### ESPECIFICACIÓN DE REQUISITOS DE SOFTWARE

**CONTROL INTELIGENTE DE ASISTENCIA ACADÉMICA DE RECONOCIMIENTO FACIAL E INFORMACIÓN DE DATOS**

**INTEGRANTES:**

**VALERY SINAÍ TRUJILLO QUINTERO MARIA JOSE RODRIGUEZ OLAYA**

**MARIANA VALENZUELA PENAGOS**

**INSTRUCTOR:**

**MOTTA VARGAS JOSÉ DE JESÚS**

**SERVICIO NACIONAL DE APRENDIZAJE – SENA PROGRAMACIÓN DE SOFTWARE – 3145555**

#### 2025

Tabla de contenido

1. [Introducción 4](#_heading=h.hwv6ei2rgovi)
   1. [Planteamiento del problema 4](#_heading=h.2d922oxbzklb)
   2. [Propósito 5](#_heading=h.ajgx6895ezh0)
   3. [Justificación 5](#_heading=h.65w964gc6dlc)
   4. [Objetivo General 5](#_heading=h.hisbnadaj3ah)
      1. [Objetivos específicos 5](#_heading=h.dage04wc062q)
   5. [Alcance 5](#_heading=h.44wktjczf848)
   6. [Personal involucrado 5](#_heading=h.tuc2wrsd35zq)
   7. [Definiciones, acrónimos y abreviaturas 6](#_heading=h.xj02cgokpory)
   8. [Referencias 6](#_heading=h.gh7m991pjeaf)
   9. [Resumen 7](#_heading=h.hsiwadczhrgb)
2. [Descripción General 7](#_heading=h.lk0zl7ni0f1k)
   1. [Perspectiva del producto 7](#_heading=h.6iiupdt4m9sv)
   2. [Características de los usuarios 7](#_heading=h.ryiec8uxhqdc)
   3. [Restricciones 8](#_heading=h.pk00l88aprty)
   4. [Suposiciones y dependencias 8](#_heading=h.pa39j73lz3e8)
3. [Requisitos Específicos 8](#_heading=h.7v20rbwb99nn)
   1. [Requisitos comunes de las interfaces 8](#_heading=h.gij3bpivdoqw)
      1. [Interfaces de usuario 8](#_heading=h.xpc3odampziv)
      2. [Interfaces de hardware 8](#_heading=h.r0pfyzbqhq1x)
      3. [Interfaces de software 8](#_heading=h.pz53agrpuwrj)
      4. [Interfaces de comunicación 9](#_heading=h.t02fn04spqy8)
   2. [Requerimientos Funcionales 9](#_heading=h.1f169f99xf63)
   3. [Requerimientos No Funcionales 27](#_heading=h.bawsdv381o9s)
4. [Requisitos de Casos de Uso 34](#_heading=h.xqdcc2yownzx)
   1. [Diagrama UML de casos de Uso 34](#_heading=h.80tqq4g6lvxn)
   2. Caracterización de Casos de Uso 35

# Introducción.

El SENA ha tenido problemas por el retraso de los aprendices y acumulación de fallas de manera constante, lo que involucra un registro manual obligatorio que deben realizar los instructores. Lo que conlleva a una pérdida de tiempo y mal control, pues los instructores deben llenar la lista por cada uno de los aprendices, preguntar si está o no y anotarlo, todos los días se repite el mismo proceso, en ocasiones hasta se olvida.

## Planteamiento del problema.

A partir de esto ha surgido la siguiente pregunta que soluciona el inconveniente. ¿Cómo automatizar el control de asistencia académica mediante reconocimiento facial para mejorar la precisión y eficiencia del registro que realizan los instructores?

## Propósito.

El presente documento tiene como propósito definir los casos de uso a través de su caracterización y la utilización de diagramas UML, además de definir las especificaciones funcionales y no funcionales para el desarrollo de una aplicación que permita a los usuarios explorar la cocina colombiana y descubrir nuevos restaurantes. Además, la interfaz debería ser fácil de usar, seguro y confiable para los usuarios y dueños de restaurantes, y proporcionar una experiencia agradable para todos.

## Justificación.

En el entorno formativo del SENA, una de las dificultades frecuentes es la ineficiencia y falta de precisión en el control de asistencia de los aprendices durante sus jornadas académicas. Actualmente, los métodos tradicionales como el registro manual en planillas o listas de control son propensos a errores, permiten la suplantación de identidad, y generan retrasos al inicio de las clases, afectando el aprovechamiento del tiempo y la calidad del proceso formativo.

Según un estudio realizado por el Observatorio de la Universidad Colombiana (2022), aproximadamente el 35% de las instituciones educativas en el país reportan dificultades en el control de asistencia, siendo la suplantación y los errores humanos dos de los principales inconvenientes. Además, investigaciones relacionadas con el uso de listas manuales indican que el registro de asistencia puede tomar entre 5 a 10 minutos por clase, lo que representa una pérdida significativa de tiempo en jornadas formativas continuas.

Ante esta problemática, se propone el desarrollo de un sistema innovador de registro automático de asistencia mediante reconocimiento facial, cuyo objetivo principal es garantizar un control preciso, seguro y eficiente del ingreso de los aprendices a las sesiones de formación. Esta solución tecnológica permitirá:

Evitar la suplantación de identidad, asegurando que cada registro de asistencia esté vinculado al rostro único del aprendiz.

Reducir significativamente el tiempo invertido en el control manual de asistencia, lo que optimiza las sesiones formativas.

Fomentar los valores institucionales, como la responsabilidad y la puntualidad, al generar reportes automatizados que evidencien el comportamiento disciplinario de cada estudiante.

## Objetivo General.

Se busca desarrollar un sistema automático de registro y el control de la asistencia de los estudiantes a clases mediante el reconocimiento facial que permita optimizar la gestión de la asistencia, reducir las inasistencias injustificadas, suplantaciones y pérdida de tiempo en asociada al control manual, y proporcionar reportes automáticos para el SENA.

### Objetivos específicos.

1. Seleccionar e investigar las tecnologías adecuadas para el reconocimiento facial.

2. Diseñar la arquitectura del sistema, incluyendo la base de datos para la gestión de usuarios y registros de asistencia.

3. Implementación de Figma para la interfaz de usuario y para la aplicación móvil/tablet.

4. Crear un módulo de generación de reportes automáticos de asistencia, incluyendo inasistencias y patrones de asistencia, para facilitar la evaluación

## Alcance.

Este SRS especifica los requerimientos de software del sistema para la creación de una aplicación:

* + 1. Una aplicación que permite buscar restaurantes con base en el plato seleccionado.
    2. Promoción de nuevos y pequeños restaurantes.

## Personal involucrado.

| **Nombre** | Valery Sinaí Trujillo Quintero |
| --- | --- |
| **Rol** | Analista |
| **Categoría Profesional** | Aprendiz del tecnólogo en análisis y desarrollo software |
| **Responsabilidad** | Análisis de información, diseño y programación |
| **Información de contacto** | valerysinaimexico@gmail.com |

| **Nombre** | Maria Jose Rodriguez Oyola |
| --- | --- |
| **Rol** | Codificación |
| **Categoría Profesional** | Aprendiz del tecnólogo en análisis y desarrollo software |
| Responsabilidad | Análisis de información, codificación y programación |
| **Información de contacto** | m[ariajoserodriguezoyola@gmail.com](mailto:Mariajoserodriguezoyola@gmail.com) |

| **Nombre** | Mariana Valenzuela Penagos |
| --- | --- |
| **Rol** | Base de datos |
| **Categoría Profesional** | Aprendiz del tecnólogo en análisis y desarrollo software |
| **Responsabilidad** | Análisis de información, base de datos y programación |
| **Información de contacto** | valenzuelapenagosm@gmail.com |

## Definiciones, acrónimos y abreviaturas.

| ***Nombre*** | ***Descripción*** |
| --- | --- |
| **Usuario** | Persona que usará la aplicación. |
| **ERS** | Especificación de Requisitos de Software. |
| **RF** | Requerimiento Funcional. |
| **RNF** | Requerimiento No Funcional. |
| **SENA** | Servicio Nacional de Aprendizaje. |
| **CU** | Caso de uso. |

## Referencias.

| **Título del Documento** | **Referencia** |
| --- | --- |
| Standard IEEE 830 - 1998 | IEEE |

## Resumen.

La aplicación consta de cuatro secciones: En la primera sección el usuario se registrará o inicia sesión.

En la segunda sección de la aplicación mostrará una lista de platos típicos, restaurantes y publicidad de pequeños y nuevos restaurantes.

En la tercera sección, al ingresar a un plato o a un restaurante se desglosará información adicional de cada uno, así mismo la opción de dejar una calificación y/o reseña del mismo.

Por último, en la cuarta sección incluirá opciones para personalizar el perfil del usuario o del restaurante.

# Descripción General.

## Perspectiva del producto.

La aplicación busca proporcionar a los usuarios una experiencia integral en la exploración y disfrute de recetas gastronómicas, así como la posibilidad de descubrir nuevos restaurantes. Con un enfoque en la facilidad de uso y la interactividad, la aplicación busca fomentar la conexión entre amantes de la comida y establecimientos culinarios.

## Características de los usuarios.

| **Nombre de usuario** | Administradores |
| --- | --- |
| **Formación** | Tecnólogo en análisis y desarrollo de Software |
| **Actividades** | Administra cada una de las características del software de la aplicación,  atiende cualquier error que se pueda presentar y ayuda a los dueños del ambiente a mantener la información actualizada, |

| **Nombre de usuario** | Instructores |
| --- | --- |
| **Formación** | Natural |
| **Actividades** | Administra la información de los estudiantes, para la asistencia y ellos también interactúan con la aplicación donde se podrán registrar los rostros de los aprendices en compañía de sus datos personales. |

## 

## restricciones.

* + 1. La aplicación requiere acceso a internet.
    2. Los usuarios deben contar con la última actualización de
    3. El software debe ser compatible con diferentes dispositivos móviles y navegadores web.

*.*

## Suposiciones y dependencias.

* + 1. Se asume que los requisitos aquí descritos son estables.
    2. Los equipos en los que se vaya a ejecutar la aplicación deben cumplir los requisitos ante sindicados para garantizar una ejecución correcta de la misma.
    3. Se diseña y unifica con los datos proporcionados por los restaurantes.
    4. Se supone que las reseñas y la publicidad se actualizan en tiempo real.
    5. El software puede depender de la participación activa de los restaurantes para proporcionar información precisa y actualizada.
    6. Se supone una capacidad constante para actualizar y agregar contenido, como nuevas recetas y restaurantes.

# Requisitos Específicos.

## Requisitos comunes de las interfaces.

### Interfaces de usuario

La interfaz de usuario será intuitiva, consistirá en un conjunto de imágenes, listas y campos de textos que harán posible la visualización de información acerca de platos típicos colombianos, recomendaciones de restaurantes para visitar según el tipo de comida que se quiera consumir y avisos promocionales para nuevos y pequeños restaurantes.

### Interfaces de hardware

Será necesario disponer de equipos de cómputos y dispositivos móviles en perfecto estado con las siguientes características:

* Conexión a internet.
* La más reciente versión de software y sistema operativo.
* Almacenamiento suficiente para guardar la aplicación.

### Interfaces de software

·▪ Sistema Operativo: Windows 7 o superior para computadores.

·▪ Sistema Operativo: la última versión disponible de Android y iOS

<<

·▪ Explorador: Mozilla, Chrome , Edge, Brave, Vivaldi, entre otros.

### Interfaces de comunicación

Los servidores y aplicaciones se comunicarán entre sí, mediante protocolos estándares en internet, siempre que sea posible. Por ejemplo, para transferir archivos o documentos deberán utilizarse protocolos existentes (FTP u otros convenientes).

## Requerimientos Funcionales

#### Datos sensibles (RF1)

#### Autoridad de Protección de Datos (RF2)

* Derecho de acceso, actualización y rectificación (RF3)
* Finalidad del tratamiento (RF4)
* Transparencia y Aviso de Privacidad // como última información (RF5)
* Iniciar Sesión(RF6)
* Restablecimiento de Contraseña ( RECUPERAR CONTRASEÑA )(RF7)
* Detección automática de archivos desde USB (RF8)
* Conversión automática de XLS a CSV(RF9)
* Almacenamiento y nomenclatura de los CSV (RF10)
* Notificación de proceso de conversión(RF11)
* Asignar roles a usuarios (RF12)
* Registro: Datos Generados por la máquina
* Permisos según rol
* Ingresar datos biométricos
* Registro usuario
* Panel principal / Home
* Historial
* Registro de Asistencia se especifica // sudrequerimientos
* Programa de Formación // Subrequerimientos
* Horario // Subrequerimientos
* Excusa // Subrequerimiento
* Notificaciones
* Genera Reportes
* Configuración

## Requerimientos Funcionales

| **RF1** | **Datos sensibles** |
| --- | --- |
| Tipo | Normativo / Legal |
| Descripción | Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.   * “Al aceptar, usted certifica que la información ingresada es verídica. En caso de ser menor de edad, confirma que cuenta con la autorización de un adulto responsable.”   ( Con esto, si el usuario miente, la **responsabilidad recae en él o en sus tutores**, no en la aplicación. )   * La imagen facial registrada por el usuario tendrá una vigencia máxima de **12 meses**. Transcurrido este periodo, el sistema solicitará al usuario la **actualización obligatoria de su registro facial** para garantizar la precisión y confiabilidad de la identificación biométrica. * El sistema permitirá al titular conocer, actualizar y rectificar sus datos personales cuando estos sean inexactos, incompletos o parciales * El sistema permitirá al titular solicitar una prueba de la autorización otorgada para el tratamiento de sus datos personales.   Para esto se necesita Copia digital de la autorización registrada. |
| Entrada | Autorización de que el formato de normativa legal este sea vista por el usuario |
| Salida | Reconocimiento y protección especial de los datos sensibles conforme a la ley. |
| Acción | * Identificar los datos que son considerados sensibles. * Proteger la intimidad del titular frente al uso indebido de dichos datos. * Garantizar que su tratamiento no genere discriminación. |
| Criterios de aceptación | * Todo tratamiento de datos sensibles debe realizarse bajo estrictas garantías legales, respetando la intimidad y los derechos fundamentales del titular. * Deben existir **políticas de seguridad de la información** aprobadas, comunicadas y revisadas periódicamente (Control 5.1). * Se deben definir **funciones y responsabilidades claras** en el manejo y protección de datos sensibles (Control 5.2). * En la **gestión de proyectos**, se deben contemplar riesgos y controles de seguridad para el manejo de datos sensibles en todas sus fases (Control 5.8). * Los datos deben estar sujetos a **clasificación de información** según su nivel de sensibilidad (Control 5.12). * Se debe aplicar **etiquetado de la información** sensible para asegurar su protección adecuada (Control 5.13). * Implementar **controles de acceso** que permitan solo a usuarios autorizados gestionar datos sensibles (Control 5.15). * Proteger el acceso mediante **mecanismos de autenticación robustos** (Control 5.17). * Asignar, modificar o revocar **derechos de acceso** conforme a la autorización del titular y roles definidos (Control 5.18). * Si se usan **servicios en la nube**, garantizar que cumplan con requisitos de seguridad establecidos en contratos y controles aplicables (Control 5.23). * Asegurar la **protección de registros** relacionados con accesos, autorizaciones y modificaciones de datos sensibles (Control 5.33). * Cumplir en todo momento con **políticas, reglas y estándares internos y legales** de seguridad de la información aplicables al tratamiento de datos sensibles (Control 5.36). * **7.2 Entrada física**   Garantiza que solo personas autorizadas tengan acceso a las instalaciones físicas donde se procesan o almacenan datos sensibles (servidores, archivos, dispositivos biométricos).  **-8.3 Restricción de acceso a la información** Solo usuarios autorizados deben acceder a los datos sensibles, alineado con el principio de mínima autoridad.  **-8.5 Autenticación segura** Imprescindible para proteger el acceso a datos sensibles con contraseñas fuertes, multifactor o biometría.  **-8.7 Protección contra malware** Evitar que datos sensibles sean comprometidos o expuestos por infecciones de software malicioso.  **-8.10 Eliminación de información** Asegurar que, al eliminar datos sensibles, se haga de forma segura (borrado seguro, destrucción digital/física).  **-8.12 Prevención de fuga de datos (DLP)** Implementar medidas que impidan copias no autorizadas, filtraciones o transferencias indebidas de datos sensibles.  **-8.13 Copia de seguridad de la información** Realizar copias seguras y protegidas de datos sensibles, garantizando disponibilidad ante fallos.  **-8.15 Registro (logging)** Mantener registros de accesos, modificaciones y autorizaciones relacionados con datos sensibles.  **-8.16 Actividades de seguimiento (monitoring)** Supervisar accesos y uso de datos sensibles para detectar anomalías o intentos de acceso indebido.  **-8.17 Sincronización de reloj** Garantizar coherencia temporal en los registros de accesos y auditoría de datos sensibles.  **-8.19 Instalación de software en sistemas operativos** Controlar la instalación de software que pueda comprometer la seguridad de los sistemas que contienen datos sensibles.  **-8.26 Requisitos de seguridad de la aplicación** Las aplicaciones que traten datos sensibles deben cumplir requisitos de seguridad (cifrado, control de sesiones, validación de entradas).  **-8.27 Principios de ingeniería y arquitectura de sistemas seguros** Diseñar e implementar sistemas con medidas de seguridad integradas desde el inicio para proteger datos sensibles.  **8.29 Pruebas de seguridad en desarrollo y aceptación** Validar que las aplicaciones que procesan datos sensibles no tengan vulnerabilidades antes de usarse en producción.  **8.32 Gestión de cambios** Controlar modificaciones en sistemas que manejan datos sensibles para evitar errores o brechas de seguridad.  **8.33 Información de prueba** Evitar el uso de datos sensibles reales en ambientes de prueba, o en caso de usarlos, garantizar su anonimización. |
|  |  |

| **RF 2** | **Autoridad de Protección de Datos** |
| --- | --- |
| Tipo | Normativo / Legal - no funcional |
| Descripción | La aplicación debe informar que la **Superintendencia de Industria y Comercio (SIC)**, a través de la Delegatura para la Protección de Datos Personales, ejerce la vigilancia sobre el tratamiento de los datos personales, garantizando que se respeten los principios, derechos, garantías y procedimientos establecidos en la Ley 1581 de 2012.  En caso de que el usuario sea **menor de edad**, el sistema deberá solicitar el **consentimiento expreso de un adulto responsable** (padre, madre o acudiente), quien autorizará el tratamiento de los datos del menor. |
| Entrada | * Datos.( fecha de nacimiento ) de la persona * Consentimiento del adulto responsable (si el usuario es menor de edad). |
| Salida | * Cumplimiento de la normativa sobre la protección de datos personales. * Registro del consentimiento del adulto responsable cuando aplique. |
| Acción | * Ejercer vigilancia sobre el tratamiento de los datos personales. * Ejercer control sobre el tratamiento de los datos personales conforme a la ley.   Verificar la edad del usuario.   * Si es mayor de edad → continuar normalmente. * Si es menor de edad → solicitar consentimiento del adulto responsable antes de continuar. |
| Criterios de aceptación | * Todo tratamiento de datos personales debe ajustarse a los principios, derechos y garantías previstos en la ley. * Si el usuario es menor de edad, no puede continuar sin el consentimiento registrado de un adulto responsable. * Se guardará en la base de datos la fecha de nacimiento que el usuario ingresó y el consentimiento aceptado, (Si luego se descubre que mintió, tienes evidencia de que la **responsabilidad no era del sistema**.)   **A.5.36 – Cumplimiento de políticas, reglas y estándares de seguridad de la información** → asegurar que el tratamiento de datos cumpla con la Ley 1581 de 2012 y normativas de la SIC.  **A.5.37 – Cumplimiento con requisitos legales y contractuales** → garantizar que se respeten las obligaciones legales de protección de datos personales.  **A.8.23 – Protección de datos personales** → proteger la información de menores y adultos según lo establecido por la ley.  **A.8.31 – Validación de datos de entrada** → verificar la fecha de nacimiento para determinar si el usuario es menor de edad.  **A.5.32 – Trazabilidad de acciones de usuarios** → registrar evidencia de consentimiento del adulto responsable.  **A.5.33 – Protección de registros** → conservar de manera íntegra y segura los consentimientos otorgados.  **A.8.10 – Eliminación de información** → definir políticas sobre eliminación o anonimización de datos personales si un usuario revoca su consentimiento. |

| **(RF 3) Derecho de acceso, actualización y rectificación** | |
| --- | --- |
| Tipo | Normativo / Legal / Funcional |
| Descripción | El titular podrá conocer, acceder, actualizar y rectificar sus datos personales cuando estos sean inexactos, incompletos o parciales, en cumplimiento de la Ley 1581 de 2012. |
| Entrada | - tiene el derecho de autorización de la modificación de los datos. |

| Salida | - “ Sus datos han sido modificados con éxito” |
| --- | --- |
| Acción | - el usuario mira su registro y si comete un error tiene todo el derecho a modificarlo.  - solo de modifica y se actualiza |
| Criterio de aceptación | - el cambio debe ser registrado, ( para que el usuario mire lo que realizo )    **A.5.36 – Cumplimiento de políticas, reglas y estándares de seguridad de la información** → asegurar que el derecho de acceso, actualización y rectificación cumpla con la Ley 1581 de 2012.  **A.5.37 – Cumplimiento con requisitos legales y contractuales** → garantizar la alineación con la normativa sobre protección de datos personales.  **A.8.23 – Protección de datos personales** → asegurar que el proceso de modificación de datos respete la confidencialidad y protección de la información del titular.  **A.8.31 – Validación de datos de entrada** → verificar que los cambios realizados sean válidos, consistentes y no introduzcan errores.  **A.5.32 – Trazabilidad de acciones de usuarios** → registrar en logs la actualización de datos, de modo que el usuario pueda evidenciar qué cambios se hicieron.  **A.5.33 – Protección de registros** → conservar los registros de cambios de manera íntegra y disponible en caso de auditoría o consulta.  **A.8.10 – Eliminación de información** → aplicar en caso de que el titular solicite rectificación mediante eliminación de datos erróneos. |

| **(RF4) Finalidad del tratamiento** | |
| --- | --- |
| Tipo | Normativo / Legal / funcional |
| Descripción | Los datos biométricos y personales sólo se utilizarán para la finalidad específica autorizada por el titular (identificación y autenticación en el sistema). |
| Acción | Prohibir usos distintos al autorizado (ej. marketing, cesión a terceros). |
| Criterio de aceptación | * Cualquier uso indebido debe ser considerado incumplimiento legal.   **A.5.36 – Cumplimiento de políticas, reglas y estándares de seguridad de la información** → asegurar que el tratamiento de datos siga políticas internas alineadas a la ley.  **A.5.37 – Cumplimiento con requisitos legales y contractuales** → garantizar que la finalidad de uso esté ajustada a la Ley 1581 de 2012 y contratos de confidencialidad.  **A.8.23 – Protección de datos personales** → proteger datos biométricos y personales asegurando que no se usen para fines no autorizados.  **A.5.1 – Políticas de seguridad de la información** → documentar y comunicar claramente la finalidad autorizada del tratamiento de los datos.  **A.5.32 – Trazabilidad de acciones de usuarios** → permitir evidenciar si alguien accedió o usó los datos fuera de la finalidad permitida.  **A.5.25 – Evaluación y decisión sobre eventos de seguridad de la información** → en caso de detectar un uso indebido, definir protocolos de respuesta inmediata. |

