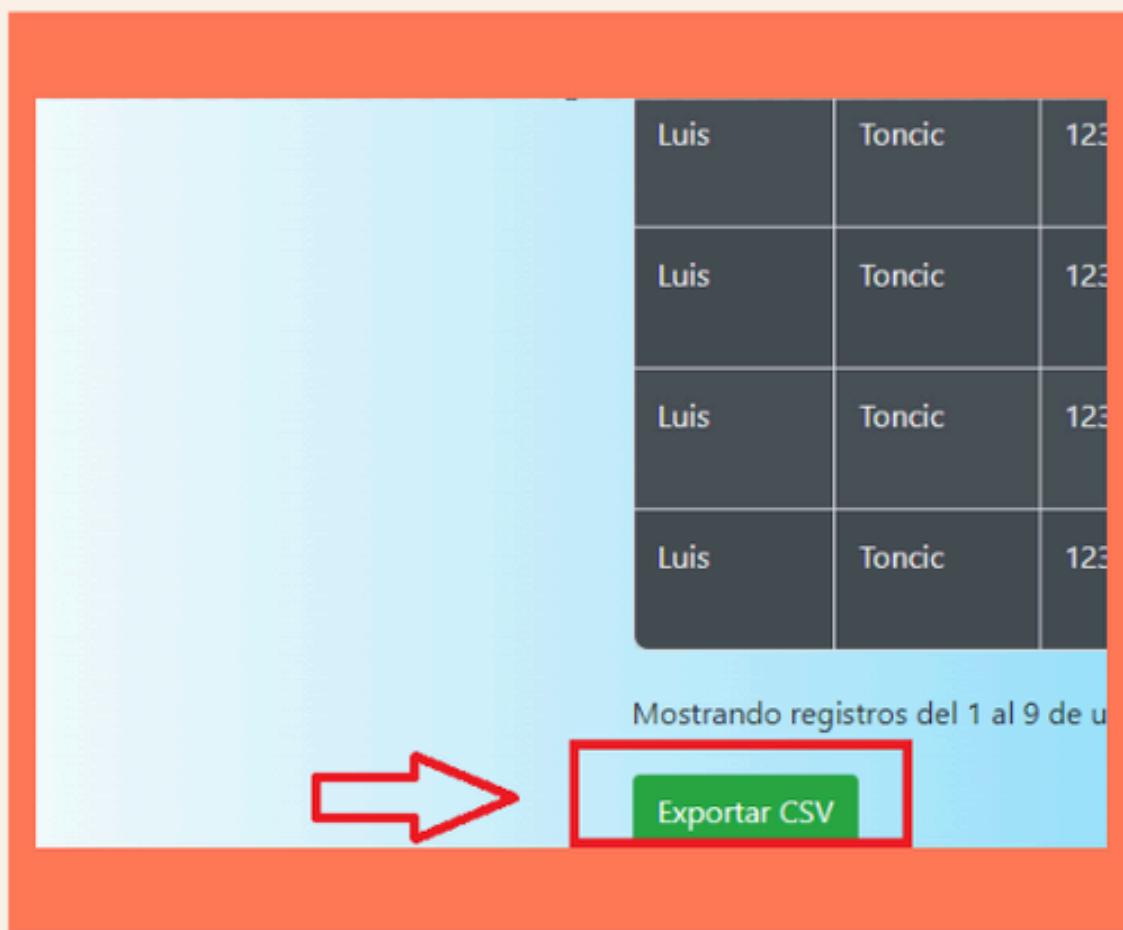
- Una vez dentro del modulo de auditoria, puedes consultar varios reportes y filtrarlos según tus necesidades de búsqueda.

| Nombre | Apellido | DNI | Usuario | Rol | Acción | Descripción | Fecha |
|--------|----------|----------|---------------|---------------|-------------------|--|---------------------|
| Luis | Gómez | 43212345 | luis.gonzalez | administrador | Modificar Reserva | Reserva modificada Luis Gómez, DNI 43212345 | 2024-09-29 21:04:36 |
| Luis | Gómez | 43212345 | luis.gonzalez | administrador | Modificar Reserva | Reserva modificada Luis Gómez, DNI 43212345 | 2024-09-29 22:09:00 |
| Luis | Toncic | 12345678 | luisito | directivo | Modificar Usuario | Usuario modificado luisito, Legajo 1001 | 2024-09-29 16:08:30 |
| Luis | Toncic | 12345678 | luisito | directivo | Modificar Reserva | Reserva modificada Luis Toncic, DNI 12345678 | 2024-09-29 16:08:30 |
| Luis | Toncic | 12345678 | luisito | directivo | Agregar Reserva | Reserva agregada por luisito, DNI 12345678 | 2024-09-29 16:08:45 |
| Luis | Toncic | 12345678 | luisito | directivo | Eliminar Usuario | Usuario eliminado por luisito | 2024-09-29 16:10:12 |
| Luis | Toncic | 12345678 | luisito | directivo | Reserva Eliminada | Reserva eliminada por luisito | 2024-09-29 16:10:12 |