| **(RF 5 ) Transparencia y Aviso de Privacidad // como última información** | |
| --- | --- |
| Tipo | Normativo / Legal // Funcional |
| Descripción | El sistema deberá mostrar al usuario un aviso de privacidad antes de recolectar datos, informando sobre:   * Responsable del tratamiento. * Finalidades del tratamiento. * Derechos del titular. |
| Acción | * Mostrar aviso y pedir aceptación explícita. |
| Criterio de aceptación | * Ningún dato será recolectado sin aceptación expresa.   **A.5.1 – Políticas de seguridad de la información**  → Deben incluir directrices sobre privacidad, transparencia y consentimiento.  **A.5.36 – Cumplimiento de políticas, reglas y estándares de seguridad de la información**  → Asegura que la aplicación cumpla con políticas internas de privacidad.  **A.5.37 – Cumplimiento con requisitos legales y contractuales**  → Obliga a respetar la Ley 1581 de 2012 y normas sobre aviso de privacidad.  **A.8.23 – Protección de datos personales**  → Protege los datos recolectados y garantiza que el aviso de privacidad se respete en el ciclo de vida del dato.  **A.5.2 – Funciones y responsabilidades de seguridad de la información**  → Define quién es el **responsable del tratamiento** y cómo se gestiona el aviso de privacidad.  **A.5.25 – Evaluación y decisión sobre eventos de seguridad de la información**  → Permite actuar si se detecta recolección de datos sin consentimiento expreso. |

| **(RF 6 ) Iniciar Sesión** | |
| --- | --- |
| Tipo | Funcional |
| Descripción | El sistema permitirá a los usuarios iniciar sesión utilizando credenciales personales (usuario y contraseña).  Durante el proceso de autenticación se garantizará la protección de los datos personales conforme a la Ley 1581 de 2012.  Se informará al usuario que sus credenciales son confidenciales, de uso exclusivo y no deben ser compartidas con terceros.  En caso de olvido de contraseña, se deberá solicitar un proceso de restablecimiento seguro, previa verificación de identidad. |
| Entrada | * Usuario y contraseña. * Solicitud de restablecimiento (si aplica). |
| Salida | * Acceso exitoso al sistema. * Mensaje de error en caso de credenciales incorrectas. * Confirmación de restablecimiento en caso de recuperación de contraseña. |
| Acción | * Solicitar credenciales al usuario. * Validar que correspondan a un usuario registrado. * En caso de error, permitir intentos limitados para proteger la cuenta. * En caso de olvido, ofrecer un mecanismo seguro de restablecimiento. * Garantizar que las contraseñas se almacenan cifradas en la base de datos. |
| Criterio de aceptación | * El inicio de sesión sólo será posible con credenciales válidas. * Las contraseñas nunca podrán almacenarse en texto plano. ( mínimo 8 máximo 15 caracteres * **No guardar contraseñas en texto plano** → Usa algoritmos de hashing como bcrypt, scrypt, * El sistema debe bloquear intentos tras múltiples fallos consecutivos. ( 3 mínimo ) * El restablecimiento de contraseña debe requerir confirmación de identidad (correo, pregunta de seguridad, etc.). * El sistema debe informar al usuario sobre la confidencialidad y uso responsable de sus credenciales. ( texto pequeño )   **A.5.17 – Autenticación de la información**  → Definir y aplicar mecanismos seguros de autenticación (usuario/contraseña, MFA si es posible).  **A.5.18 – Gestión de información de autenticación secreta**  → Proteger credenciales durante todo su ciclo de vida (creación, transmisión, almacenamiento y destrucción).  **A.8.24 – Uso de información de autenticación**  → Implementar buenas prácticas en el uso de contraseñas (mínimo de caracteres, complejidad, no compartir credenciales).  **A.5.34 – Privacidad y protección de la información de identificación personal (PII)**  → Cumplimiento con la Ley 1581 de 2012 para proteger datos personales durante el inicio de sesión.  **A.8.11 – Controles de registro y monitoreo**  → Registrar intentos de inicio de sesión (exitosos y fallidos) y mantener auditoría de accesos.  **A.8.20 – Restricción de acceso a la información**  → Solo se permite el acceso a usuarios con credenciales válidas. **A.8.21 – Segregación de acceso**  → Evitar accesos indebidos y garantizar que cada cuenta sea personal e intransferible.  **A.8.23 – Restricción de intentos de acceso**  → Bloquear la cuenta tras múltiples intentos fallidos (ejemplo: 3 intentos).  **A.5.17 + A.5.18 (combinados)**  → El proceso de restablecimiento debe verificar la identidad del usuario antes de permitir cambio de contraseña (correo, token, pregunta de seguridad). |

| **(RF 7 ) Restablecimiento de Contraseña ( RECUPERAR CONTRASEÑA )** | |
| --- | --- |
| Tipo | Funcional / Normativo - Legal |
| Descripción | El sistema permitirá al usuario restablecer su contraseña en caso de olvido o pérdida.  Este proceso deberá garantizar la confidencialidad de los datos personales, evitando accesos no autorizados.  El restablecimiento deberá realizarse únicamente tras verificar la identidad del titular mediante mecanismos seguros (correo electrónico, código temporal. |
| Entrada | * Solicitud de restablecimiento de contraseña. * Dato de verificación (correo registrado) * **Tokens temporales** para recuperación : válidos sólo unos minutos y de un solo uso. * **Enlaces de recuperación seguros** : enviados al correo del usuario con HTTPS obligatorio. * **Verificación de identidad** : correo, SMS, aplicación autenticadora (2FA). * **Bloqueo por intentos fallidos** : evitar ataques de fuerza bruta. * **Logs de actividad :** registra intentos de recuperación para auditoría.   EJEMPLO ( para poder ver su utilizo ) //  Cuando alguien hace clic en “¿Olvidaste tu contraseña?”   * Ingresa su **correo o usuario**. * Se genera un **token único** y se envía al correo/SMS. * El token expira en **10-15 minutos**. * El usuario ingresa el token y puede crear una **nueva contraseña**. |
| Salida | -Confirmación de identidad verificada.  -Contraseña restablecida exitosamente.  -Mensaje de error en caso de fallar la verificación. |
| Acción | * Solicitar al usuario un dato de verificación (correo, token enviado al celular, etc.). * Validar que la información coincida con la registrada en la base de datos. * Permitir el registro de una nueva contraseña cumpliendo criterios de seguridad (mínimo de caracteres, mayúsculas, números, símbolos). |
| Criterio de aceptación | * El sistema nunca debe mostrar la contraseña anterior. * La nueva contraseña debe cumplir reglas mínimas de seguridad. * El restablecimiento sólo será posible tras verificar la identidad del usuario. * Todo restablecimiento debe quedar registrado en la bitácora (auditoría).   **A.5.17 – Autenticación de la información**  → El proceso de restablecimiento debe ser seguro, validando la identidad del usuario antes de permitir cambios.  **A.5.18 – Gestión de información de autenticación secreta**  → Garantizar que las contraseñas nunca se muestren ni se almacenan en texto plano.  **A.8.24 – Uso de información de autenticación**  → Aplicar políticas de contraseñas fuertes (mínimo caracteres, complejidad, caducidad).  **A.8.23 – Restricción de intentos de acceso**  → Evitar ataques de fuerza bruta mediante bloqueo de múltiples intentos fallidos en recuperación.  **A.5.15 – Seguridad en servicios de red**  → Los enlaces de recuperación deben transmitirse por **HTTPS/TLS** para garantizar la confidencialidad.  **A.5.17 + A.8.20 – Control de acceso**  → Uso de tokens únicos, de un solo uso, con expiración corta (10-15 minutos).  **A.5.34 – Privacidad y protección de PII**  → El proceso de recuperación debe cumplir con la **Ley 1581 de 2012**, protegiendo datos sensibles del usuario.  **A.8.21 – Segregación de acceso**  → Garantizar que el restablecimiento sea individual y no permita accesos indebidos.  **A.8.11 – Registro de eventos de seguridad**  → Todos los intentos (exitosos o fallidos) de restablecimiento deben quedar registrados en logs.  **A.8.16 – Monitoreo de actividades**  → Supervisar intentos sospechosos de recuperación de contraseña para detectar ataques. |

| **(RF 8 ) Definición de Rol al Iniciar Sesión** | |
| --- | --- |
| Tipo | Funcional |
| Descripción | * Al momento de iniciar sesión, el sistema debe solicitar y validar el **rol del usuario** (Aprendiz, Instructor, Administrador, Bienestar, Coordinador, Secretaría).   Con base en el rol registrado, se determinarán automáticamente los permisos que el usuario tendrá dentro del sistema, incluyendo el acceso al botón **“Descomprimir”**. |
| Entrada | * Credenciales de inicio de sesión (usuario y contraseña). * Selección o validación del rol asignado al usuario. |
| Salida | * Interfaz personalizada según el rol. * Visibilidad o no del botón **“Descomprimir”**. |
| Acción | * El sistema valida las credenciales. * Asocia el rol correspondiente al usuario. * Ajusta dinámicamente la interfaz mostrando únicamente las opciones habilitadas para ese rol. |
| Criterio de aceptación | * El Aprendiz no verá el botón “Descomprimir”. * Instructor, Administrador, Bienestar, Coordinador y Secretaría sí verán el botón “Descomprimir”. * Cada usuario solo podrá ejecutar las funciones que correspondan a su rol. * El rol debe quedar registrado en la sesión activa del usuario para auditoría.   **A.5.17 – Autenticación de la información**  → Validar la identidad del usuario antes de asignar un rol.  **A.8.2 – Control de acceso basado en roles (RBAC)**  → Asignar permisos y funciones de acuerdo con el rol definido (Aprendiz, Instructor, etc.).  **A.8.3 – Gestión de privilegios de acceso**  → Garantizar que los permisos sean mínimos y adecuados según el rol (Principio de Mínimos Privilegios).  **A.8.4 – Revisión de derechos de acceso**  → Revisar periódicamente que los roles y permisos sean correctos y no haya accesos indebidos.  **A.8.20 – Restricciones de acceso a información**  → La interfaz debe mostrar solo las opciones autorizadas (ej. el Aprendiz no ve “Descomprimir”).  **A.8.21 – Segregación de acceso**  → Evitar que un rol acceda a funciones de otro, asegurando separación clara de responsabilidades.  **A.8.11 – Registro de eventos de seguridad**  → Registrar el rol asignado a la sesión y las acciones realizadas.  **A.8.16 – Monitoreo de actividades**  → Permitir la trazabilidad para detectar usos indebidos de privilegios. |

| **(RF 9) Recepción Automática de Datos por WiFi** | |
| --- | --- |
| Tipo | Funcional |
| Descripción | * El sistema debe recibir automáticamente los datos enviados por la máquina a través de conexión WiFi y almacenarlos en la base de datos sin intervención manual. |
| Entrada | * Paquete de datos transmitidos por la máquina vía WiFi. |
| Salida | * Registro almacenado en la base de datos. * Confirmación de recepción exitosa. |
| Acción | * Escuchar continuamente los datos enviados por la máquina. * Validar el formato y la integridad de los datos recibidos. * Guardar los datos en la tabla correspondiente de la BD. * Registrar la fecha y hora de recepción. |
| Criterio de aceptación | * Todos los datos enviados deben ser recibidos sin pérdida. * Los registros se deben almacenar de forma inmediata y sin duplicidad. * La conexión WiFi debe ser segura (uso de protocolo HTTPS o similar). * **5.15 Control de acceso** → Garantizar que solo sistemas/máquinas autorizadas puedan enviar datos. * **5.17 Información de autenticación** → Validar identidad del dispositivo/máquina antes de aceptar los datos. * **5.18 Derechos de acceso** → Definir permisos claros sobre quién puede acceder, modificar o leer los datos recibidos. * **5.33 Protección de registros** → Mantener integridad y disponibilidad de registros de transmisión. * **7.2 Entrada física** → Controlar acceso físico a equipos de red y servidores donde se reciben/almacenan los datos. * **8.3 Restricción de acceso a la información** → Evitar que terceros no autorizados capten los datos transmitidos. * **8.5 Autenticación segura** → Validar identidad de la máquina que envía datos vía WiFi. * **8.7 Protección contra malware** → Evitar que software malicioso altere la recepción/validación de datos. * **8.12 Prevención de fuga de datos** → Impedir que los paquetes de datos transmitidos puedan ser copiados o interceptados. * **8.13 Copia de seguridad de la información** → Respaldar los registros recibidos para evitar pérdida de datos. * **8.15 Registro (logging)** → Guardar logs de transmisión (fecha, hora, estado de la conexión). * **8.16 Actividades de seguimiento** → Monitorear la recepción de datos y alertar en caso de fallos. * **8.17 Sincronización de reloj** → Asegurar que todos los registros tengan hora/fecha consistente y verificable. * **8.26 Requisitos de seguridad de la aplicación** → La app que gestiona la recepción debe cumplir estándares de seguridad (cifrado, validación). * **8.27 Principios de ingeniería y arquitectura de sistemas seguros** → Arquitectura segura para la recepción, validación y almacenamiento. * **8.29 Pruebas de seguridad en desarrollo y aceptación** → Antes de implementar, probar que no haya vulnerabilidades en la recepción WiFi. * **8.32 Gestión de cambios** → Controlar cambios en la aplicación de recepción para evitar fallos en la seguridad. |

| **(RF 9. 1 ) Asociación de Registros con Roles** | |
| --- | --- |
| Tipo | Funcional |
| **Integridad de Datos** | * Cada registro debe vincularse a un rol válido (Aprendiz, Instructor, Administrador, Bienestar, Coordinador, Secretaría). * No debe existir en la base de datos un registro sin rol definido. |
| **Consistencia** | * La asignación de roles debe ser **transaccional**: si falla la asociación, el registro no se debe guardar. * El sistema debe garantizar que los roles definidos en RF 8 se mantengan sincronizados con los registros guardados. * Cada registro debe estar vinculado a un rol válido y verificable, asegurando integridad de datos (Controles 5.33, 8.3). * La asignación de roles debe ser **transaccional**: si falla, no se guarda el registro (Control 8.26). * Solo usuarios autenticados y autorizados pueden consultar registros según su rol (Controles 5.15, 5.17, 5.18, 8.5). * La relación entre usuario y rol debe cifrarse para evitar accesos indebidos (Control 8.12). * Cada operación debe quedar registrada con fecha, hora, ID de usuario y rol asignado (Controles 8.15, 8.16, 8.17). * El sistema debe mantener historial de cambios y soportar auditoría completa (Control 5.36). * Se deben realizar copias de seguridad de los registros y roles (Control 8.13). * La lógica de roles debe ser escalable y segura, permitiendo crecer sin comprometer integridad (Controles 8.27, 8.32). * Los entornos de prueba deben proteger los datos reales de roles y usuarios (Control 8.33). |
| Seguridad y Confidencialidad | * Solo usuarios autorizados podrán consultar registros asociados a un rol específico. * La base de datos debe cifrar la relación entre usuario y rol para evitar accesos indebidos. |
| **Auditoría y Trazabilidad** | * Cada registro debe guardar **fecha, hora, ID del usuario y rol asignado**. * Se debe mantener un historial de cambios en caso de que un rol sea modificado. |
| Escalabilidad | El sistema debe permitir crecer en número de roles (ejemplo: si mañana se agrega “Supervisor”), sin modificar la lógica principal de almacenamiento. |

| **(RF 10 ) Gestión de Fichas Técnicas** | |
| --- | --- |
| Tipo | Funcional |
| **Integridad de Datos** | * El sistema permitirá registrar, consultar, modificar y eliminar fichas de formación, cada una con un identificador único (ID de ficha ) cantidad de aprendices asociados. |
| **Entrada** | * ID de la ficha (ejemplo: 3145555, 3145556). Nombre del departamento. Número de aprendices. |
| **Salida** | * Interfaz organizada que muestre todas las fichas con su cantidad de aprendices. |
| **Acción:** | * Crear nuevas fichas. * Modificar datos de una ficha existente. * Eliminar una ficha. |
| **Criterio de aceptación** | * Solo el Administrador puede gestionar fichas. * No debe permitirse duplicar ID de fichas.   **5.1 Políticas de seguridad de la información** Garantiza que la gestión de fichas esté alineada a las políticas generales de seguridad de la información.  **5.2 Funciones y responsabilidades de seguridad de la información** Refuerza que **solo el administrador** puede gestionar fichas (criterio de aceptación).  **5.8 Seguridad de la información en la gestión de proyectos** Aplica si el sistema de gestión de fichas se implementa como proyecto, para identificar riesgos desde el diseño.  **5.12 Clasificación de la información** Las fichas deben clasificarse según su sensibilidad (por ejemplo, datos personales de aprendices).  **5.15 Control de acceso** Solo usuarios autorizados (administradores) pueden crear, modificar o eliminar fichas.  **5.17 Información de autenticación** Debe haber autenticación segura para que solo usuarios válidos puedan gestionar fichas.  **5.18 Derechos de acceso** Define los permisos de gestión de fichas, por ejemplo: administrador crea/modifica, otros solo consultan.  **5.26 Respuesta a incidentes de seguridad de la información** Si se elimina o modifica una ficha de manera indebida, debe existir un plan de respuesta.  **5.28 Recolección de evidencia** Si ocurre un incidente, debe guardarse evidencia (logs de quién eliminó/modificó una ficha). **5.33 Protección de registros** Garantiza integridad, confidencialidad y disponibilidad de los registros de fichas.  **5.36 Cumplimiento de políticas, reglas y estándares** Asegura que la gestión de fichas cumpla con regulaciones (ejemplo: protección de datos personales).  **8.3 Restricción de acceso a la información**  Solo el Administrador puede gestionar fichas (crear, modificar, eliminar).  **8.5 Autenticación segura**  Garantiza que solo usuarios autenticados con credenciales válidas puedan acceder a la gestión de fichas.  **8.10 Eliminación de información**  Asegura que cuando se elimine una ficha, se haga de forma segura, evitando rastros o recuperación indebida.  **8.12 Prevención de fuga de datos**  Aplica porque las fichas contienen información de aprendices y departamentos que no debe filtrarse.  **8.13 Copia de seguridad de la información**  Garantiza respaldos periódicos de las fichas y sus registros.  **8.15 Registro (logging)**  Cada acción sobre fichas debe quedar registrada (quién creó, modificó o eliminó).  **8.16 Actividades de seguimiento (monitoring)**  Permite monitorear cambios, accesos y posibles usos indebidos de la gestión de fichas. **8.17 Sincronización de reloj**  Importante para que los registros de auditoría (fecha y hora de creación, modificación, eliminación de fichas) sean consistentes. |

| **(RF 11 ) Horario de Fichas Técnicas** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | * El sistema permitirá configurar horarios diferenciados por cada día de la semana y franja horaria, ya que la máquina solo maneja un horario único.   De esta manera, se podrán definir turnos distintos (mañana, tarde, noche, horas extras) para cada día de la semana. |
| **Entrada** | * Día de la semana (lunes a domingo). * Franja horaria (ejemplo: 06:00–12:00, 12:00–18:00, 18:00–22:00). * Ficha a la que aplica. |
| **Salida** | * Calendario de horarios semanales configurados en el sistema. |
| **Acción:** | * Crear horarios por día y franja. Modificar horarios ya configurados. * Asociar fichas a esos horarios. |
| **Criterio de aceptación** | * Solo el Administrador puede crear o modificar horarios. * Debe permitirse hasta 24 turnos por día. * No se permiten solapamientos en la misma ficha y franja.   **5.1 Políticas de seguridad de la información**  Respaldan que la gestión de horarios siga políticas aprobadas y consistentes.  **5.2 Funciones y responsabilidades de seguridad de la información**  Define claramente quién (Administrador) puede crear/modificar horarios y quién no.  **5.8 Seguridad de la información en la gestión de proyectos**  El desarrollo del módulo de horarios debe considerar riesgos de seguridad desde su concepción.  **5.12 Clasificación de la información**  Los horarios pueden contener datos sensibles (como grupos de formación, instructores, ambientes). Se deben clasificar adecuadamente.  **5.13 Etiquetado de la información**  Relacionado a la clasificación: si los horarios son internos o confidenciales, deben etiquetarse para evitar uso indebido.  **5.15 Control de acceso**  Solo el Administrador puede modificar los horarios. Control fundamental en este RF.  **5.17 Información de autenticación**  Garantiza que solo usuarios autenticados gestionen horarios.  **5.18 Derechos de acceso**  Asigna y revoca permisos según roles (Administrador, Instructor, Aprendiz).  **5.33 Protección de registros**  Los logs de creación, modificación o eliminación de horarios deben protegerse (no alterarse).  **5.36 Cumplimiento de políticas, reglas y estándares**  Garantiza que la gestión de horarios cumpla con las normas y políticas institucionales.  **8.3 Restricción de acceso a la información**  Solo el Administrador puede crear o modificar horarios.  **8.5 Autenticación segura**  Asegura que solo usuarios autenticados gestionen los horarios.  **8.10 Eliminación de información**  Si se elimina un horario, debe hacerse de forma segura (sin dejar datos huérfanos en las fichas asociadas).  **8.12 Prevención de fuga de datos**  Los calendarios de fichas no deben exponerse a usuarios no autorizados.  **8.13 Copia de seguridad de la información**  Respaldo periódico de los calendarios y horarios ya configurados.  **8.15 Registro (logging)**  Se debe registrar qué usuario creó, modificó o eliminó un horario.  **8.16 Actividades de seguimiento (monitoring)**  Permite rastrear y auditar cambios en la gestión de horarios.  **8.17 Sincronización de reloj**  Fundamental para garantizar que los horarios creados y registrados no tengan inconsistencias de tiempo. |

| **(RF 11.1 ) Asociación de Instructores a Horarios de Ficha** | |
| --- | --- |
| Tipo | Funcional |
| **Integridad de Datos** | * El sistema permitirá asignar instructores a las fichas en función del horario y del día de la semana. * Un mismo instructor puede cubrir varios horarios, y una ficha puede tener instructores distintos según el día o franja horaria. |
| **Entrada** | * ID de la ficha. * Día de la semana. * Franja horaria. * ID del instructor. |
| **Salida** | * Lista de instructores asignados a cada ficha por día y horario. |
| **Acción:** | * Asignar un instructor a un horario de ficha. * Modificar la asignación (cambiar de instructor). * Consultar instructores por ficha y día. |
| **Criterio de aceptación** | * Cada franja de la ficha debe tener al menos un instructor asignado. * No se permiten asignaciones duplicadas (mismo día, franja, ficha e instructor). * Solo el Administrador puede gestionar estas asignaciones.   **5.1 Políticas de seguridad de la información**  Asegura que la asignación de instructores se haga bajo políticas claras.  **5.2 Funciones y responsabilidades**  Refleja que *solo el Administrador puede gestionar las asignaciones*.  **5.8 Seguridad en la gestión de proyectos**  El desarrollo de este módulo debe contemplar riesgos como asignaciones erróneas o duplicadas.  **5.12 Clasificación de la información**  Las asignaciones contienen datos personales (instructores, horarios, fichas). Deben clasificarse como información sensible.  **5.13 Etiquetado de la información**  Si las asignaciones se exportan o consultan, deberían etiquetarse como “Uso interno” o “Confidencial”.  **5.15 Control de acceso**  Garantiza que solo usuarios autorizados (Administrador) puedan crear/modificar asignaciones.  **5.17 Información de autenticación**  Refuerza que el acceso al módulo de asignación de instructores requiera credenciales válidas.  **5.18 Derechos de acceso**  Diferencia roles (Administrador vs. Instructor que solo consulta su horario).  **5.33 Protección de registros**  Los cambios en asignaciones deben quedar registrados en logs, protegidos contra alteración.  **5.36 Cumplimiento de políticas**  Asegura que la asignación de instructores cumpla con regulaciones laborales y de seguridad.  **8.2 Gestión de identidades**  Cada instructor debe tener una identidad única en el sistema para asociarlo a horarios.  **8.3 Gestión de derechos de acceso**  Define permisos para que instructores solo consulten y administradores gestionen asignaciones.  **8.4 Gestión de información confidencial**  Protege datos personales de instructores (no se deben exponer más allá de lo necesario).  **8.9 Registro y monitoreo de actividades**  Los cambios de asignación deben registrarse (qué admin hizo el cambio, cuándo, qué instructor fue reasignado).  **8.10 Validación de entradas**  Evita asignaciones duplicadas (mismo día, franja, ficha e instructor) → criterio de aceptación clave. |

| **(RF 12 ) Cálculo de retrasos** | |
| --- | --- |
| Tipo | Funcional |
| **Integridad de Datos** | * El sistema calculará automáticamente los retrasos de los usuarios comparando la **hora real de entrada** (recibida desde la máquina) con la **hora configurada en el horario de la ficha**. |
| **Entrada** | * Hora de entrada registrada por la máquina. * Hora de entrada esperada según el horario configurado en el sistema. |
| **Salida** | * Registro del retraso (minutos de tardanza). * Historial del usuario con sus entradas y retrasos. |
| **Acción:** | * Comparar hora de entrada registrada con la esperada. * Guardar en BD el tiempo exacto de retraso. * Mostrar retrasos en el historial del usuario. |
| **Criterio de aceptación** | * Todo retraso debe calcularse en minutos. * Si la entrada es igual o anterior a la hora esperada → 0 minutos de retraso. * El historial debe mostrar fecha, hora de entrada y retraso. * **5.1 Políticas de seguridad de la información**  Para asegurar que el manejo de registros de entrada/salida siga políticas definidas. * **5.2 Funciones y responsabilidades**  Solo ciertos roles (Administrador o Supervisor) deben poder consultar, modificar o auditar retrasos. * **5.12 Clasificación de la información**  Los registros de asistencia son información sensible de los empleados → deben clasificarse. * **5.13 Etiquetado de la información**  Al exportar o consultar retrasos, los reportes deben ir identificados como "Confidencial". * **5.15 Control de acceso**  Restringir quién puede ver los retrasos o modificarlos. * **5.17 Información de autenticación**  Garantizar que solo usuarios autenticados ingresen y accedan a registros de asistencia. * **5.18 Derechos de acceso**  Definir permisos según rol (ejemplo: empleados solo consultan su historial, administradores acceden a todos). * **5.33 Protección de registros**  Asegurar la integridad y disponibilidad del historial de retrasos (no debe ser alterado sin control). * **5.36 Cumplimiento de políticas y regulaciones**  Asegurar que los registros cumplan con la normatividad laboral y de protección de datos. * **8.3 Restricción de acceso a la información**  Solo usuarios autorizados pueden acceder al historial de retrasos. * **8.5 Autenticación segura**  El ingreso a la plataforma para ver o calcular retrasos debe tener autenticación robusta. * **8.15 Registro (Logging)**  Los accesos y cambios a los datos de retrasos deben quedar registrados. * **8.16 Actividades de seguimiento (Monitoring)**  Monitorear intentos de manipulación o accesos indebidos a registros de asistencia. * **8.17 Sincronización de reloj**  Fundamental: las horas de entrada deben ser consistentes y sincronizadas para calcular retrasos correctamente. * **8.33 Información de prueba**  Si se realizan pruebas sobre este módulo, no deben usarse datos reales de empleados. |

| **(RF 13 ) Estadísticas personales del usuario** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción:** | * Cada usuario podrá ver su propio historial y estadísticas personales de puntualidad |
| **Entrada** | * Registros de asistencia del usuario. |
| **Salida** | * Lista de entradas con sus retrasos. * Gráficas de puntualidad personal. |
| **Acción:** | * Mostrar historial en orden cronológico. * Calcular el total de retrasos y puntualidad personal. |
| **Criterio de aceptación** | * Debe poder visualizarse de manera resumida (ejemplo: "Ficha 3145555: 85% puntualidad, 15% retrasos"). * El administrador e instructor pueden acceder a esta vista. * **5.1 Políticas de seguridad de la información**  Para que el acceso y presentación de estadísticas siga lineamientos claros. * **5.2 Funciones y responsabilidades**  Definir quién puede ver qué: el usuario solo su historial; el administrador e instructores pueden consultar estadísticas de los usuarios asignados. * **5.12 Clasificación de la información**  Las estadísticas de asistencia son datos sensibles de desempeño → deben protegerse. * **5.13 Etiquetado de la información**  Reportes exportados deben marcarse como “Confidencial”. * **5.15 Control de acceso**  Restringir que cada usuario solo pueda consultar su propia información, y administradores/instructores solo la de sus fichas asignadas. * **5.17 Información de autenticación**  Autenticación obligatoria para acceder al historial personal. * **5.18 Derechos de acceso**  Perfiles definidos: el usuario no puede ver estadísticas de otros. * **5.33 Protección de registros**  Evitar alteración o pérdida del historial que alimenta las estadísticas. * **8.3 Restricción de acceso a la información**  Solo el dueño del historial, administradores e instructores autorizados pueden consultarlo. * **8.5 Autenticación segura**  El sistema debe exigir autenticación robusta para acceder a la vista de estadísticas. * **8.12 Prevención de fuga de datos**  Proteger la exportación de reportes de puntualidad (evitar copias indebidas). * **8.15 Registro (Logging)**  Registrar quién accede a estadísticas y cuándo. * **8.16 Actividades de seguimiento (Monitoring)**  Monitorear accesos indebidos a los datos personales de puntualidad. * **8.33 Información de prueba**  En pruebas del módulo, no usar datos reales de usuarios. |

| **(RF 14 ) Historial de Asistencia con Calendario** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | * Datos El sistema mostrará al usuario un historial de asistencia en formato de calendario, donde podrá consultar por día si asistió, no asistió, llegó tarde o salió antes de tiempo |
| **Entrada** | * ID del usuario. Registros de la máquina (entrada/salida con fecha y hora). Salida Calendario visual con estados diarios: ✅ Asistió. ❌ No asistió. ⏰ Llegó tarde. |
| **Salida** | * Salida anticipada (si aplica). |
| **Acción:** | * Mostrar en calendario los registros históricos. Permitir filtrar por semana, mes o rango de fechas. Generar reportes descargables en PDF o Excel (opcional) |
| **Criterios de aceptación** | El calendario debe mostrar claramente cada día con su estado. El usuario solo puede ver su propio historial. Los instructores/administradores pueden ver el historial de los aprendices asignados.  **5.1** Políticas de seguridad de la información Garantizar que la gestión del historial de asistencia siga políticas establecidas.  **5.2 Funciones y responsabilidades Definir claramente: Usuario → solo ve su historial. Instructor/Admin** → solo los de aprendices a cargo.  **5.12 Clasificación de la información** El historial de asistencia es información sensible de desempeño.  **5.13 Etiquetado de la información Reportes descargables (PDF, Excel) deben marcarse como “Confidencial”.**  5.15 Control de acceso Restringir accesos según roles (usuario, instructor, administrador). 5.17 Información de autenticación Credenciales necesarias para acceder al historial. 5.18 Derechos de acceso Control granular sobre quién consulta y descarga reportes. 5.33 Protección de registros Proteger los datos de asistencia contra modificaciones indebidas. 8.3 Restricción de acceso a la información Cada usuario solo accede a su propio calendario. 8.5 Autenticación segura Para acceder al historial o descargar reportes. 8.12 Prevención de fuga de datos Evitar que los reportes exportados se filtren fuera del entorno autorizado. 8.13 Copia de seguridad de la información Resguardar el historial de asistencia en respaldos seguros. 8.15 Registro (Logging) Registrar accesos a los historiales y descargas de reportes. 8.16 Actividades de seguimiento (Monitoring) Monitorear intentos de acceso indebido a historiales. 8.33 Información de prueba Durante pruebas del módulo, no deben usarse datos reales de usuarios. |

| **(RF 15 ) Generación automática de notificaciones** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | * El sistema generará notificaciones de manera automática cuando ocurran eventos específicos (asistencia, retrasos, faltas, envío de excusas, cambios de horario). |
| **Entrada** | * Datos de asistencia enviados por la máquina, registro de excusas, cambios de horario en el sistema. |
| **Salida** | * Notificación registrada en la BD y visible para el usuario en el sistema. |
| **Acción:** | * El sistema analiza los registros recibidos. Si se cumple una condición (ej: retraso, falta, excusa enviada), crea automáticamente una notificación asociada al usuario. La notificación se almacena en la BD y se muestra en la interfaz. |
| **Criterios de aceptación** | Toda notificación debe quedar registrada con fecha, hora, ID del usuario y estado (leída/no leída). El usuario debe poder visualizar notificaciones pendientes al iniciar sesión. A.5.1 Políticas de seguridad de la información → Se deben definir políticas claras sobre el uso de notificaciones y comunicación de eventos. A.5.23 Seguridad de la información en el uso de servicios en la nube (si se usan notificaciones en nube). A.8.15 Registro de eventos → Toda notificación debe quedar registrada (fecha, hora, usuario, estado). A.8.16 Monitoreo de actividades → El sistema debe garantizar que se registren eventos relevantes como retrasos, faltas o cambios de horario. A.8.20 Registro de actividades del usuario → Cada usuario debe tener trazabilidad de las notificaciones recibidas y consultadas. A.8.27 Seguridad en aplicaciones web → La interfaz donde se muestran las notificaciones debe estar protegida contra accesos indebidos. A.9.1 Gestión de identidad y acceso → Solo el usuario debe ver sus notificaciones; administradores e instructores solo las de sus aprendices. A.9.2 Autenticación del usuario → Verificación de que solo usuarios autorizados reciban las notificaciones. A.12.4 Protección de registros → Asegurar que las notificaciones y eventos no sean alterados o borrados sin autorización. A.12.6 Integridad de la información → Garantizar que las notificaciones reflejen de manera exacta los eventos que ocurrieron. (RF 15.1 ) Visualización de notificaciones en la interfaz Tipo Funcional Descripción El sistema mostrará notificaciones automáticas en una sección dedicada (ejemplo: campanita o panel lateral). Entrada Consulta de notificaciones desde la BD. Salida Listado de notificaciones pendientes. Acción: Mostrar en la interfaz todas las notificaciones del usuario. Permitir marcar como “Leída”. Mantener un historial para consulta futura. Restricciones: No se permiten excusas enviadas el mismo día de la Sausencia. El usuario solo puede enviar una excusa por día. Criterios de aceptación El usuario debe distinguir claramente entre notificaciones nuevas y leídas. Las notificaciones deben mostrarse en orden cronológico. A.5.12 Clasificación de la información → Asegurar que las notificaciones tengan un nivel de protección acorde a su sensibilidad (ej. solo visibles para el usuario). A.5.15 Control de acceso → Definir reglas claras para quién puede visualizar, enviar o gestionar notificaciones. A.8.3 Restricción de acceso a la información → Solo el usuario debe visualizar sus propias notificaciones. A.8.5 Autenticación segura → Validar que solo el usuario autenticado pueda acceder a su bandeja de notificaciones. A.8.15 Registro de eventos → Cada acción con notificaciones (leer, marcar como leída, enviar excusa) debe quedar registrada. A.8.16 Actividades de seguimiento → Permite monitorear la interacción del usuario con las notificaciones. A.8.20 Registro de actividades del usuario → Controlar y evidenciar el historial de notificaciones y cambios de estado. A.8.27 Seguridad de aplicaciones web → La interfaz gráfica (campanita/panel) debe estar protegida contra ataques tipo XSS, CSRF, inyecciones, etc. A.9.1 Gestión de identidad y acceso → Garantizar que cada usuario solo vea sus notificaciones. A.9.2 Derechos de acceso → El sistema debe limitar las acciones (ejemplo: un usuario no puede eliminar notificaciones de otro, un instructor solo ve las de aprendices). A.12.4 Protección de registros → Asegurar que el historial de notificaciones no pueda ser manipulado o borrado sin autorización. (RF 16 ) Notificaciones por correo electrónico (automáticas) Tipo Funcional Descripción El sistema enviará notificaciones automáticas al correo registrado del usuario en caso de eventos importantes (ejemplo: ausencia, cambios de horario, restablecimiento de contraseña). Entrada Generación de eventos en el sistema. Salida Correo enviado automáticamente al email registrado del usuario. Acción: El sistema detecta un evento crítico. Genera un correo con un mensaje estándar. Envía el correo Restricciones: No se permiten excusas enviadas el mismo día de la ausencia. El usuario solo puede enviar una excusa por día. Criterios de aceptación El correo debe enviarse en menos de 1 minuto tras generarse el evento. El sistema no debe permitir correos vacíos ni direcciones no registradas. A.5.1 Políticas de seguridad de la información → Definir reglas sobre el envío de correos automáticos (uso permitido, restricciones, protección de datos). A.5.12 Clasificación de la información → El contenido del correo debe ajustarse a su nivel de sensibilidad (ejemplo: no incluir datos confidenciales en texto plano). A.5.15 Control de acceso → Solo el sistema autorizado debe poder generar y enviar correos, evitando abuso o spam. A.8.5 Autenticación segura → Garantizar que el envío de correos esté autenticado (por ejemplo, uso de SMTP seguro con credenciales protegidas). A.8.7 Protección contra malware → Evitar que los correos enviados contengan enlaces o adjuntos maliciosos. A.8.12 Prevención de fuga de datos (DLP) → Evitar que la funcionalidad de notificaciones por correo exponga información sensible a destinatarios no autorizados. A.8.15 Registro de eventos → Registrar intentos de envío, correos entregados y fallidos. A.8.16 Actividades de seguimiento → Monitorear el uso del sistema de notificaciones para detectar anomalías (ejemplo: envío masivo no autorizado). A.9.2 Derechos de acceso → Definir qué módulos del sistema pueden generar notificaciones por correo (ejemplo: asistencias, seguridad de cuentas). A.9.4 Restricción de acceso a información → Asegurar que el correo solo se envíe al dueño de la cuenta registrada. A.12.4 Protección de registros → Mantener logs de correos enviados con integridad y trazabilidad (fecha, hora, usuario, tipo de evento). MIra ahora sigue la parte de las notificaciones y Ver un historial de asistencia con el canlendario ( creo que ya esta lo de asistencia ) |

| **(RF 15.1 ) Visualización de notificaciones en la interfaz** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | * El sistema mostrará notificaciones automáticas en una sección dedicada (ejemplo: campanita o panel lateral). |
| **Entrada** | * Consulta de notificaciones desde la BD |
| **Salida** | * Listado de notificaciones pendientes. |
| **Acción:** | * Mostrar en la interfaz todas las notificaciones del usuario. Permitir marcar como “Leída”. Mantener un historial para consulta futura. Restricciones: No se permiten excusas enviadas el mismo día de la Sausencia. El usuario solo puede enviar una excusa por día.muestra en la interfaz. |
| **Criterios de aceptación** | Criterios de aceptación El usuario debe distinguir claramente entre notificaciones nuevas y leídas. Las notificaciones deben mostrarse en orden cronológico. A.5.12 Clasificación de la información → Asegurar que las notificaciones tengan un nivel de protección acorde a su sensibilidad (ej. solo visibles para el usuario). A.5.15 Control de acceso → Definir reglas claras para quién puede visualizar, enviar o gestionar notificaciones. A.8.3 Restricción de acceso a la información → Solo el usuario debe visualizar sus propias notificaciones. A.8.5 Autenticación segura → Validar que solo el usuario autenticado pueda acceder a su bandeja de notificaciones. A.8.15 Registro de eventos → Cada acción con notificaciones (leer, marcar como leída, enviar excusa) debe quedar registrada. A.8.16 Actividades de seguimiento → Permite monitorear la interacción del usuario con las notificaciones. A.8.20 Registro de actividades del usuario → Controlar y evidenciar el historial de notificaciones y cambios de estado. A.8.27 Seguridad de aplicaciones web → La interfaz gráfica (campanita/panel) debe estar protegida contra ataques tipo XSS, CSRF, inyecciones, etc. A.9.1 Gestión de identidad y acceso → Garantizar que cada usuario solo vea sus notificaciones. A.9.2 Derechos de acceso → El sistema debe limitar las acciones (ejemplo: un usuario no puede eliminar notificaciones de otro, un instructor solo ve las de aprendices). A.12.4 Protección de registros → Asegurar que el historial de notificaciones no pueda ser manipulado o borrado sin autorización. |

| **(RF 16 ) Notificaciones por correo electrónico (automáticas)** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | * El sistema enviará notificaciones automáticas al correo registrado del usuario en caso de eventos importantes (ejemplo: ausencia, cambios de horario, restablecimiento de contraseña). |
| **Entrada** | * Generación de eventos en el sistema |
| **Salida** | * Correo enviado automáticamente al email registrado del usuario |
| **Acción:** | * El sistema detecta un evento crítico. Genera un correo con un mensaje estándar. Envía el correo Restricciones: No se permiten excusas enviadas el mismo día de la ausencia. El usuario solo puede enviar una excusa por día. |
| **Criterios de aceptación** | El correo debe enviarse en menos de 1 minuto tras generarse el evento. El sistema no debe permitir correos vacíos ni direcciones no registradas. A.5.1 Políticas de seguridad de la información → Definir reglas sobre el envío de correos automáticos (uso permitido, restricciones, protección de datos). A.5.12 Clasificación de la información → El contenido del correo debe ajustarse a su nivel de sensibilidad (ejemplo: no incluir datos confidenciales en texto plano). A.5.15 Control de acceso → Solo el sistema autorizado debe poder generar y enviar correos, evitando abuso o spam. A.8.5 Autenticación segura → Garantizar que el envío de correos esté autenticado (por ejemplo, uso de SMTP seguro con credenciales protegidas). A.8.7 Protección contra malware → Evitar que los correos enviados contengan enlaces o adjuntos maliciosos. A.8.12 Prevención de fuga de datos (DLP) → Evitar que la funcionalidad de notificaciones por correo exponga información sensible a destinatarios no autorizados. A.8.15 Registro de eventos → Registrar intentos de envío, correos entregados y fallidos. A.8.16 Actividades de seguimiento → Monitorear el uso del sistema de notificaciones para detectar anomalías (ejemplo: envío masivo no autorizado). A.9.2 Derechos de acceso → Definir qué módulos del sistema pueden generar notificaciones por correo (ejemplo: asistencias, seguridad de cuentas). A.9.4 Restricción de acceso a información → Asegurar que el correo solo se envíe al dueño de la cuenta registrada. A.12.4 Protección de registros → Mantener logs de correos enviados con integridad y trazabilidad (fecha, hora, usuario, tipo de evento). MIra ahora sigue la parte de las notificaciones y Ver un historial de asistencia con el canlendario ( creo que ya esta lo de asistencia ) |

| **(RF 17 ) Visualización del perfil personal** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | * **Descripción**: El sistema permitirá al usuario visualizar únicamente su información personal en un espacio de perfil. |
| **Entrada** | **Datos visibles**:   * Nombre y apellido. * Foto registrada (imagen de perfil vinculada al registro inicial). * Ficha a la que pertenece. * Jornada (horarios asignados). * Rol (aprendiz, instructor, administrador). * Tipo de registro utilizado (clave, rostro, huella). |
| **Salida** | mostrar los datos al usuario |
| **Acción:** | * el usuario ingresa a perfil personal * puede ver mirara y modificar sus datos * tiene la configuración |
| **Criterios de aceptación** | * solo el usuario puede ver sus propios datos * solo lo puede modificar el usuario   **A.5.1 Políticas de seguridad de la información** → Define cómo se maneja la información personal en perfiles de usuario.  **A.5.12 Clasificación de la información** → Los datos personales deben tratarse como sensibles y protegerse acorde a su nivel de confidencialidad.  **A.5.13 Etiquetado de la información** → Identificar y marcar los datos personales como "Privados" o "Confidenciales". **A.5.36 Cumplimiento de políticas y regulaciones** → Garantizar que el manejo de perfiles cumpla con leyes de protección de datos (ej. Habeas Data, GDPR).  **A.8.3 Restricción de acceso a la información** → Solo el usuario dueño del perfil debe poder ver y editar su información.  **A.8.5 Autenticación segura** → Asegurar que el acceso al perfil se realice solo tras autenticación válida (usuario/clave, biometría, etc.).  **A.8.12 Prevención de fuga de datos** → Evitar que la información personal del perfil se filtre hacia otros usuarios o aplicaciones no autorizadas.  **A.8.15 Registro de eventos** → Registrar accesos y modificaciones al perfil para trazabilidad.  **A.8.16 Actividades de seguimiento** → Monitorear accesos inusuales a perfiles personales.  **A.9.2 Derechos de acceso** → Establecer que solo el usuario autenticado tiene permisos de visualización y modificación de su perfil.  **A.9.4 Restricción de acceso a la información** → Asegurar que un usuario no pueda visualizar el perfil de otro.  **A.12.4 Protección de registros** → Los logs de accesos/modificaciones al perfil deben mantenerse íntegros y disponibles para auditoría. |

| **(RF 18 ) Edición de nombre y apellido** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | * El usuario podrá modificar **únicamente su nombre y apellido**. |
| **Entrada** | * Nuevos valores de nombre y/o apellido. |
| **Salida** | * Confirmación de cambios exitosos. |
| **Acción:** | * puede modificar sus datos de forma rapida y segura |
| **Criterios de aceptación** | * No se permite modificar ficha, jornada, rol ni tipo de registro. * El cambio se guarda en la base de datos y se refleja en próximos accesos.   **A.5.1 Políticas de seguridad de la información** → Asegurar que los cambios en datos personales se ajusten a las políticas internas.  **A.5.12 Clasificación de la información** → Los datos de identificación personal deben manejarse como información sensible.  **A.5.36 Cumplimiento de políticas y regulaciones** → El tratamiento de datos personales debe cumplir con normativas de protección de datos.  **A.8.3 Restricción de acceso a la información** → Solo el usuario autenticado debe poder modificar su propio nombre y apellido.  **A.8.5 Autenticación segura** → Validar identidad antes de permitir cambios (ej. autenticación con contraseña/biometría). **A.8.15 Registro de eventos** → Registrar toda modificación de datos (qué se cambió, cuándo, y por quién).  **A.8.16 Actividades de seguimiento** → Monitorear cambios para detectar accesos o modificaciones indebidas.  **A.9.2 Derechos de acceso** → Definir claramente que solo el usuario dueño de la cuenta puede modificar sus datos personales.  **A.9.4 Restricción de acceso a información** → Evitar que otro usuario (aprendiz, instructor o administrador) pueda cambiar información personal de un tercero.  **A.12.4 Protección de registros** → Mantener integridad de los logs de edición para auditorías futuras. |