7/7

COMO DESCARGAR REPORTES

- A parte de visualizar los reportes de manera online, esta incluida la funcionalidad que te permite descargar el reporte generado con los filtros elegidos en formato CSV. El botón se encuentra en la parte inferior izquierda del modulo.



The screenshot shows a table with four rows of data:

| | | |
|------|--------|-----|
| Luis | Toncic | 123 |

Below the table, a message reads "Mostrando registros del 1 al 9 de u". A large red arrow points from the left towards a green button labeled "Exportar CSV", which is also highlighted with a red border.

5.3 Historias de Usuario



| Nombre del proyecto | Modulo de acceso | Periodo del informe |
|--------------------------|------------------|-------------------------|
| Propietario del proyecto | Equipo B | |
| Preparado por | Equipo B | 13/05/2024 - 29/05/2024 |

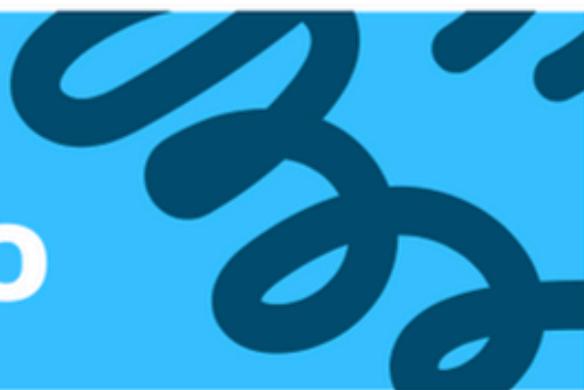
DESCRIPCIÓN

- Proceso (A): Inicio de Sesión del Usuario
- Como usuario de la aplicación, quiero iniciar sesión con mi nombre de usuario y contraseña. Para acceder a mi cuenta y utilizar las funcionalidades de la aplicación.

CRITERIOS DE ACEPTACIÓN

- Campo de Nombre de Usuario: El sistema debe proporcionar un campo de entrada para que el usuario ingrese su nombre de usuario. El campo debe estar claramente etiquetado como "Nombre de Usuario".
- Campo de Contraseña: El sistema debe proporcionar un campo de entrada para que el usuario ingrese su contraseña. El campo debe estar claramente etiquetado como "Contraseña". La contraseña debe ser oculta mientras se escribe (caracteres sustituidos por asteriscos o puntos).
- Botón de Iniciar Sesión: El sistema debe proporcionar un botón de "Iniciar Sesión". Al hacer clic en el botón, el sistema debe validar las credenciales del usuario.
- Validación de Credenciales: El sistema debe verificar las credenciales ingresadas contra la base de datos de usuarios. Si las credenciales son correctas, el usuario debe ser redirigido a la página principal de la aplicación. Si las credenciales son incorrectas, el sistema debe mostrar un mensaje de error claro que indique "Error: Credenciales inválidas".

HISTORIA DE USUARIO



| Nombre del proyecto | Modulo de acceso | Periodo del informe |
|--------------------------|------------------|-------------------------|
| Propietario del proyecto | Equipo B | 13/05/2024 - 29/05/2024 |
| Preparado por | Equipo B | |

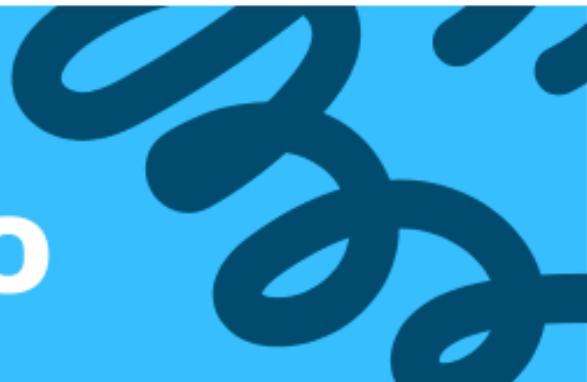
DESCRIPCIÓN

- Proceso (B): Generación del Código QR
- Como usuario autenticado de la aplicación, Quiero generar un código QR único después de iniciar sesión. Para utilizarlo en la autenticación y validación en otros servicios o dispositivos.