| **(RF 19 ) Eliminación de perfil personal** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | * El usuario tendrá la opción de **borrar su cuenta** en caso de no pertenecer más al sistema. |
| **Entrada** | * Eliminar cuenta |
| **Salida** | * dar Acceso al usuario para que elimine su cuenta |
| **Acción:** | -El usuario selecciona “Eliminar cuenta”. - El sistema solicitará confirmación para evitar borrados accidentales. -Los datos quedan desactivados (no se pierden registros históricos, sólo se deshabilita el usuario). |
| **Criterios de aceptación** | * solo el miami usuario puede eliminar su cuenta   **A.5.1 Políticas de seguridad de la información** → El proceso de baja de cuentas debe estar regulado por políticas internas.  **A.5.12 Clasificación de la información** → Los datos de perfil y registros asociados son sensibles y deben gestionarse con cuidado incluso tras la desactivación.  **A.5.36 Cumplimiento normativo** → Garantizar que la eliminación respete leyes de protección de datos  **A.8.3 Restricción de acceso a la información** → Solo el usuario autenticado debe poder eliminar su propio perfil.  **A.8.5 Autenticación segura** → Antes de la eliminación, validar la identidad del usuario (ej. reingreso de credenciales o autenticación multifactor).  **A.8.10 Eliminación de información** → Asegurar que los datos personales eliminados o desactivados se gestionen correctamente para evitar recuperación no autorizada.  **A.8.15 Registro de eventos** → Toda eliminación de perfil debe quedar registrada (quién, cuándo y cómo se realizó).  **A.8.16 Actividades de seguimiento** → Monitoreo de estas acciones críticas para prevenir usos indebidos.  **A.9.2 Derechos de acceso** → Definir que solo el propietario del perfil puede solicitar su eliminación.  **A.9.4 Restricción de acceso a información** → Evitar que administradores u otros usuarios eliminen perfiles sin autorización formal del titular.  **A.12.4 Protección de registros** → Aunque el perfil se elimine, los registros históricos (asistencia, notificaciones, auditorías) deben preservarse íntegros para fines legales y de trazabilidad. |

| **(RF 20 ) Configuración** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | * El sistema contará con un espacio de configuración accesible desde el perfil del usuario. |
| **Entrada** | * **Cerrar sesión** → el usuario sale de la sesión activa. * **Cambiar de cuenta** → permite volver a la pantalla de inicio e ingresar con otro usuario. |
| **Criterios de aceptación** | **A.5.1 Políticas de seguridad de la información →** Las políticas deben definir cómo manejar sesiones activas y cierres de sesión seguros.  **A.5.36 Cumplimiento de políticas, reglas y estándares →** Asegurar que el manejo de sesiones cumpla con las regulaciones y estándares internos.  **A.8.3 Restricción de acceso a la información** → Al cerrar sesión, garantizar que nadie más pueda acceder a la información del usuario.  **A.8.5 Autenticación segura** → Obligar a una nueva autenticación cuando el usuario cambie de cuenta o vuelva a iniciar sesión.  **A.8.15 Registro de eventos** → Registrar la apertura, cambio y cierre de sesiones para auditoría.  **A.8.16 Actividades de seguimiento** → Monitorear intentos de inicio/cierre de sesión sospechosos o cambios de usuario frecuentes.   * **A.9.2 Derechos de acceso** → Verificar que cada usuario solo pueda acceder a su propia cuenta tras el cambio de sesión. * **A.9.4 Restricción de acceso a información** → Al cambiar de cuenta, evitar que la sesión anterior deje datos en memoria caché o accesibles. |

| **(RF 21 ) Estadísticas de Usuarios** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | * El sistema permitirá la visualización de estadísticas de asistencia, puntualidad y retrasos. * El **Instructor** podrá ver estadísticas únicamente de sus aprendices. * El **Administrador** tendrá acceso a estadísticas globales. * El **Bienestar** podrá ver estadísticas de los aprendices. * El **Coordinador** podrá ver estadísticas de los instructores. * La **Secretaría** podrá ver estadísticas tanto de instructores como de fichas de formación. |
| **Entrada** | * Selección de rango de fechas. * Selección de ficha, aprendiz o instructor (según el rol). |
| **Salida** | * Gráficas de estadísticas personalizadas (asistencias, inasistencias, retrasos). |
| **Acción:** | -Consultar datos desde la BD.  - Filtrar según permisos del rol.  - Mostrar visualizaciones dinámicas. |
| **Criterios de aceptación** | * Cada usuario solo podrá ver estadísticas de acuerdo a su rol. * El sistema debe permitir exportar estadísticas en formato Excel , PDF (para roles con permisos de gestión).   **A.5.17** Gestión de identidades y acceso de usuarios → asegurar que cada rol solo acceda a las estadísticas que le corresponden.  **A.8.23** Protección de datos personales → proteger datos de aprendices, instructores y fichas.  **A.8.12** Registro de actividades → mantener trazabilidad de consultas y exportaciones.  **A.5.7** Segregación de funciones → diferenciar permisos de acceso según roles (Instructor, Coordinador, Bienestar, etc.).  **A.5.32** Trazabilidad de acciones de usuarios → garantizar auditoría en generación de estadísticas y exportación de informes.  **A.8.24** Restricciones en la transferencia de información → controlar exportación de reportes en Excel/PDF. |

| **(RF 22 ) Gestión de Horarios/Turnos** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | El sistema permitirá configurar y modificar horarios/turnos de cada ficha.   * **Administrador**, **Instructor** y **Secretaría** podrán realizar esta acción. |
| **Entrada** | -Día de la semana.  - Hora de inicio y fin. - Selección de ficha. |
| **Salida** | * Calendario semanal con horarios configurados. |
| **Acción:** | -Crear horarios nuevos.  - Modificar horarios existentes.  - Eliminar horarios que ya no se apliquen. |
| **Criterios de aceptación** | * No debe haber solapamientos de horarios en una misma ficha. * Solo los roles con permisos podrán crear, modificar o eliminar.   **A.5.17 – Gestión de identidades y acceso de usuarios** → garantizar que solo Administrador, Instructor y Secretaría tengan permisos de crear, modificar o eliminar horarios.  **A.5.18 – Registro y gestión de privilegios de usuario** → asegurar que los privilegios de edición estén restringidos a los roles definidos.  **A.5.7 – Segregación de funciones** → separar funciones de consulta (todos los usuarios) de funciones de gestión (solo roles autorizados).  **A.8.12 – Registro de actividades** → registrar en logs las creaciones, modificaciones o eliminaciones de horarios.  **A.5.32 – Trazabilidad de acciones de usuarios** → permitir auditoría de quién creó, modificó o eliminó un horario.  **A.8.23 – Protección de datos personales** → proteger información sensible asociada a las fichas y horarios de los aprendices.  **A.8.31 – Validación de datos de entrada** → evitar solapamientos de horarios mediante controles de validación antes de guardar cambios. |

| **(RF 23 ) Asociación de Instructores a Fichas** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | * El sistema permitirá asignar instructores a fichas de formación. * Esta acción solo podrá ser realizada por **Administrador**, **Instructor** y **Secretaría**. |
| **Entrada** | * Selección de ficha. * Selección de instructor. * Definición de días/horarios donde el instructor acompaña la ficha. |
| **Salida** | * Relación ficha-instructor registrada en la BD. |
| **Acción:** | -Consultar fichas disponibles  - Asociar al instructor a ficha y horario.  - Guardar registro en el sistema. |
| **Criterios de aceptación** | * Una ficha debe tener al menos un instructor asignado. * No debe asignarse un instructor en dos fichas a la misma hora.   **A.5.17 – Gestión de identidades y acceso de usuarios** → solo Administrador, Instructor y Secretaría deben poder realizar la asociación.  **A.5.18 – Registro y gestión de privilegios de usuario** → asegurar que solo roles con privilegios puedan modificar las asociaciones ficha-instructor.  **A.5.7 – Segregación de funciones** → separar funciones de consulta (aprendices e instructores pueden visualizar) de funciones de gestión (solo roles autorizados).  **A.8.12 – Registro de actividades** → registrar en logs quién creó, modificó o eliminó asociaciones.  **A.5.32 – Trazabilidad de acciones de usuarios** → permitir auditoría completa de las asignaciones (qué usuario hizo el cambio y cuándo).  **A.8.31 – Validación de datos de entrada** → evitar asignar un mismo instructor a dos fichas en horarios solapados.  **A.8.23 – Protección de datos personales** → proteger la información de instructores y aprendices relacionada a la ficha. |

| **(RF 24 ) Configuración Personal del Usuario** | |
| --- | --- |
| Tipo | Funcional |
| **Descripción** | Cada usuario tendrá un módulo de configuración donde podrá:   * Cerrar sesión. -Cambiar de cuenta. * Modificar su nombre y apellidos. * Ver sus datos personales (rol, ficha, jornada, foto, tipo de registro). * Eliminar su cuenta si ya no hace parte del sistema. |
| **Entrada** | * Selección de la opción de configuración. * Datos a modificar (nombre, apellido). |
| **Salida** | * Confirmación de cambios aplicados. * Datos actualizados en la BD. |
| Acción: | Mostrar información personal del usuario.  Permitir modificaciones limitadas (solo nombre/apellido).  Ejecutar cierre o cambio de sesión. |
| **Criterios de aceptación** | * Cada usuario solo puede modificar sus propios datos. * El cierre de sesión debe terminar inmediatamente la sesión activa. * El cambio de cuenta se debe redirigir a la pantalla de inicio de sesión.   **A.5.17 – Gestión de identidades y acceso de usuarios** → garantizar que cada usuario solo acceda a su propia configuración.  **A.5.18 – Registro y gestión de privilegios de usuario** → restringir la edición solo a campos permitidos (nombre/apellido).  **A.8.3 – Restricción de acceso a la información** → evitar que un usuario acceda o modifique información de otro perfil.  **A.8.5 – Autenticación segura** → validar que el cierre de sesión y cambio de cuenta se realice de manera segura.  **A.8.10 – Eliminación de información** → aplicar en la opción de eliminar cuenta (desactivar usuario sin borrar historial).  **A.8.12 – Registro de actividades** → registrar en logs quién modificó datos, eliminó su cuenta o cerró sesión.  **A.5.32 – Trazabilidad de acciones de usuarios** → garantizar auditoría de cambios en configuraciones de perfil.  **A.8.23 – Protección de datos personales** → proteger datos sensibles del usuario (foto, rol, ficha, jornada, tipo de registro).  **A.8.31 – Validación de datos de entrada** → verificar que solo se permitan cambios válidos en nombre y apellido. |

**3.3 REQUERIMIENTOS NO FUNCIONALES**

| **RF1** Requerimientos no funcionales | |
| --- | --- |
| Usabilidad | El sistema debe ser intuitivo y fácil de usar. |
| Seguridad | No se compartirá información de los perfiles de usuarios, los datos deben tener una vigencia. |
| Capacidad | El usuario podrá operar de manera rápida, aunque tenga a varios usuarios conectados. |
| Tiempo de respuesta | Las respuestas no deben demorar más de 5 segundos. |
| Almacenamiento | En caso de no tener acceso a internet, el sistema podrá almacenar información local. |
| Compatibilidad | El sistema será compatible con los diferentes buscadores. |

| **RN 2** | Validación de correo electrónico único |
| --- | --- |
| **Tipo** | Requerimiento no funcional |
| **Descripción** | El sistema no permite que se registre dos veces un mismo correo electrónico para los usuarios ni contraseña. |
| **Entrada** | * Intento registrarme con un correo electrónico ya existente. |
| **Salida** | * Mensaje de error indicando que el correo ya está en uso |
| **Acción** | * Validar en la base de datos si el correo ya existe antes de registrar un nuevo usuario. |
| **Criterios de aceptación** | * El sistema bloquea el registro duplicado. * El usuario recibe un mensaje claro: *“Este correo ya está registrado”*. |

| **RN 3** | Uso único de cuenta por usuario |
| --- | --- |
| Tipo | Requerimiento no funcional |
| Descripción | El sistema no permitirá que un mismo usuario tenga más de una cuenta activa. Cada persona solo podrá registrarse con una cuenta única. |
| Entrada | * Intento registrar un nuevo perfil con los mismos datos de identificación. |
| Salida | * Mensaje de error indicando que ya existe un perfil para ese usuario. |
| Acción | * Validar coincidencia de documento de identidad antes de crear la cuenta. |
| Criterios de aceptación | * Cada documento de identidad solo puede asociarse a una cuenta. * El sistema muestra un mensaje: *“Ya existe una cuenta registrada con este documento”*. |

| **RN 4** | Validación de campos de datos |
| --- | --- |
| **Tipo** | Requerimiento no funcional |
| **Descripción** | El sistema validará que los campos de entrada correspondan al tipo de dato correcto. |
| **Entrada** | * Documento y teléfono → solo números. * Nombre, apellido, género, rol → solo letras. |
| **Salida** | * Mensaje de error en caso de formato inválido. |
| **Acción** | * Aplicar validaciones en formularios de registro. |
| **Criterios de aceptación** | * El sistema no permite registrar letras en campos numéricos ni números en campos de texto. * Se muestra un mensaje: *“Formato de datos inválido”*. |

**\_**

| **RN 6** | No duplicar datos personales |
| --- | --- |
| **Tipo** | Requerimiento no funcional |
| **Descripción** | El sistema no permite ingresar mismos datos a otro usuario que tenga correo y contraseña diferente ejemplo (María José no puede tener los mismos datos de Natalia así las dos tengan correo y contraseñas diferentes) |
| **Entrada** | * Intento registrar un usuario con los mismos datos de identidad que otro ya registrado. |
| **Salida** | * Mensaje de error indicando duplicidad de datos. |
| **Acción** | * Comparar los datos personales con los registros existentes en la base de datos. |
| **Criterios de aceptación** | * No existen dos usuarios con datos idénticos.   Mensaje mostrado: *“Los datos ingresados ya corresponden a otro usuario”*. |

| **RN 7** | **Registro de Errores en el Sistema** |
| --- | --- |
| **Tipo** | Requerimiento no funcional |
| **Descripción** | El sistema deberá registrar automáticamente en la tabla *Log Errores* cada error que ocurra durante la autenticación o el uso de funcionalidades críticas, incluyendo la fecha del evento, el usuario involucrado (si aplica), el tipo de error y una descripción detallada del mismo. |
| **Entrada** | * Acciones que generen un error en el sistema (ejemplo: intento fallido de inicio de sesión, usuario no encontrado, error de validación, etc.) |
| **Salida** | Registro en la base de datos con los siguientes datos:   * Fecha y hora del error. * Identificador del usuario (si estaba autenticado). * Tipo de error. * Descripción detallada. |
| **Acción** | * El sistema guardará automáticamente la información en la tabla Log Error cada vez que se detecte un error. |
| **Criterios de aceptación** | * Cada error debe quedar almacenado con sus respectivos detalles. * Si no hay usuario activo en el momento del error, el campo Id Credenciales deberá quedar como null . * Los registros deben permitir rastrear el historial de fallos para fines de auditoría y diagnóstico. |

**\_\_**

| **RN 8** | **Registro de Auditoría de Acciones de Usuario** |
| --- | --- |
| **Tipo** | Requerimiento no funcional |
| **Descripción** | El sistema deberá almacenar en la tabla auditoria todas las acciones realizadas por los usuarios dentro de la aplicación (ejemplo: inicio/cierre de sesión, cambios en la configuración, creación o modificación de datos), incluyendo la fecha, descripción de la acción y la dirección IP de origen. |
| **Entrada** | * Cualquier acción ejecutada por un usuario autenticado (ejemplo: login, logout, actualización de perfil, consulta de información, intentos fallidos). |
| **Salida** | Registro en la base de datos con los siguientes datos:   * Identificador del usuario que realizó la acción . * Acción realizada (ejemplo: “Inicio de sesión”, “Actualización de perfil”). * Fecha y hora de la acción. * Descripción detallada de la acción. * Dirección IP desde la cual se ejecutó la acción. |
| **Acción** | * Cada vez que un usuario realice una acción relevante en el sistema, se deberá insertar un registro en la tabla auditoria |
| **Criterios de aceptación** | * Toda acción relevante debe quedar almacenada con su respectiva información. * Si un error ocurre durante la acción, también debe reflejarse la auditoría con la descripción correspondiente. * Los registros deben ser consultables para fines de auditoría, seguridad y diagnóstico de fallos. |

| **RN 9 //gestión de Permisos por Rol** | La seguridad de control del acceso según su rol en específico |
| --- | --- |
| **Tipo** | Requerimiento no funcional |
| **Descripcin** | El sistema debe implementar un mecanismo de **gestión de permisos basada en roles (RBAC – Role Based Access Control)**. los controles que tiene según su rol.  Cada usuario tendrá permisos diferenciados según su rol, los cuales definirán:   * Qué menús y botones puede ver. * Qué acciones puede ejecutar.   - Qué información puede consultar o modificar. |
| **Acción** | * El sistema debe tener una **matriz de permisos por rol** (ej. tabla en base de datos). * Al iniciar sesión, el rol del usuario se valida contra esa matriz. * La interfaz se renderiza dinámicamente, mostrando solo lo autorizado. * Cualquier intento de acceder a opciones no autorizadas debe ser bloqueado y registrado en un log de seguridad. |

| **RN 10 // Claridad en la información** | Claridad en la información |
| --- | --- |
| **Tipo** | No funcional – Seguridad |
| **Descripción** | - Toda la información legal (avisos de privacidad, derechos, normativa) debe mostrarse en un lenguaje claro y comprensible para cualquier usuario. |
| **Entrada** | * texto legal mostrado en pantalla. |
| **Salida** | * Usuario entiende lo que acepta. |
| **Acción** | * Redactar textos sin tecnicismos ni ambigüedades.. |
| **Criterios de aceptación** | * El usuario puede leer y comprender la información antes de aceptar. |

| **RN 11 // Validación de edad** | Validación de edad |
| --- | --- |
| **Tipo** | No funcional – Legal |
| **Descripción** | * El sistema debe validar que los usuarios menores de edad no continúen sin consentimiento expreso de un adulto responsable. |
| **Entrada** | * Fecha de nacimiento ingresada. |
| **Salida** | * Usuario entiende lo que acepta. |
| **Acción** | * Comparar edad con la mayoría de edad definida en la ley. |
| **Criterios de aceptación** | * Ningún menor puede usar el sistema sin consentimiento registrado. |

| **RN 12 // Evidencia de consentimiento** | **Evidencia de consentimiento** |
| --- | --- |
| **Tipo** | No funcional – Legal / Seguridad básica |
| **Descripción** | * El sistema debe registrar la aceptación del usuario (o del tutor en caso de menores) como evidencia legal. |
| **Entrada** | * Aceptación del aviso de privacidad. |
| **Salida** | * Registro de consentimiento en base de datos. |
| **Acción** | * Guardar fecha, hora y tipo de aceptación. |
| **Criterios de aceptación** | * El sistema puede mostrar historial de aceptaciones si se solicita. |

| **RN 13 // Acceso limitado a la información legal** | **Acceso limitado a la información legal** |
| --- | --- |
| **Tipo** | No funcional – Seguridad básica |
| **Descripción** | * Solo el usuario dueño de la cuenta puede ver y aceptar la información legal, no terceros. |
| **Entrada** | * Usuario autenticado. |
| **Salida** | * Acceso al aviso legal. |
| **Acción** | * Mostrar aviso únicamente al usuario que inicia sesión. |
| **Criterios de aceptación** | * Nadie puede aceptar términos en nombre de otro usuario. |

| **RN 14.1 // – Cifrado de credenciales** | **Registro de modificaciones (Iniciar Sesión)** |
| --- | --- |
| **Tipo** | No funcional – Legal / Seguridad |
| **Descripción** | * Las contraseñas deben almacenarse siempre en la base de datos mediante hashing seguro * Ninguna contraseña podrá estar en texto plano. |

| **RN 14.2 // Bloqueo por intentos fallidos** | **Acceso limitado a la información legal (Iniciar Sesión)** |
| --- | --- |
| **Tipo** | No funcional – Seguridad Disponibilidad |
| **Descripción** | * Después de 3 intentos fallidos, la cuenta debe bloquearse temporalmente para evitar ataques de fuerza bruta. |

| **RN 14.3 // Sesiones seguras** | **Sesiones seguras (Iniciar Sesión)** |
| --- | --- |
| **Tipo** | No funcional – Seguridad |
| **Descripción** | * Toda sesión debe manejarse con tokens de sesión cifrados. * Expiran tras un tiempo definido de inactividad (ejemplo: 15 minutos). |

| **RN 14.4 // Confidencialidad del proceso de login** | **Confidencialidad del proceso de login (Iniciar Sesión)** |
| --- | --- |
| **Tipo** | Legal / Seguridad |
| **Descripción** | - El sistema debe mostrar un aviso al usuario sobre la importancia de no compartir sus credenciales. |

| **RN 14.5 //Auditoría de accesos** | **Auditoría de accesos (Iniciar Sesión)** |
| --- | --- |
| **Tipo** | Trazabilidad |
| **Descripción** | * Cada inicio de sesión exitoso o fallido debe registrarse en logs para auditoría. |

| **RN 15.1 // Tokens temporales y de un solo uso** | **Auditoría de accesos (Restablecimiento de Contraseña)** |
| --- | --- |
| **Tipo** | Seguridad |
| **Descripción** | -Los enlaces de recuperación deben incluir tokens válidos máximo 10–15 minutos y que solo puedan usarse una vez. |

| **RN 15.2 // Canales seguros** | **Seguridad / Legal (Restablecimiento de Contraseña)** |
| --- | --- |
| **Tipo** | Seguridad |
| **Descripción** | -El enlace de restablecimiento debe enviarse solo a correos previamente verificados, usando HTTPS obligatorio. |

| **RN 15.3 // Cumplimiento de reglas de contraseña** | **Cumplimiento de reglas de contraseña (Restablecimiento de Contraseña)** |
| --- | --- |
| **Tipo** | Seguridad |
| **Descripción** | * La nueva contraseña debe tener entre 8 y 15 caracteres, incluir mayúsculas, números y símbolos. |

| **RN 15.4 // Bloqueo de intentos de recuperación fallidos** | **Bloqueo de intentos de recuperación fallidos (Restablecimiento de Contraseña)** |
| --- | --- |
| **Tipo** | Seguridad |
| **Descripción** | * Tras varios intentos incorrectos de token, el sistema debe bloquear temporalmente el proceso. |

| **RN 16.1 // Control de acceso basado en role** | **(Definición de Rol al Iniciar Sesión)** |
| --- | --- |
| **Tipo** | Seguridad / Control |
| **Descripción** | - El sistema debe implementar control de acceso por rol, evitando que un usuario ejecute acciones fuera de sus permisos. |

| **RN 16.2 // Interfaz dinámica y clara** | **Interfaz dinámica y clara** **(Definición de Rol al Iniciar Sesión)** |
| --- | --- |
| **Tipo** | Usabilidad REQUERIMIENTO NO FUNCIONAL |
| **Descripción** | * La interfaz debe adaptarse automáticamente al rol, mostrando solo las funciones autorizadas. |

| **RN 16..3 // No manipulación del rol** | **Interfaz dinámica y clara** **(Definición de Rol al Iniciar Sesión)** |
| --- | --- |
| **Tipo** | seguridad REQUERIMIENTO NO FUNCIONAL |
| **Descripción** | * El rol debe estar ligado al perfil en la base de datos y no puede ser cambiado por el usuario desde la interfaz. |

| **RN 16.4 // Registro de rol en la sesión** | **Interfaz dinámica y clara** **(Definición de Rol al Iniciar Sesión)** |
| --- | --- |
| **Tipo** | Auditoría REQUERIMIENTO NO FUNCIONAL |
| **Descripción** | * El sistema debe guardar en logs el rol con el que inició sesión el usuario, para trazabilidad. |

| **RN 17 // Recepción Automática de Datos por WiFi** | Recepción Automática de Datos por WiFi // No funciona |
| --- | --- |
| **tipo** | No funcional – Seguridad |
| **Rendimiento** | * El sistema debe procesar y almacenar los datos recibidos en un máximo de 2 segundos desde su llegada. * La recepción debe soportar al menos 15 registros por minuto sin pérdida de información. |
| **Confiabilidad** | * El sistema debe garantizar una **tasa de pérdida de datos menor al 0.1%**. * En caso de pérdida de conexión WiFi, el sistema debe reintentar la recepción automáticamente hasta restablecer el enlace. |
| **Seguridad** | * La transmisión de datos debe realizarse bajo **protocolos seguros (HTTPS** * **Todo paquete recibido debe validarse contra ataques de inyección de datos** |
| Disponibilidad | * El servicio de recepción debe estar activo 24/7, escuchando continuamente los paquetes enviados por la máquina. * Se debe implementar un log de errores para registrar fallos de conexión o recepción corrupta. |

| **RN 18 // Asociación de Registros con Roles** | Asociación de Registros con Roles |
| --- | --- |
| **tipo** | No funcional – Seguridad |
| **Rendimiento** | * Cada registro debe vincularse a un rol válido (Aprendiz, Instructor, Administrador, Bienestar, Coordinador, Secretaría). * No debe existir en la base de datos un registro sin rol definido. |
| **Consistencia** | * La asignación de roles debe ser **transaccional**: si falla la asociación, el registro no se debe guardar. * El sistema debe garantizar que los roles definidos en RF 8 se mantengan sincronizados con los registros guardados. |
| **Seguridad y Confidencialidad** | * Solo usuarios autorizados podrán consultar registros asociados a un rol específico. * La base de datos debe cifrar la relación entre usuario y rol para evitar accesos indebidos. |
| Auditoría y Trazabilidad | * Cada registro debe guardar **fecha, hora, ID del usuario y rol asignado**. * Se debe mantener un historial de cambios en caso de que un rol sea modificado. |
| Escalabilidad | * El sistema debe permitir crecer en número de roles (ejemplo: si mañana se agrega “Supervisor”), sin modificar la lógica principal de almacenamiento. |

| **RN 19 // Gestión de Fichas Técnicas** | Descripción / Integridad de Datos |
| --- | --- |
| **tipo** | No funcional – Seguridad |
| **Rendimiento** | * La búsqueda y visualización de fichas debe responder en menos de **2 segundos**. * El sistema debe soportar hasta **10.000 fichas registradas** sin pérdida de rendimiento. |
| **Usabilidad** | * La interfaz debe permitir **filtros y ordenamiento** por ID, cantidad de aprendices. * La vista de fichas debe ser **clara y organizada**, con paginación cuando existan más de 24 fichas. * Se debe mostrar **mensaje de confirmación** antes de eliminar una ficha. |
| **Seguridad** | * Solo los usuarios con rol **Administrador** podrá gestionar fichas. * Los intentos fallidos de gestión deben ser **registrados en auditoría**. * La comunicación con la base de datos debe realizarse bajo protocolo **HTTPS/TLS**. |
| Integridad de datos | * No se permite la **duplicidad de ID de fichas**. * Una ficha con horarios o usuarios asociados **no puede ser eliminada** sin gestionar previamente esas dependencias. |

| **RN 20 // Gestión de Fichas Técnicas** | Descripción / Integridad de Datos |
| --- | --- |
| **tipo** | No funcional – Seguridad |
| **Rendimiento** | * La búsqueda y visualización de fichas debe responder en menos de **2 segundos**. * El sistema debe soportar hasta **10.000 fichas registradas** sin pérdida de rendimiento. |
| **Usabilidad** | * La interfaz debe permitir **filtros y ordenamiento** por ID, cantidad de aprendices. * La vista de fichas debe ser **clara y organizada**, con paginación cuando existan más de 24 fichas. * Se debe mostrar **mensaje de confirmación** antes de eliminar una ficha. |
| **Seguridad** | * Solo los usuarios con rol **Administrador** podrá gestionar fichas. * Los intentos fallidos de gestión deben ser **registrados en auditoría**. * La comunicación con la base de datos debe realizarse bajo protocolo **HTTPS/TLS**. |
| Integridad de datos | * No se permite la **duplicidad de ID de fichas**. * Una ficha con horarios o usuarios asociados **no puede ser eliminada** sin gestionar previamente esas dependencias. |

| **RN 21 // Gestión de Horarios Diferenciado** | Gestión de Horarios Diferenciado |
| --- | --- |
| **tipo** | No funcional – Seguridad |
| **Rendimiento** | * **La validación de solapamientos debe realizarse en menos de 1 segundo al intentar guardar un horario.** * **El sistema debe soportar hasta 24 turnos diarios por ficha sin errores.** |
| **Usabilidad** | * La interfaz debe mostrar un **calendario semanal o tabla** con días y franjas horarias diferenciadas. * Los horarios deben visualizarse de forma **intuitiva y editable** (colores distintos para mañana, tarde, noche, horas extras). * En caso de error (ejemplo: solapamiento), el sistema debe mostrar un **mensaje claro y orientado al usuario**. |
| **Seguridad** | * Solo los usuarios con rol **Administrador** pueden crear, modificar o eliminar horarios. * Todas las modificaciones deben registrarse en un **log de auditoría** indicando usuario, fecha y acción. |
| Escalabilidad y consistencia | * El sistema debe soportar al menos **24 fichas simultáneamente con horarios semanales distintos**. * Los cambios en horarios deben reflejarse **en tiempo real** en el historial y estadísticas del sistema. * No se deben permitir **solapamientos en la misma ficha y franja horaria** |

| **RN 22 // Interfaz dinámica y clara** | **Módulo Historial + Excusas** |
| --- | --- |
| **Tipo** | REQUERIMIENTO NO FUNCIONAL |
| **Usabilidad** | * El calendario debe ser **intuitivo y visual**, usando colores o íconos claros para diferenciar: asistencia, ausencia, tardanza y salida anticipada. * El formulario de excusas debe ser sencillo: seleccionar fecha, escribir motivo y adjuntar evidencia. * El usuario debe poder **navegar fácilmente entre semanas y meses**. |
| **Rendimiento** | * El historial de un usuario debe cargarse en un tiempo máximo de **2 segundos** para un rango de un mes. * El sistema debe ser capaz de mostrar al menos **12 meses de historial sin degradación perceptible del rendimiento**. |
| **Seguridad** | -El sistema debe validar que las excusas solo puedan enviarse **para días futuros y con al menos 1 día de anticipación**. -Cada excusa enviada debe quedar asociada al usuario autenticado (no se permiten registros anónimos). -Las evidencias adjuntas (archivos) deben almacenarse en un repositorio seguro y encriptado. |
| **Disponibilidad** | * El historial debe estar disponible en todo momento mientras el sistema esté en línea (99% uptime). * - Las excusas deben poder registrarte desde cualquier dispositivo con conexión a internet. |
| **Confiabilidad e Integridad de Datos** | * Una vez enviada una excusa, esta debe quedar registrada en la base de datos **sin posibilidad de ser alterada por el aprendiz**. * Solo el instructor o administrador podrá aprobar o rechazar la excusa, quedando la acción registrada en la auditoría. * No se debe permitir duplicar excusas para el mismo usuario y misma fecha. |
| **Auditoría y Trazabilidad** | Cada acción relacionada con el historial o excusas debe generar un registro en el **log de auditoría** con:   * Usuario * Fecha y hora de la acción. * Tipo de acción (envió excusa, modificó horario, consultó historial). |

| **RN 23 // Estadísticas de Usuarios** | **Estadísticas de Usuarios** |
| --- | --- |
| **tipo** | No funcional – Seguridad |
| **seguridad** | * Solo los usuarios con rol autorizado pueden acceder a las estadísticas asignadas. * No se deben exponer datos de otros roles ni en consultas directas a la base de datos. |
| **Usabilidad** | * Las estadísticas deben mostrarse en **gráficas claras e interactivas** (ej. barras, pastel, líneas). |

| **RN 24 // Gestión de Horarios/Turnos** | Gestión de Horarios/Turnos |
| --- | --- |
| **tipo** | No funcional – Seguridad |
| **Seguridad** | * Solo los roles autorizados (**Administrador, Instructor, Secretaría**) podrán modificar los horarios. * Los cambios deben quedar registrados en la bitácora de auditoría. |
| **Usabilidad** | * Los horarios deben mostrarse en un **calendario semanal interactivo** (tipo grid o tabla visual). |

| **RN 25 // Asociación de Instructores a Fichas** | Asociación de Instructores a Fichas |
| --- | --- |
| **tipo** | No funcional – Seguridad |
| **integridad de datos:** | * No se debe permitir que un instructor quede asignado a dos fichas en la misma franja horaria. * Una ficha no puede quedar sin instructor asignado. |
| **Trazabilidad** | * Todas las asociaciones o cambios deben quedar registradas en la bitácora con: usuario que realizó el cambio, fecha y hora. |
| **Usabilidad** | * La interfaz debe permitir seleccionar **fácilmente fichas e instructores desde menús desplegables**. |
| **Seguridad** | * Solo los roles autorizados (**Administrador, Instructor, Secretaría**) podrán realizar asociaciones. |

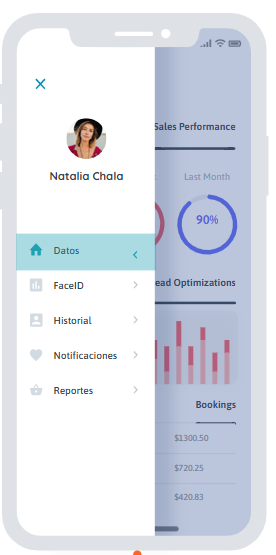
| **RN 26 // Configuración Personal del Usuario** | Configuración Personal del Usuario |
| --- | --- |
| **tipo** | No funcional – Seguridad |
| **Seguridad** | * Solo el usuario autenticado puede acceder a su propia configuración. * No se permitirá que un usuario modifique los datos de otro. * La eliminación de cuenta debe pedir confirmación adicional (ej. “¿Está seguro?”). |
| **Usabilidad** | * La interfaz de configuración debe ser clara, con botones visibles para **Cerrar sesión, Cambiar de cuenta y Modificar datos**. * El sistema debe actualizar los cambios del perfil en tiempo real. |
| **Disponibilidad** | * Las opciones de configuración deben estar siempre accesibles desde cualquier módulo (ej. menú superior). |
| **Auditoría:** | * Cada cambio de nombre, apellido o eliminación de cuenta debe registrarse en el log del sistema. |

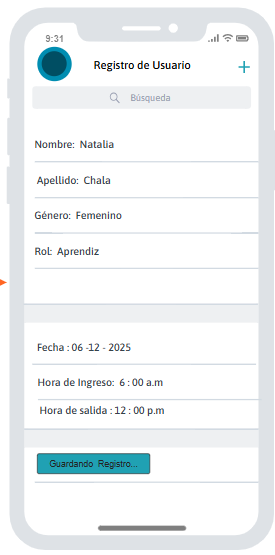
**BOSQUEJO DE REQUERIMIENTOS FUNCIONALES.**

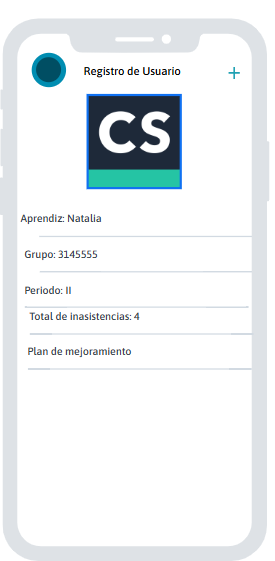
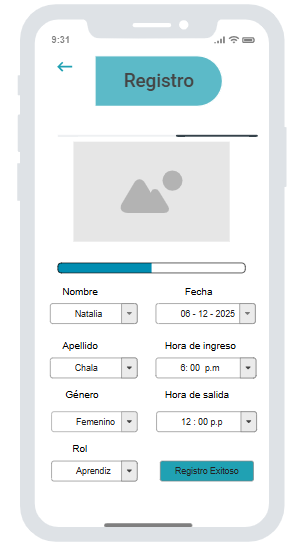
Interfaz de usuario gráfica, Aplicación

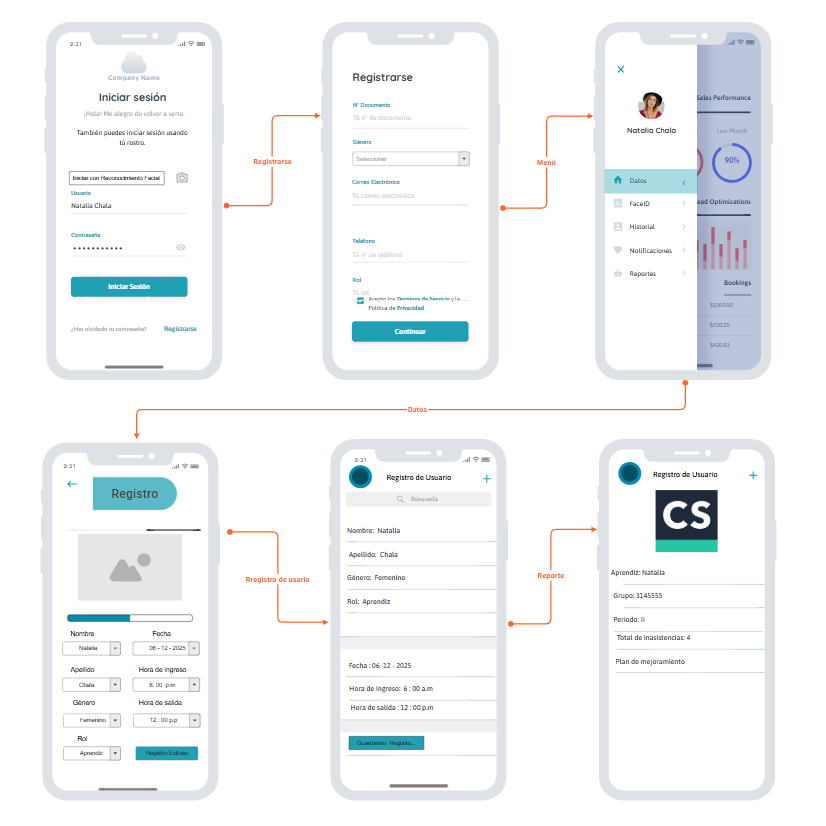
El contenido generado por IA puede ser incorrecto.Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.



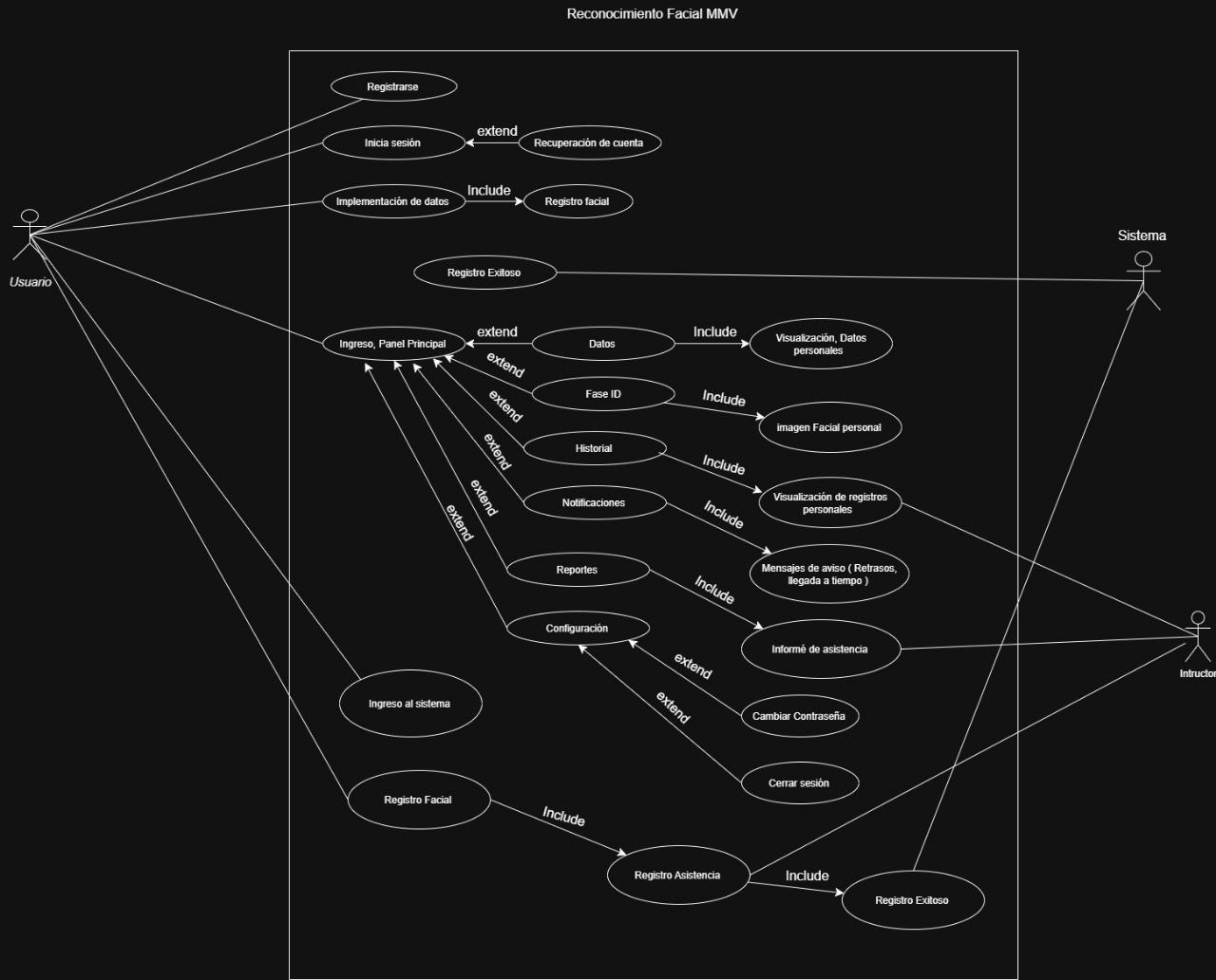




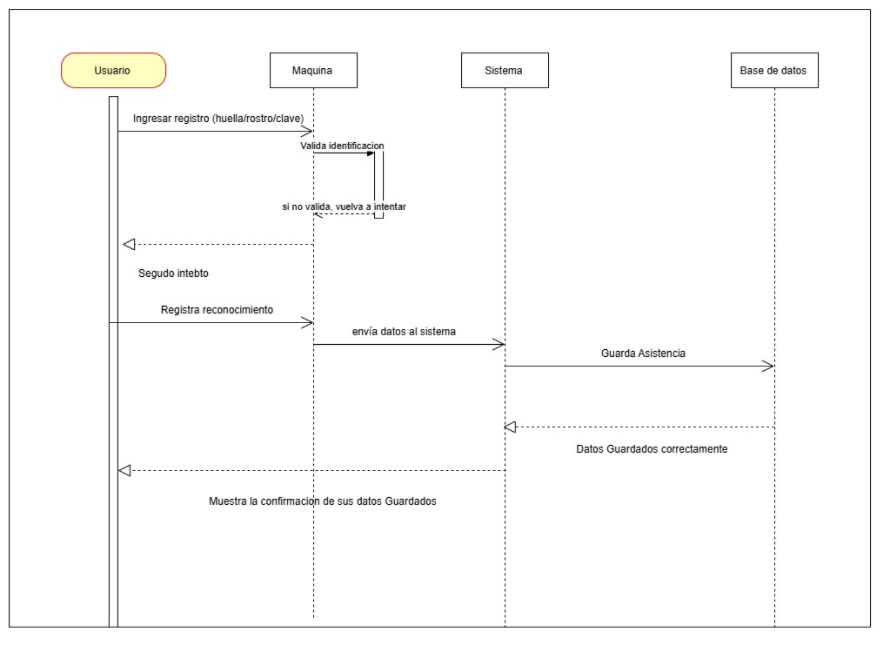


# Requisitos de Casos de Uso.

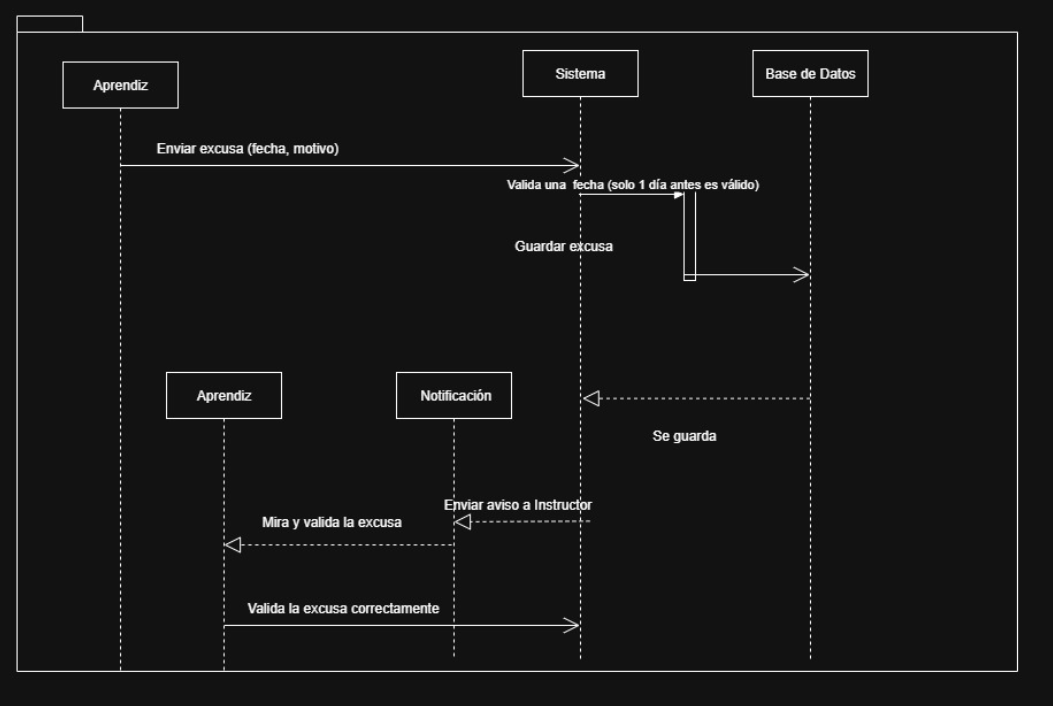
## Diagrama UML de casos de uso.