CRITERIOS DE ACEPTACIÓN

- Generación del Código QR: El sistema debe generar un código QR único cada vez que un usuario inicia sesión exitosamente. El código QR debe incluir un token único y una marca de tiempo.
- Visualización del Código QR: El sistema debe mostrar el código QR en la pantalla una vez que se haya generado. El código QR debe ser de un tamaño adecuado para ser escaneado fácilmente.
- Seguridad del Código QR: El código QR debe ser válido solo por un período de tiempo limitado (por ejemplo, 5 minutos). Los datos del código QR deben estar cifrados para garantizar su seguridad.
- Almacenamiento del Token: El token y la marca de tiempo deben ser almacenados en la base de datos. El token debe estar marcado como no utilizado al momento de la creación.
- Uso del Código QR: El usuario debe poder escanear el código QR con otra aplicación o dispositivo para validarla. Una vez validado, el token debe ser marcado como utilizado en la base de datos.

HISTORIA DE USUARIO



| Nombre del proyecto | Modulo de acceso | Periodo del informe |
|--------------------------|------------------|------------------------|
| Propietario del proyecto | Equipo B | 3/06/2024 - 26/06/2024 |
| Preparado por | Equipo B | |

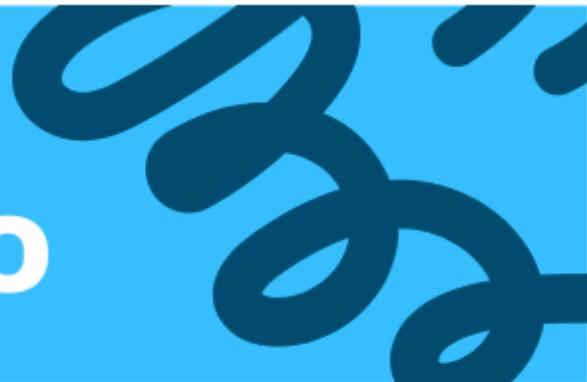
DESCRIPCIÓN

- Proceso (C): Gestión de Usuarios
- Como administrador del sistema, quiero gestionar usuarios, es decir, realizar altas, bajas y modificaciones de usuarios para mantener actualizado el acceso al sistema.

CRITERIOS DE ACEPTACIÓN

- Alta de Usuarios: El sistema debe permitir crear un nuevo usuario ingresando datos como nombre, apellido, edad, DNI, mail, teléfono, dirección, localidad, legajo, carrera, turno, nick, contraseña y rol.
- Modificación de Usuarios: El sistema debe permitir modificar la información de un usuario existente.
- Baja de Usuarios: El sistema debe permitir desactivar a un usuario existente, cambiando su estado.
- Validación de Datos: El sistema debe validar que los campos obligatorios estén completos y que el email y el DNI sean únicos.
- Confirmación de Acciones: El sistema debe solicitar confirmación antes de eliminar un usuario.

HISTORIA DE USUARIO



| Nombre del proyecto | Modulo de acceso | Periodo del informe |
|--------------------------|------------------|------------------------|
| Propietario del proyecto | Equipo B | 8/07/2024 - 14/08/2024 |
| Preparado por | Equipo B | |

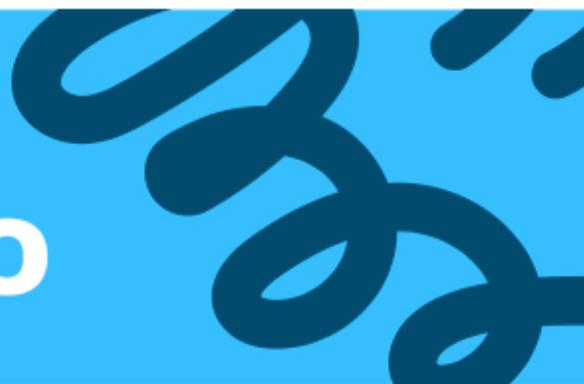
DESCRIPCIÓN

- Como usuario de un sitio web, quiero que se implemente un CAPTCHA en los formularios de registro y inicio de sesión, para evitar el acceso no autorizado mediante bots y asegurar que solo los humanos interactúen con el sistema.

CRITERIOS DE ACEPTACIÓN

- El CAPTCHA debe cambiar con cada recarga de la página o después de un intento fallido.
- El sistema debe bloquear el envío del formulario si el CAPTCHA no es resuelto correctamente. Es decir dar error.