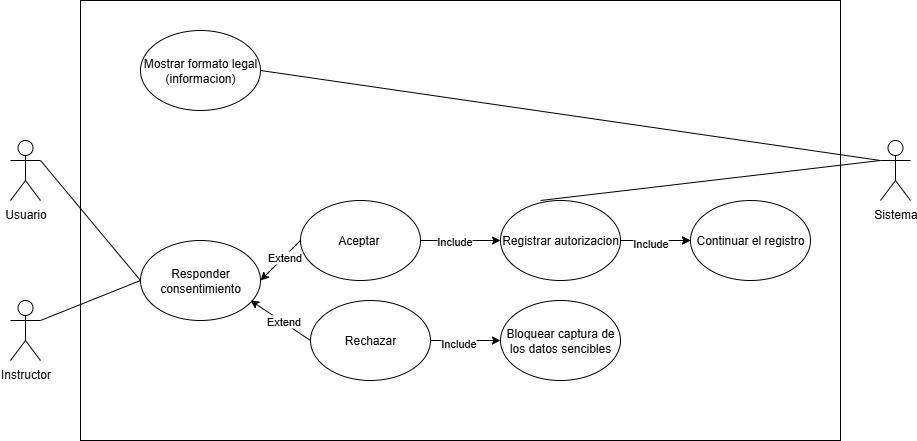
**1 ) visualisacion de diagrama de secuencia**

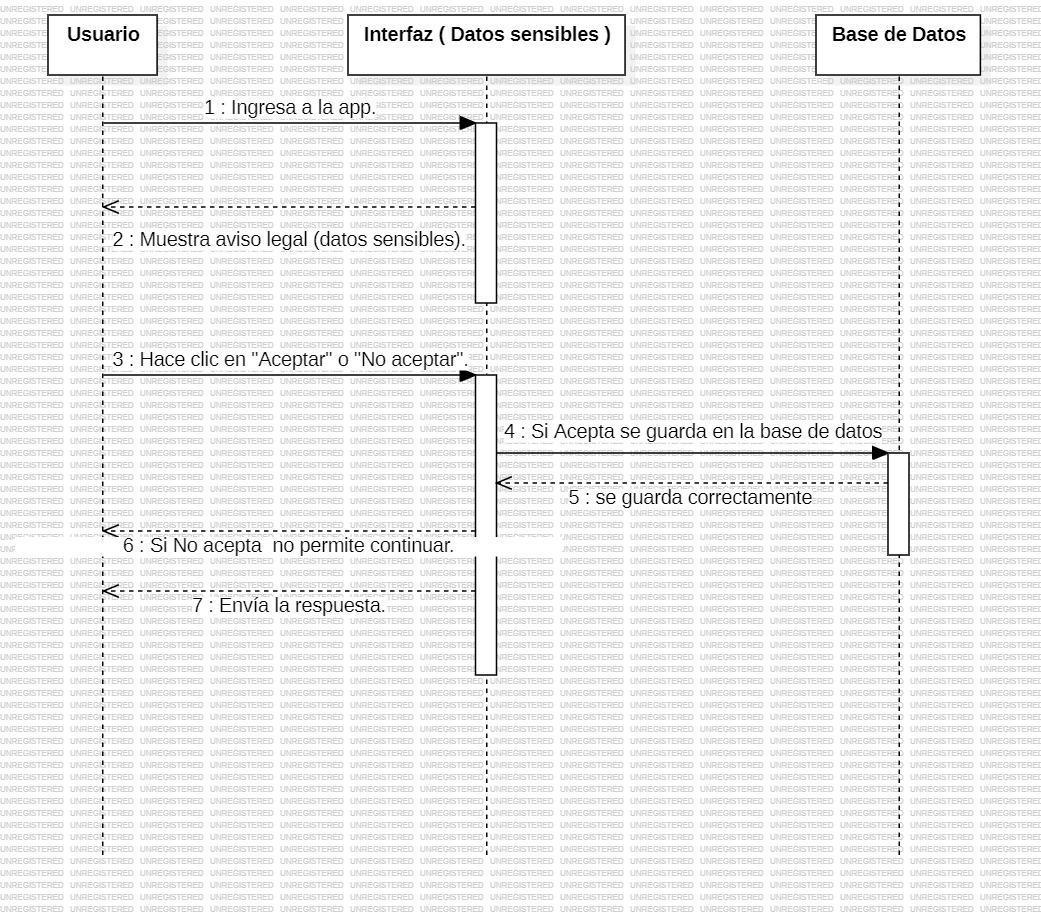


**2. ) enviar excusas**

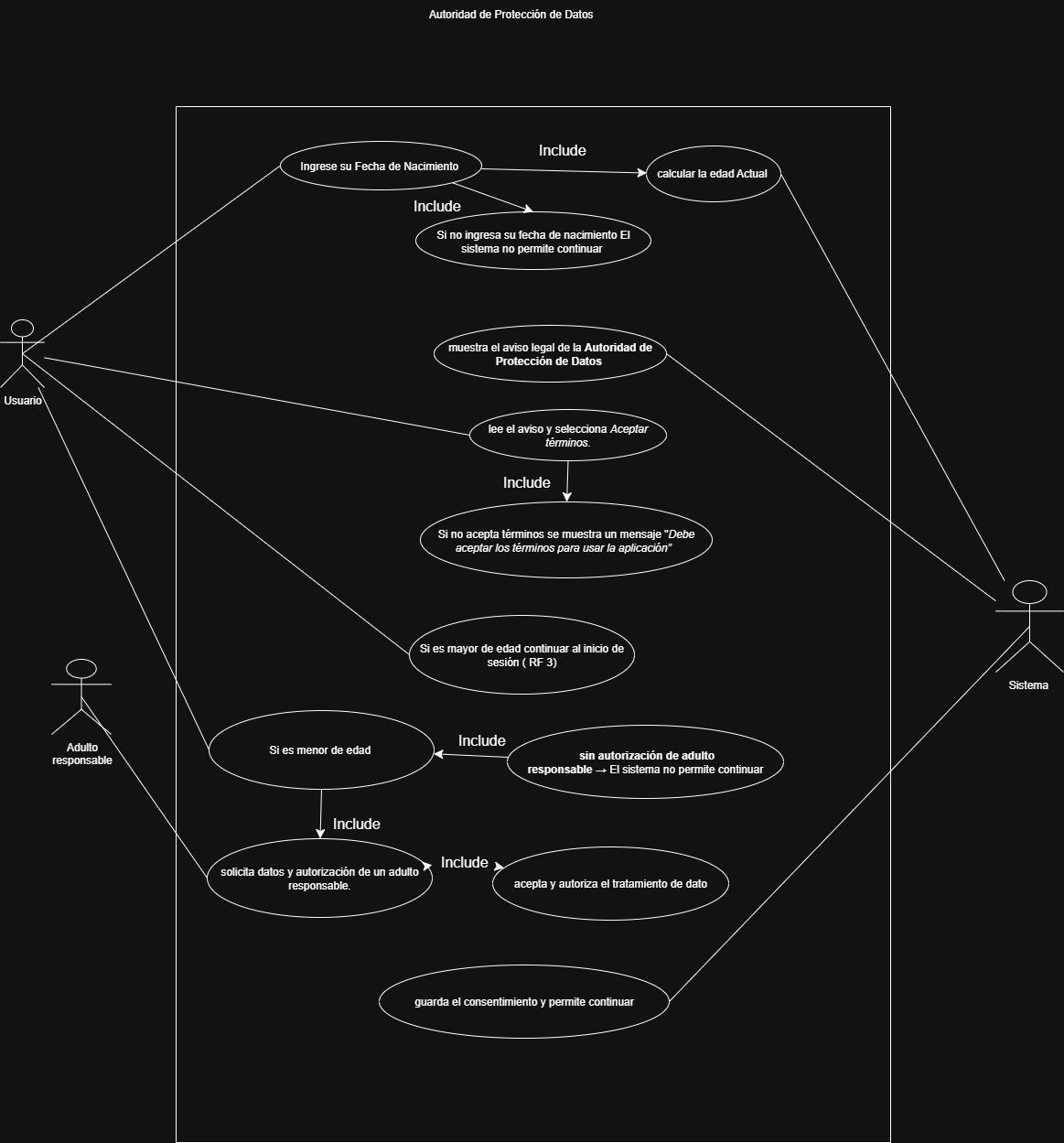


***Casos de uso ( Imagen ) CASO 1 #***

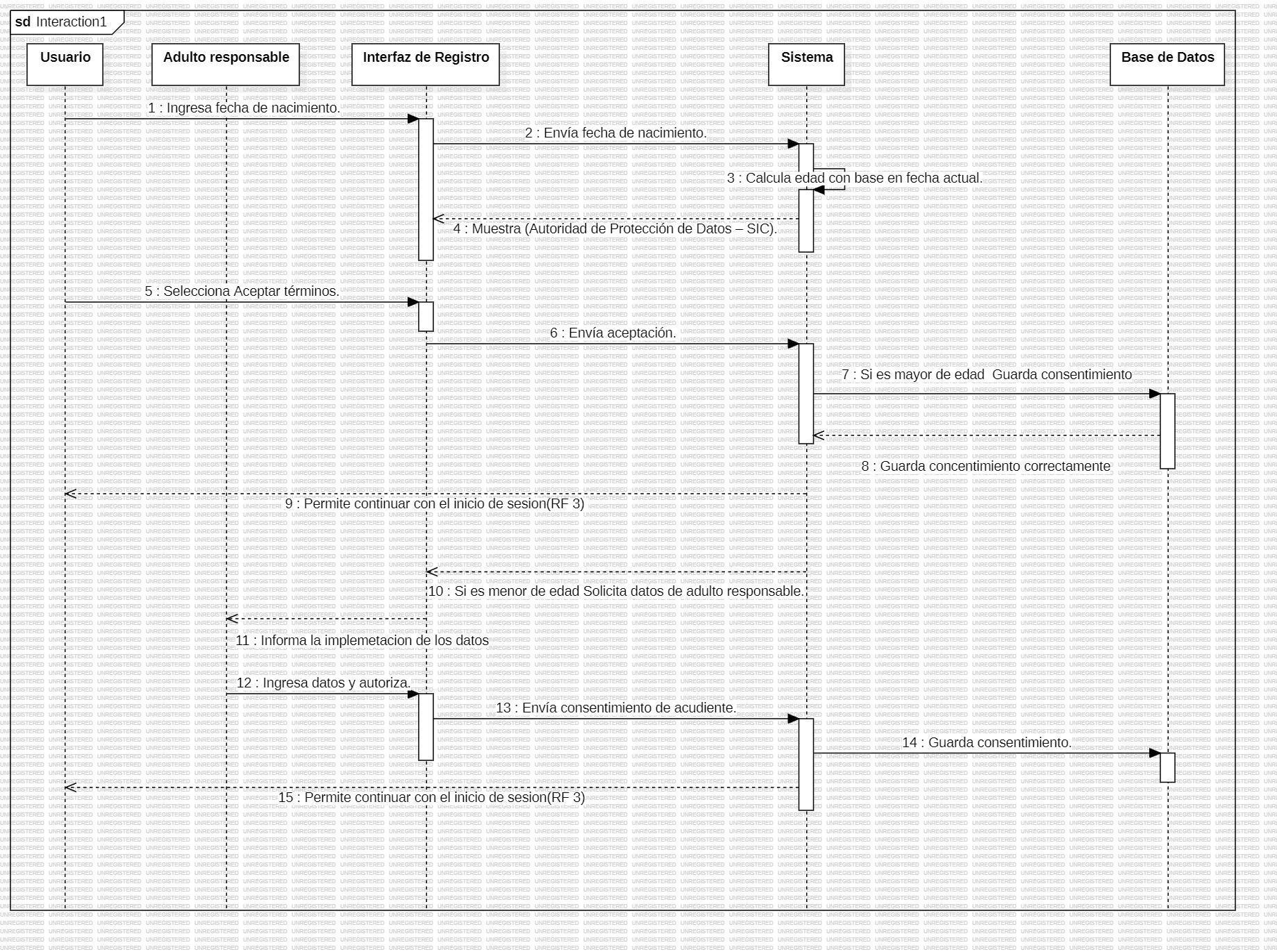


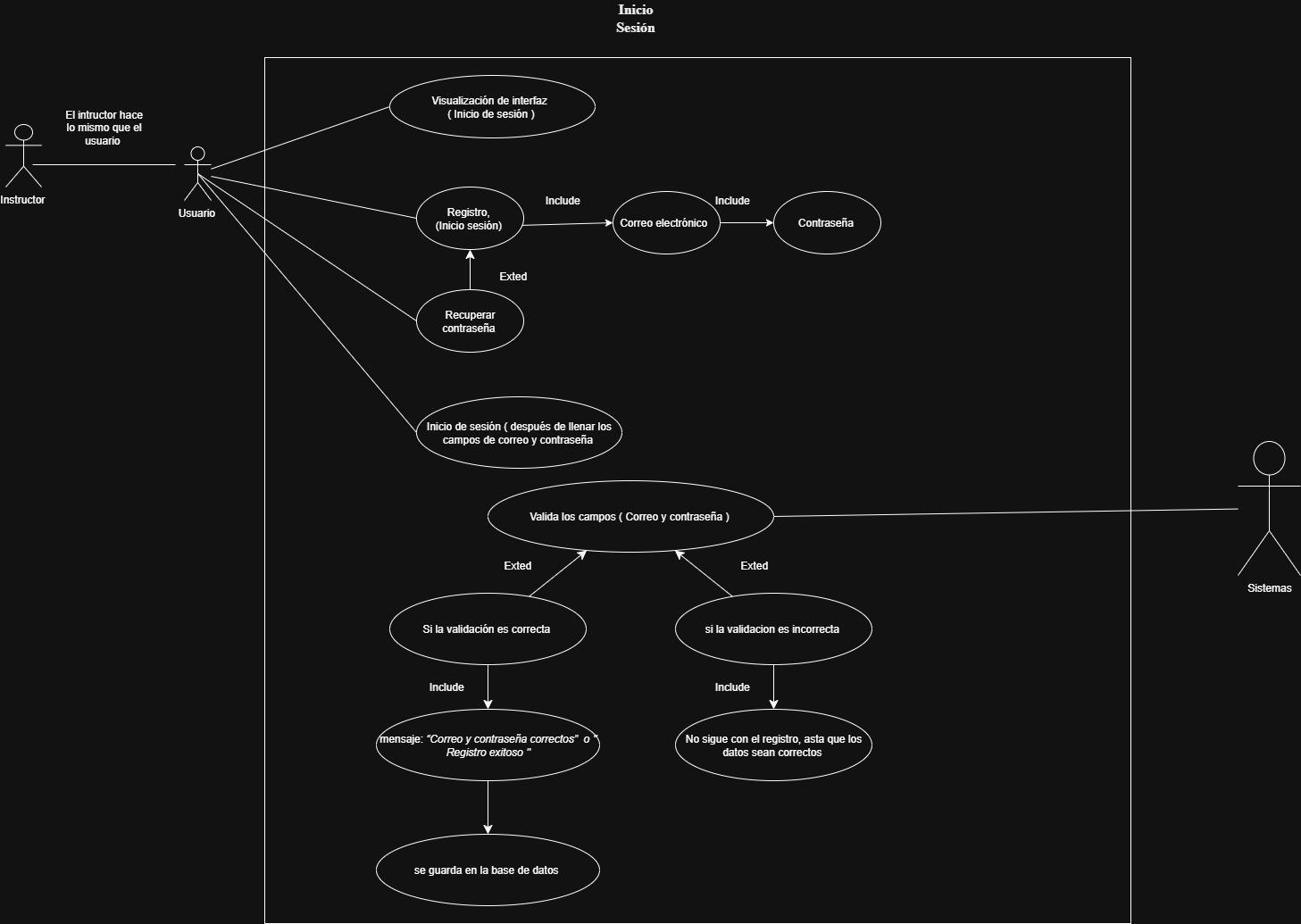
***DIAGRAM DE SECUENCIA 1*** 

***caso de uso 2***

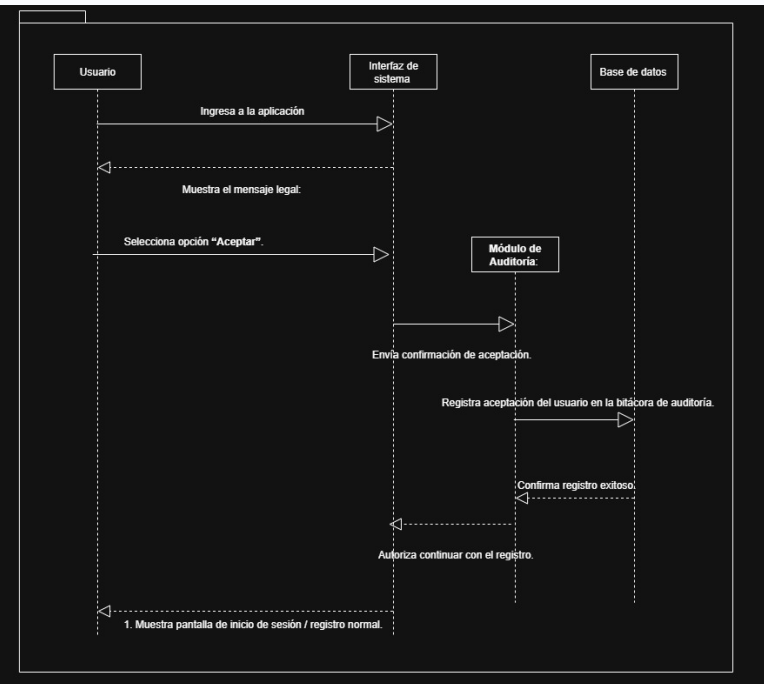


***Diagrama de secuencia 2***

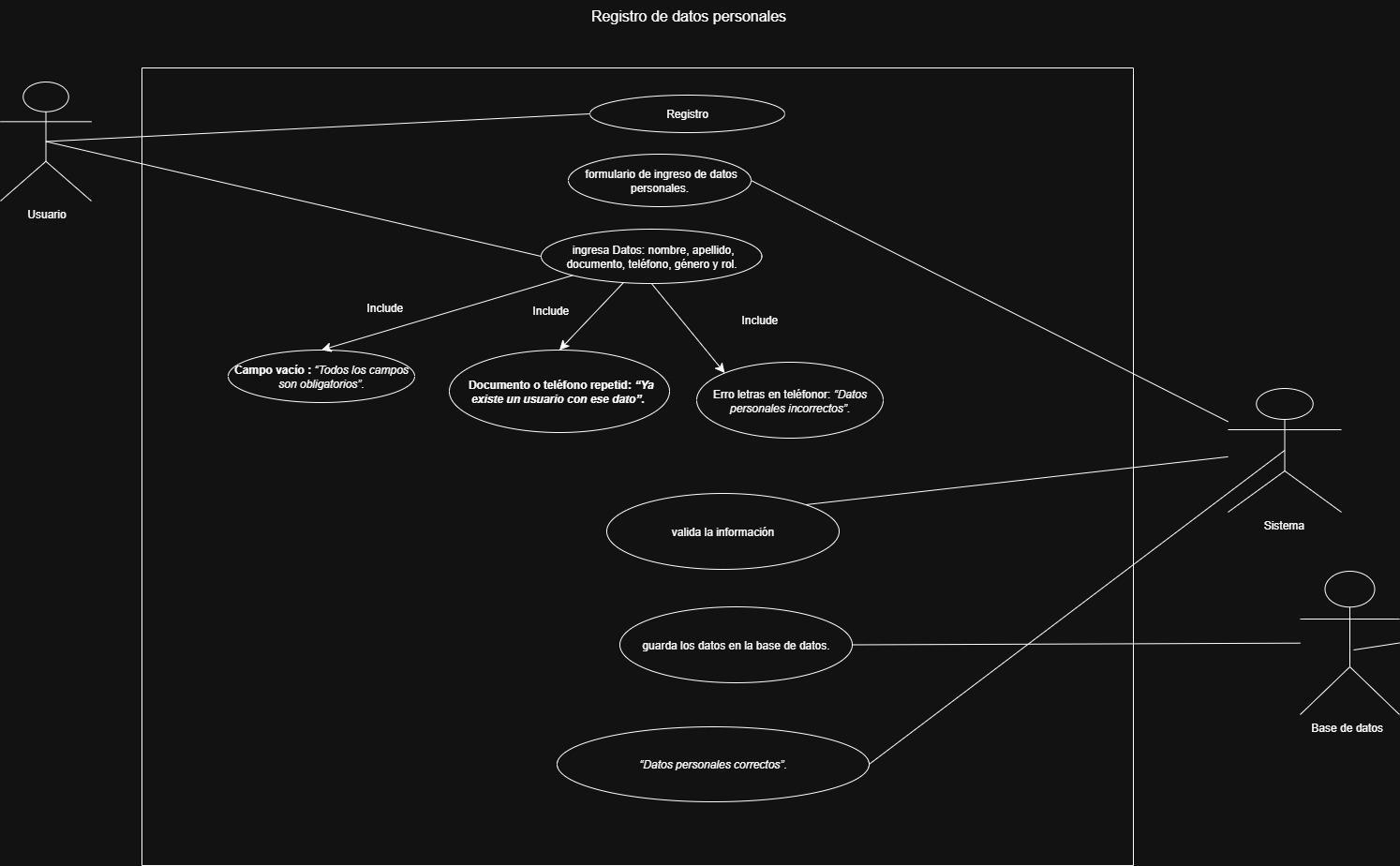


***CASO 3 #*** 

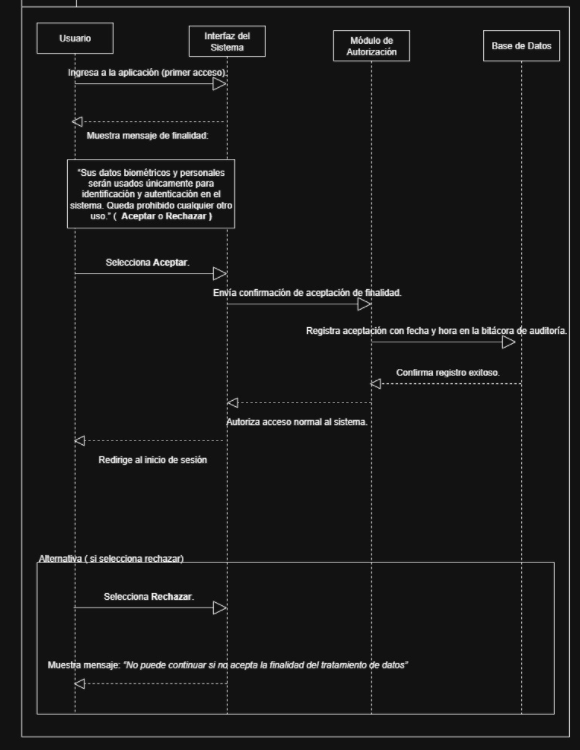
***Diagrama de secuencia 3***



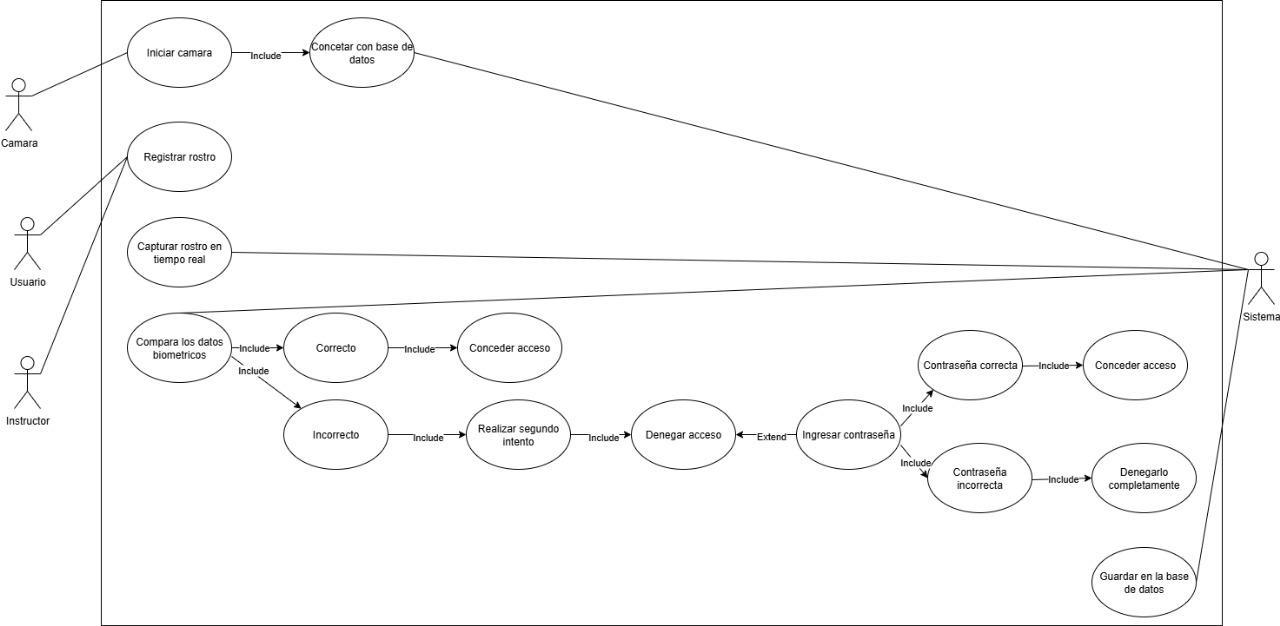
***Caso de uso 4 #***



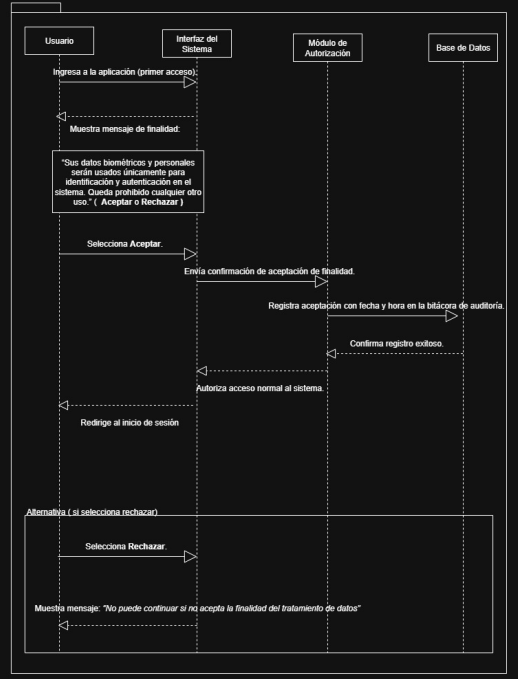
***DIAGRAMA DE SECUENCIA 4 #***



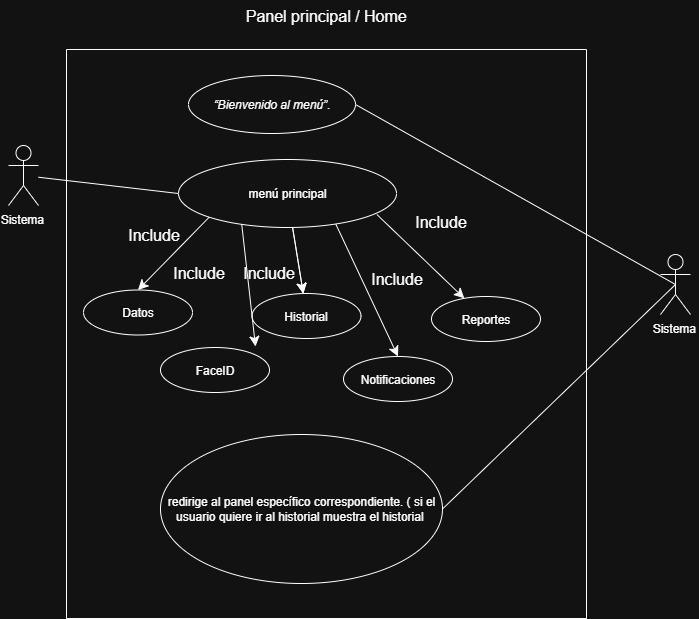
***Casos de uso 5 #***



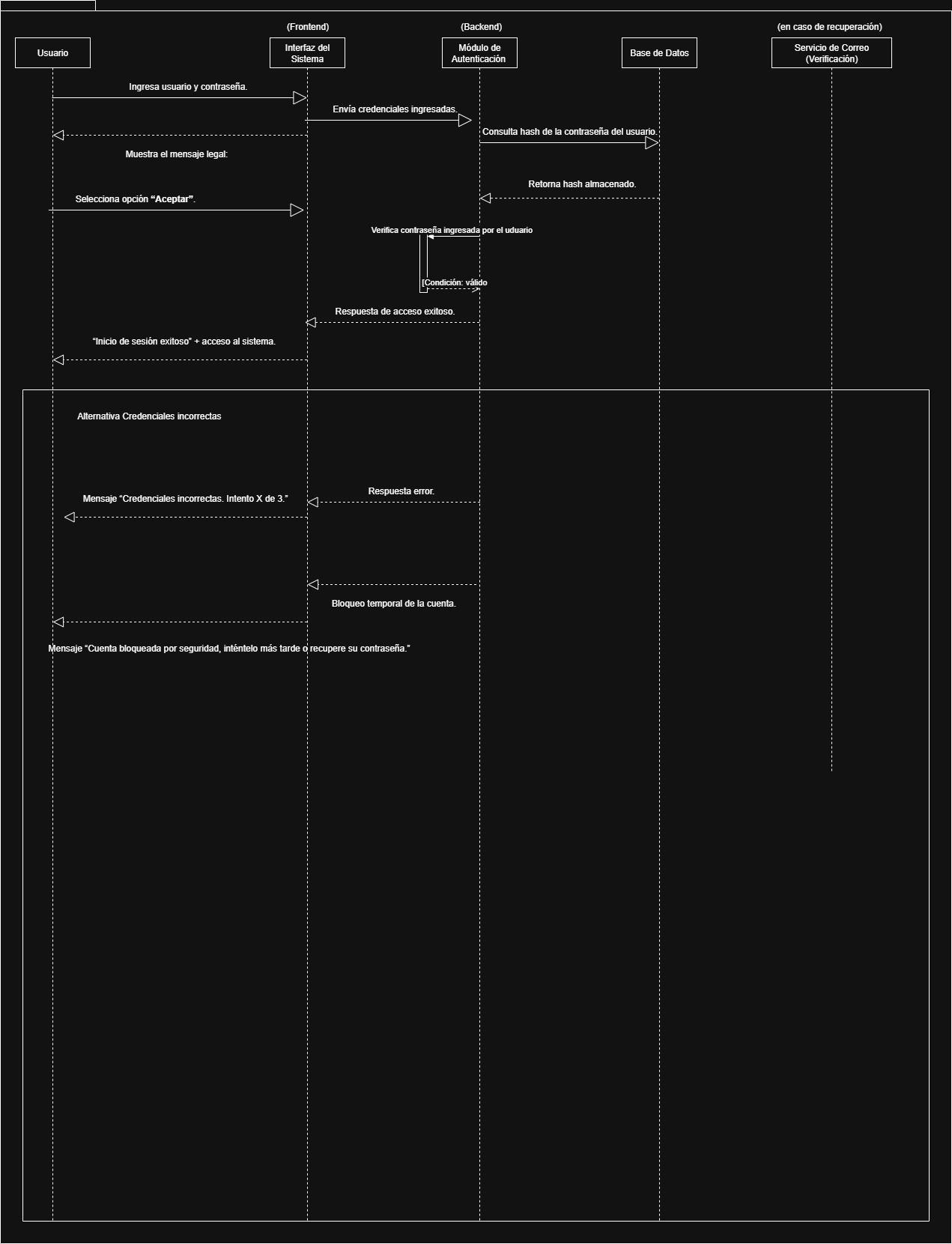
***Diagrama de secuencias 5 #***



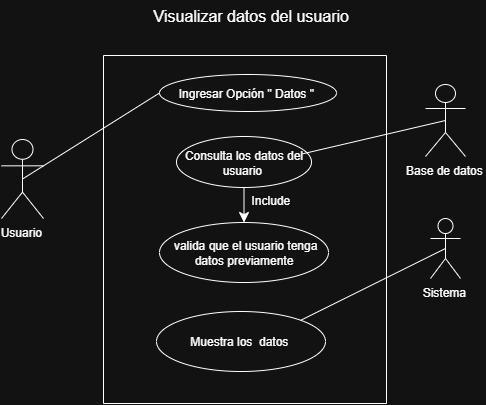
***Caso de uso 6 # ( Panel principal )***



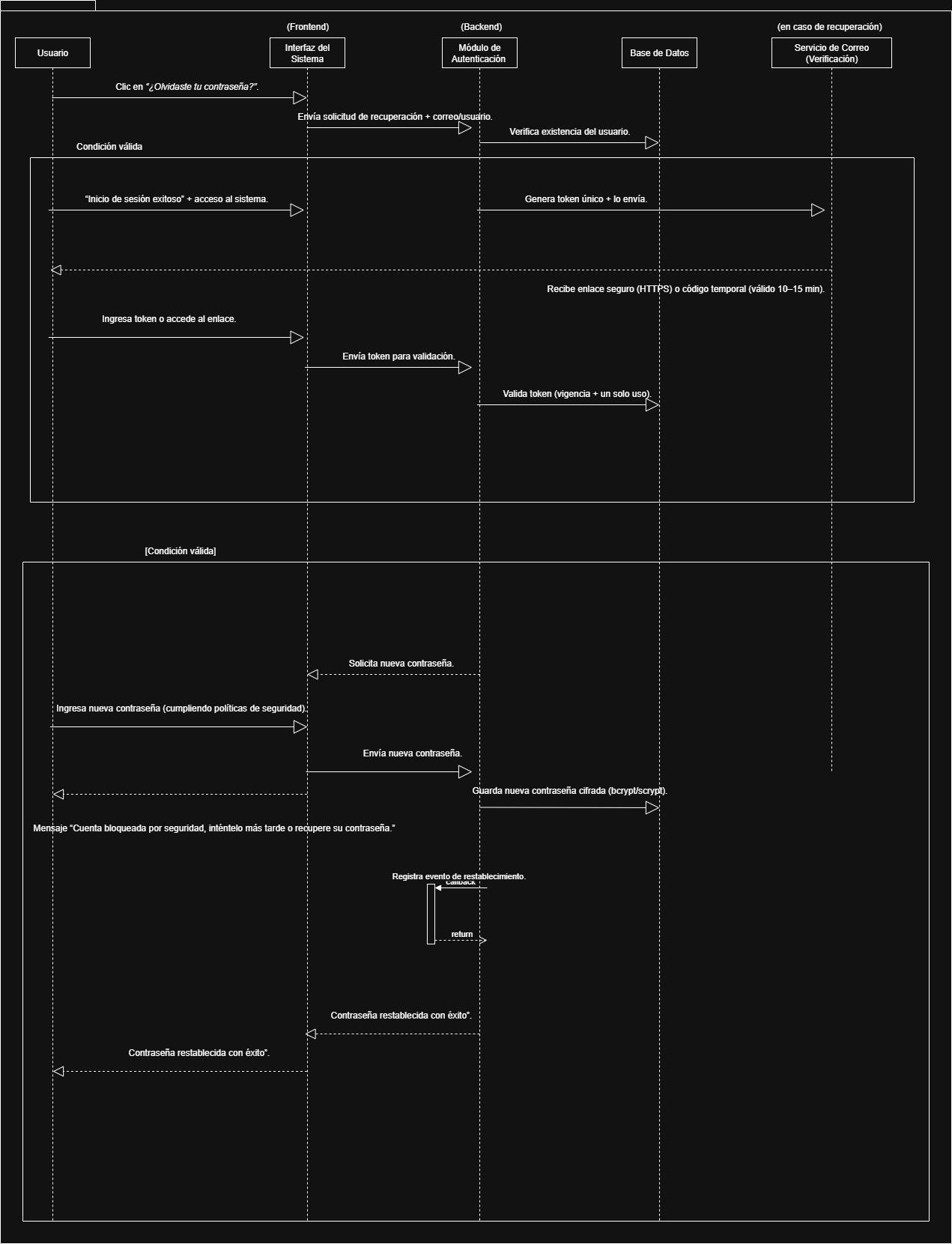
***Diagrama de secuencias 6***



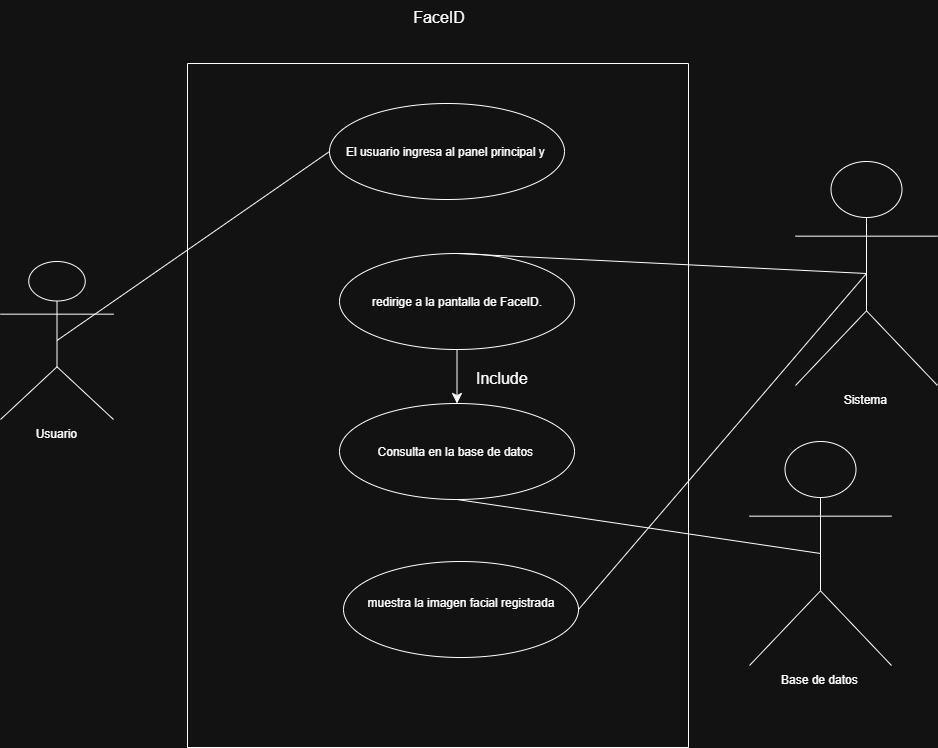
***Caso de uso 7 ( Visualización de datos )***



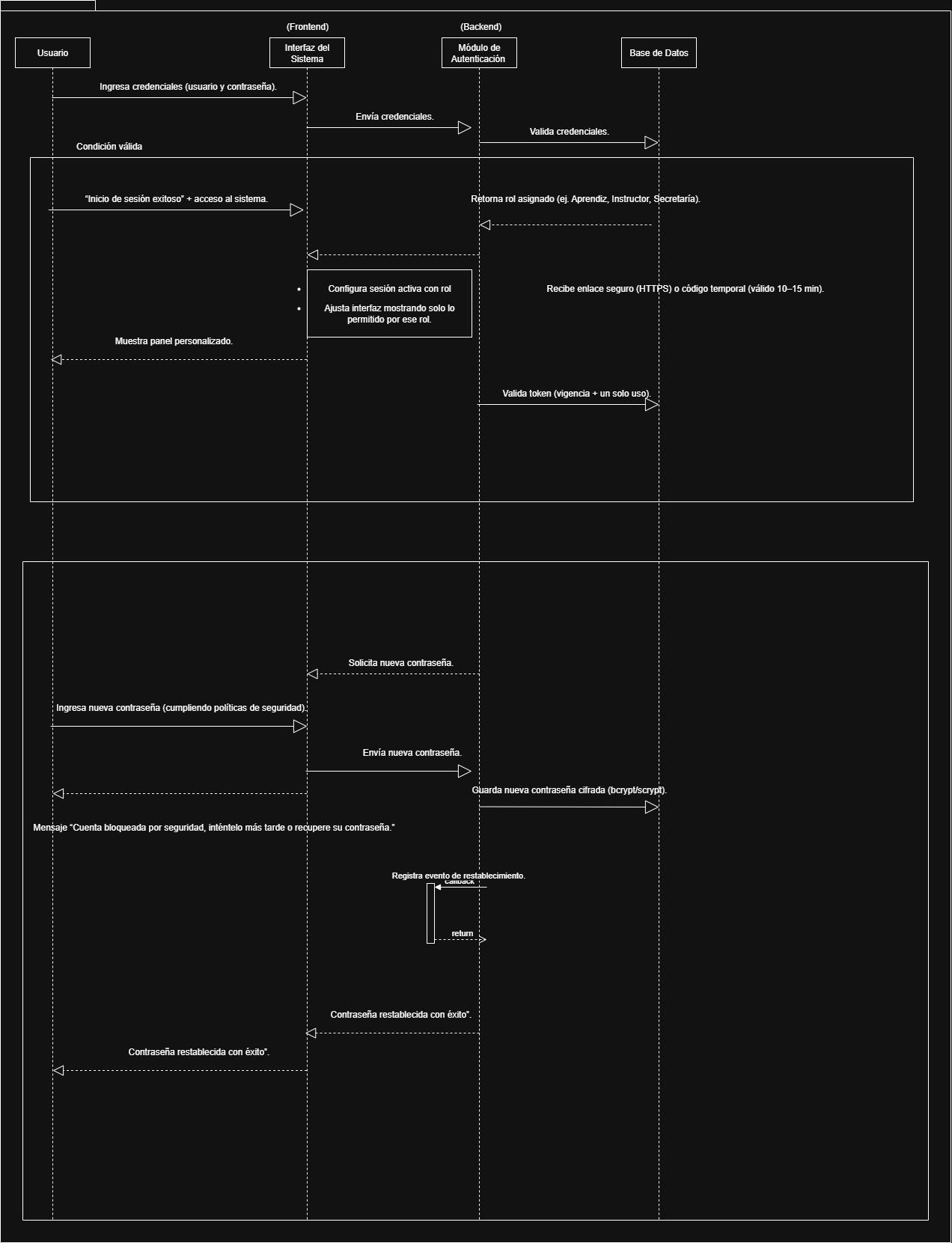
***Diagrama de secuencia 7***



***Caso de uso 8 ( Visualización Face ID )***



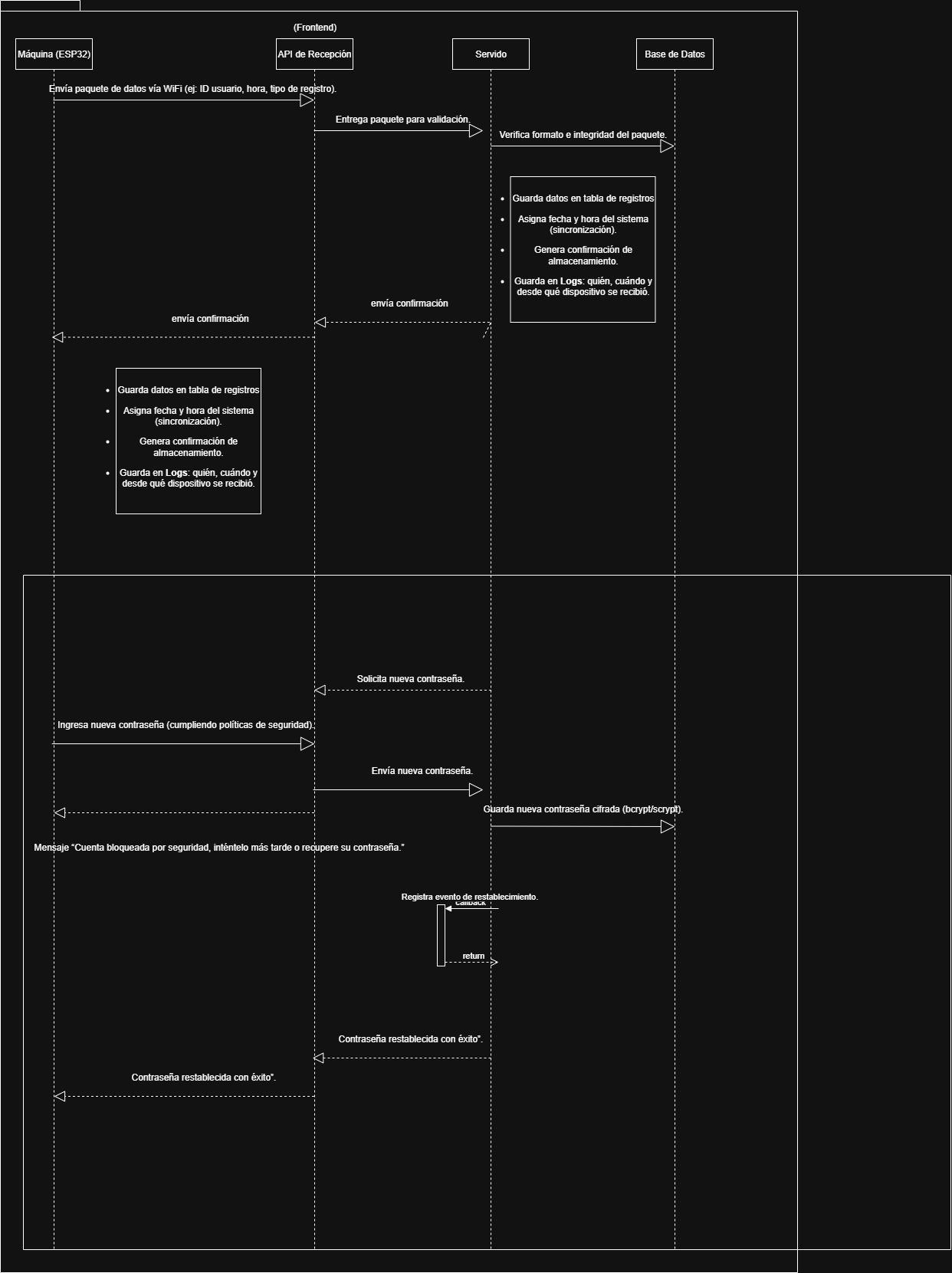
***Diagrama de secuencia 8***



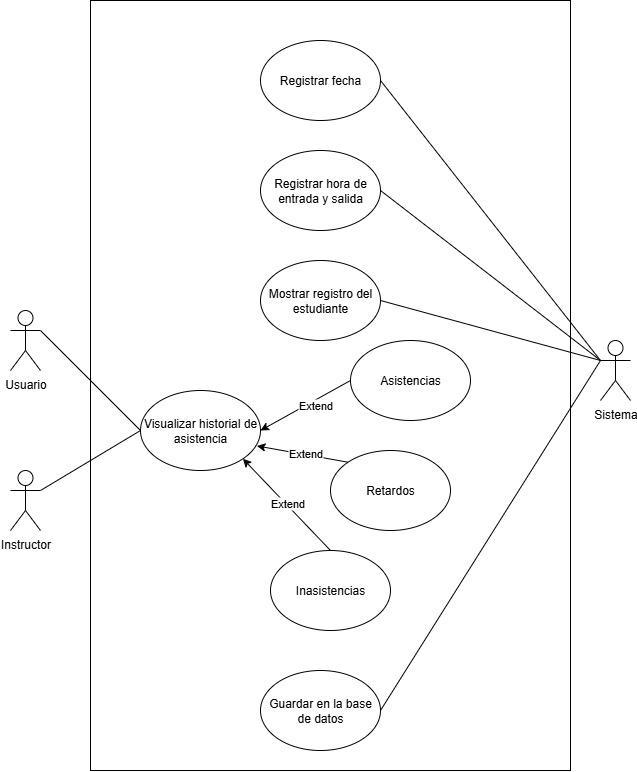
***Caso de uso 9 ( Ingresar FACE ID ya para lista )***