HISTORIA DE USUARIO



| Nombre del proyecto | Modulo de acceso | Periodo del informe |
|--------------------------|------------------|-------------------------|
| Propietario del proyecto | Equipo B | 19/08/2024 - 09/09/2024 |
| Preparado por | Equipo B | |

DESCRIPCIÓN

- Como directivo del sistema, quiero registrar y revisar eventos de auditoria, para generar reportes y alertas sobre el uso del sistema.

CRITERIOS DE ACEPTACIÓN

- Registro de eventos: El sistema debe registrar eventos significativos, cambios en la información de los usuarios y generación de códigos QR.
- Almacenamiento de Datos: los eventos deben ser almacenados en una base de datos con información como el tipo de evento, id del usuario, descripción y fecha.
- Generación de Reportes: el sistema debe permitir generar reportes de auditoria filtrados por fechas, tipo de evento y usuario.
- Consulta de Accesos: El sistema debe permitir la consulta de los registros de accesos, incluyendo la fecha de ingreso y egreso de los usuarios.

Apéndices

Glosario

Acción Administrativa:

Acciones realizadas por un usuario que afectan el sistema o los datos, tales como crear, modificar o eliminar registros.

Auditoría:

Proceso de registrar todas las acciones realizadas en el sistema para garantizar la trazabilidad y el control de accesos, modificaciones y otros eventos.

Autenticación:

Proceso mediante el cual el sistema verifica la identidad de un usuario a través de credenciales (usuario y contraseña).

Base de Datos (DB):

Conjunto organizado de datos que se almacenan y gestionan en un sistema informático. En el contexto de este proyecto, contiene información de usuarios, roles, auditorías, entre otros.

Borrado Lógico:

Método de eliminar registros de manera que se marquen como eliminados pero no sean realmente eliminados de la base de datos. Los registros permanecen en el sistema para auditoría o posibles restauraciones.

Captcha:

Técnica utilizada en formularios web para verificar que el usuario es humano y no un bot. Se utiliza generalmente en el proceso de inicio de sesión o registro.

CSV (Comma-Separated Values):

Formato de archivo utilizado para almacenar datos tabulares, donde cada campo se separa por comas. Se utiliza para la exportación de datos a partir de las bases de datos.



Estado del Usuario:

Indica la situación del usuario dentro del sistema, como "activo", "inactivo", "borrado lógicamente", etc.

Expiración de Token:

Proceso mediante el cual un token pierde su validez después de un periodo de tiempo determinado. Los tokens expiran para evitar el uso no autorizado.

Flujo Alternativo:

Secuencia de pasos que describe una variación en el flujo principal debido a condiciones excepcionales o errores en el sistema.

Flujo Principal:

Secuencia de pasos que describen el comportamiento esperado de un sistema en un escenario normal o típico.

Identificador de Usuario:

Valor único asignado a cada usuario del sistema para identificarlo de manera individual.

Login:

Proceso de inicio de sesión, mediante el cual el usuario accede al sistema proporcionando sus credenciales (usuario y contraseña).

Postcondiciones:

Condiciones que deben cumplirse después de la ejecución de una acción o proceso, reflejando el estado esperado del sistema tras su ejecución.

Precondiciones:

Condiciones que deben cumplirse antes de ejecutar una acción o proceso, asegurando que el sistema está en el estado adecuado para proceder con la operación.

ReCAPTCHA:

Servicio proporcionado por Google que ayuda a proteger los sitios web de registros automatizados (bots). Utiliza desafíos interactivos para verificar que el usuario es humano.

Registro de Auditoría:

Registro detallado de cada acción administrativa que se realiza en el sistema. Permite a los administradores rastrear las actividades realizadas.

Rol de Usuario:

Categoría asignada a cada usuario que define sus permisos y privilegios dentro del sistema, como "administrador", "docente", "alumno", "invitado", etc.

Sistema de Control de Accesos:

Sistema encargado de verificar las credenciales de los usuarios y permitir o denegar el acceso a los recursos del sistema, basado en roles y permisos.

Token:

Cadena única de caracteres generada para autenticar a un usuario o proceso específico, usada en sistemas de autenticación o autorización (por ejemplo, en generación de códigos QR).

Token QR:

Token generado en formato QR para ser utilizado como acceso de entrada a un sistema o recurso. Permite una forma rápida y segura de autenticación a través de dispositivos móviles.

Usuario:

Persona que tiene acceso al sistema, identificado por un nombre de usuario y una contraseña, con privilegios según el rol asignado.

Validación de Credenciales:

Proceso que verifica si el nombre de usuario y la contraseña ingresados coinciden con los registros almacenados en la base de datos para permitir o denegar el acceso.