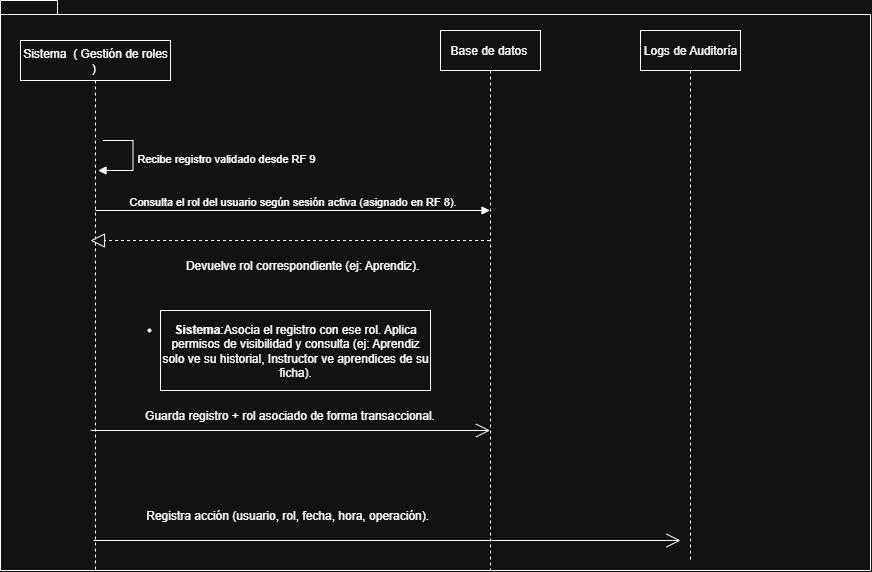
***Diagrama de secuencia 9 #***



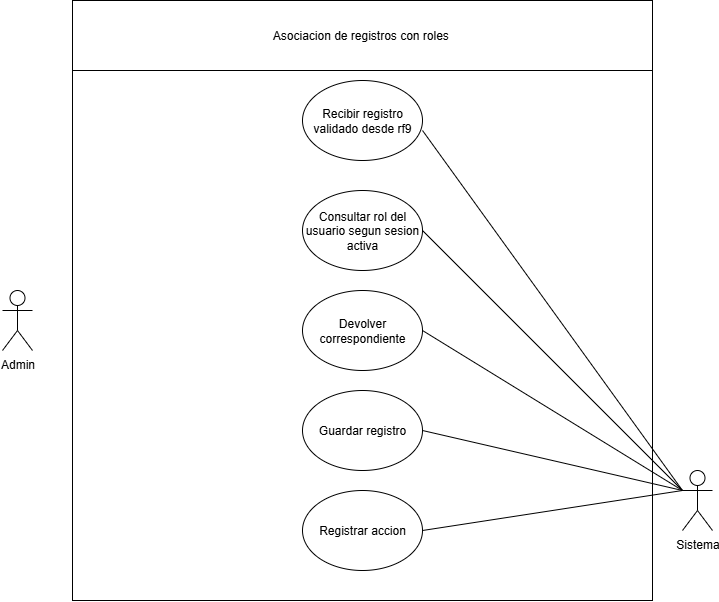
***Caso de uso #***



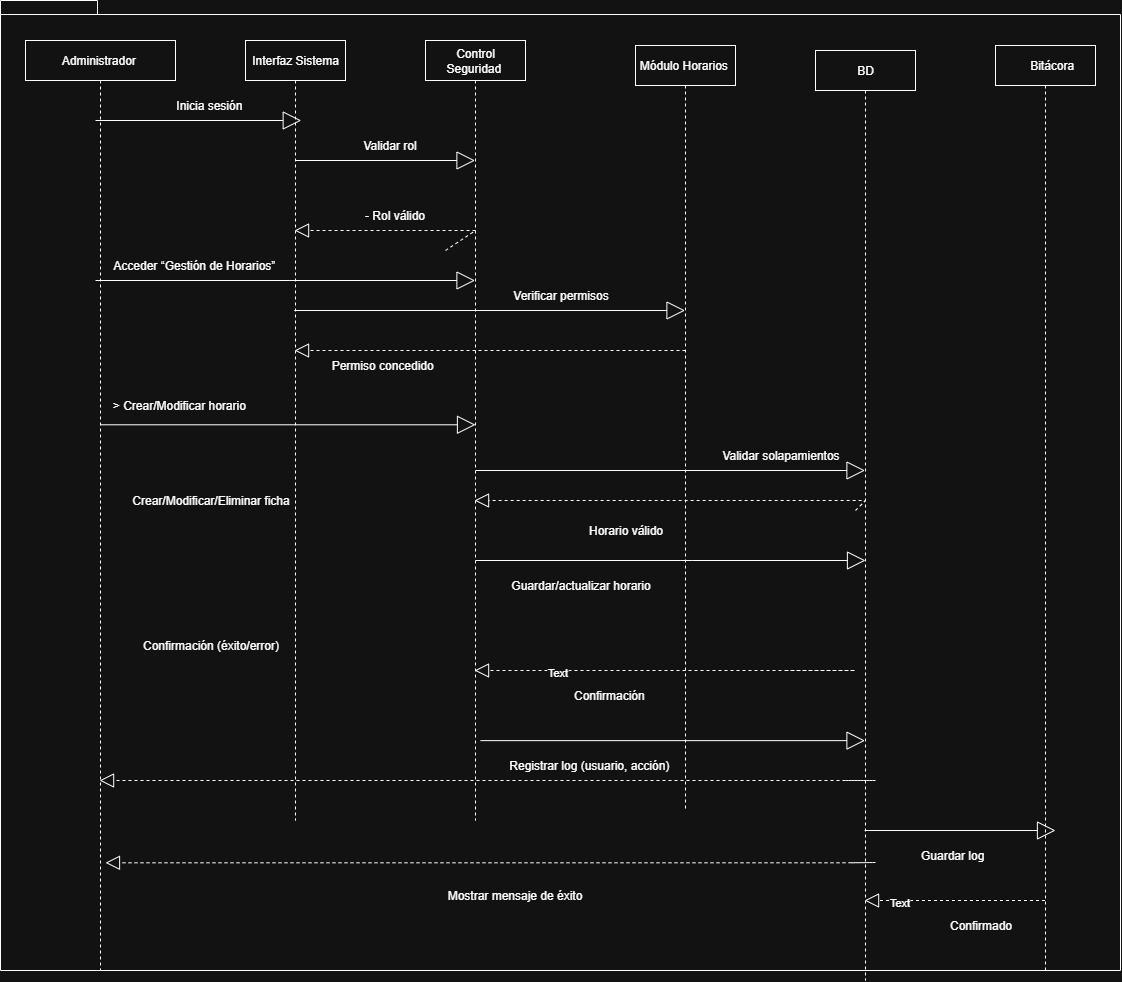
***Diagrama de secuencia 9.1 #***



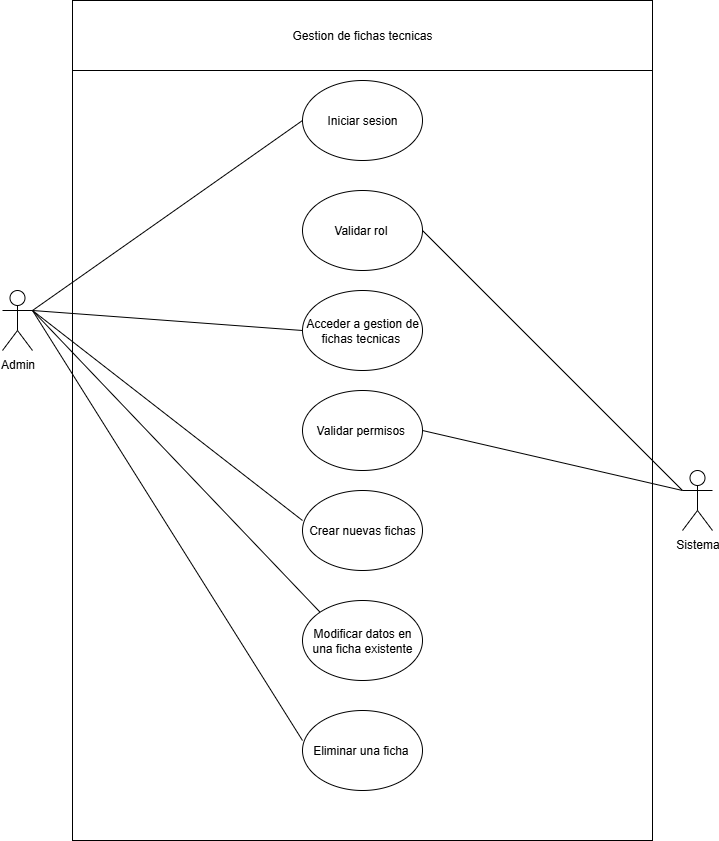
***Caso de uso 9.1 #***

******

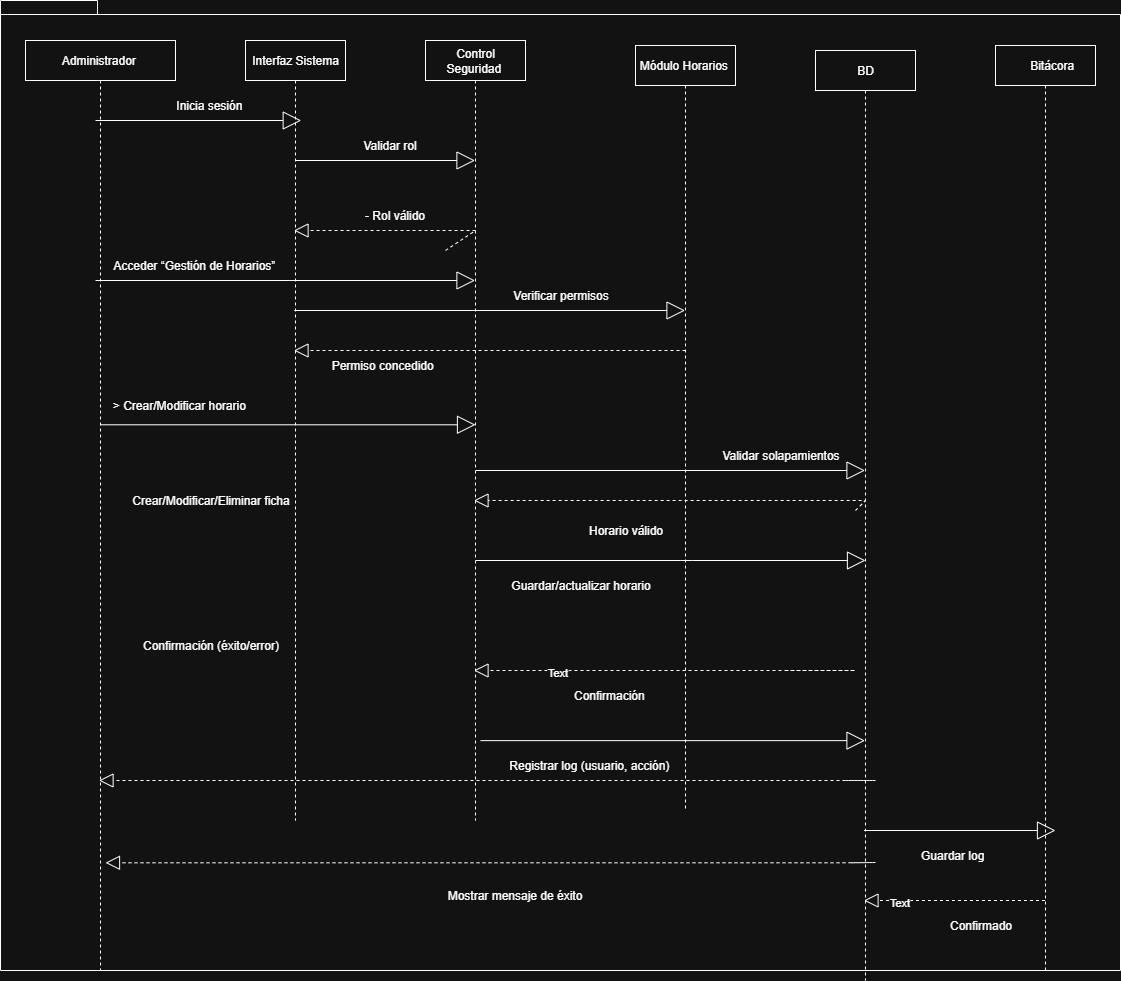
***Diagrama se secuencia 10 #***



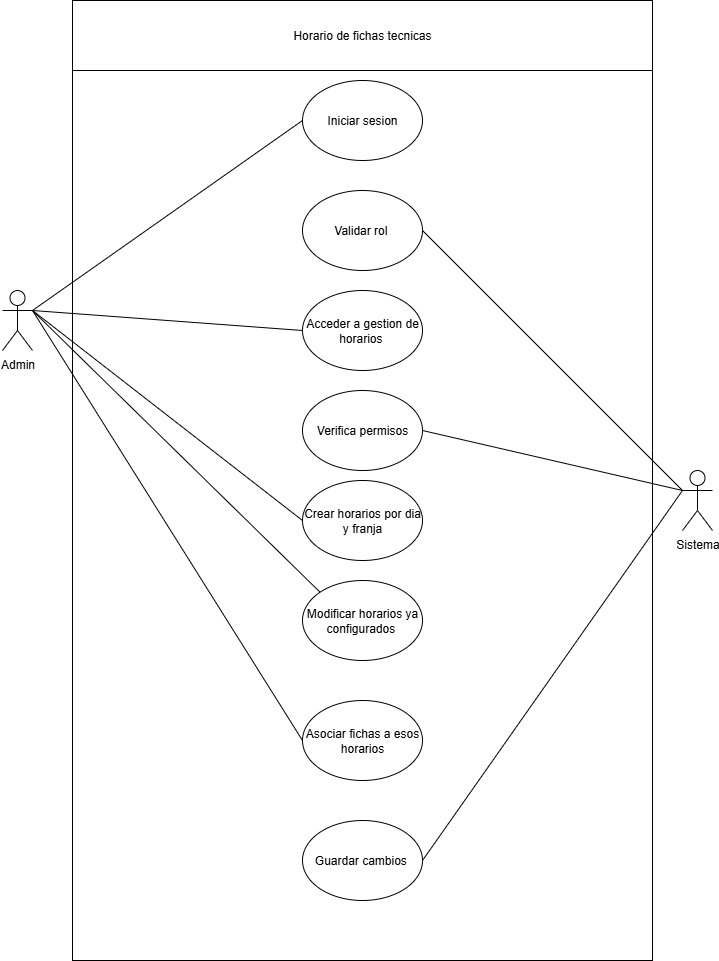
***Caso de uso 10 #***

******

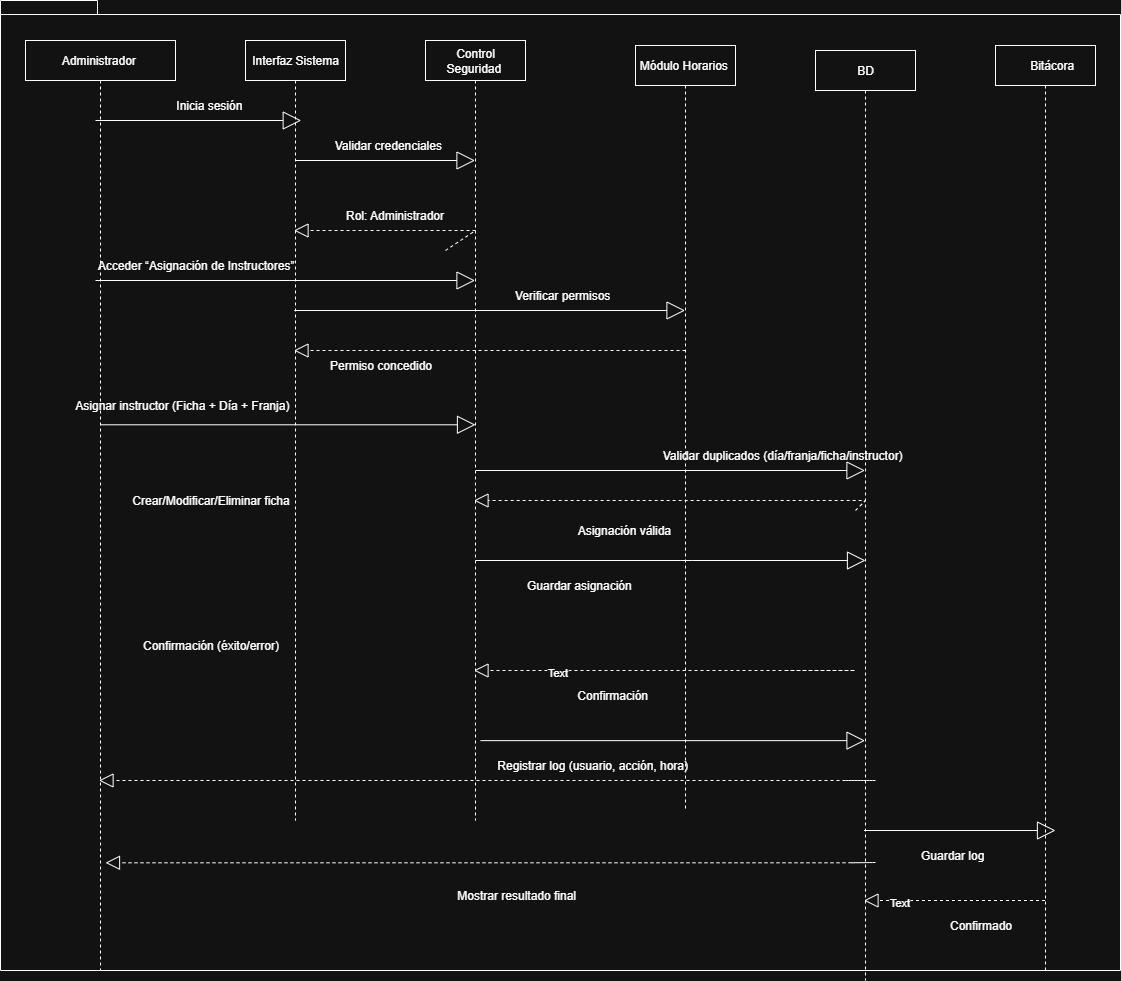
***Diagrama de secuencia 11 #***

******

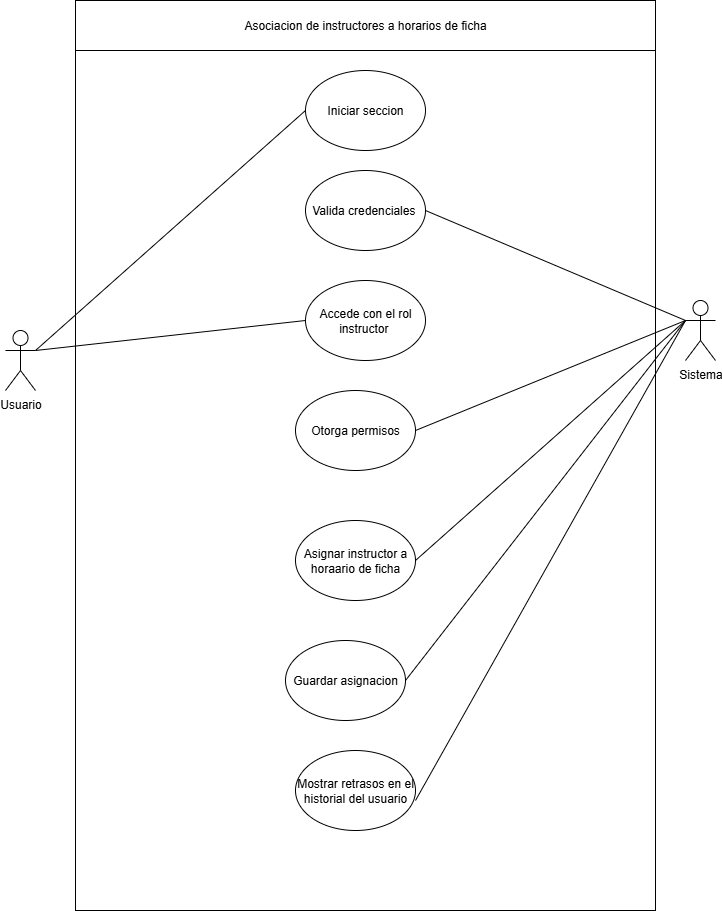
***Caso de uso 11 #***

******

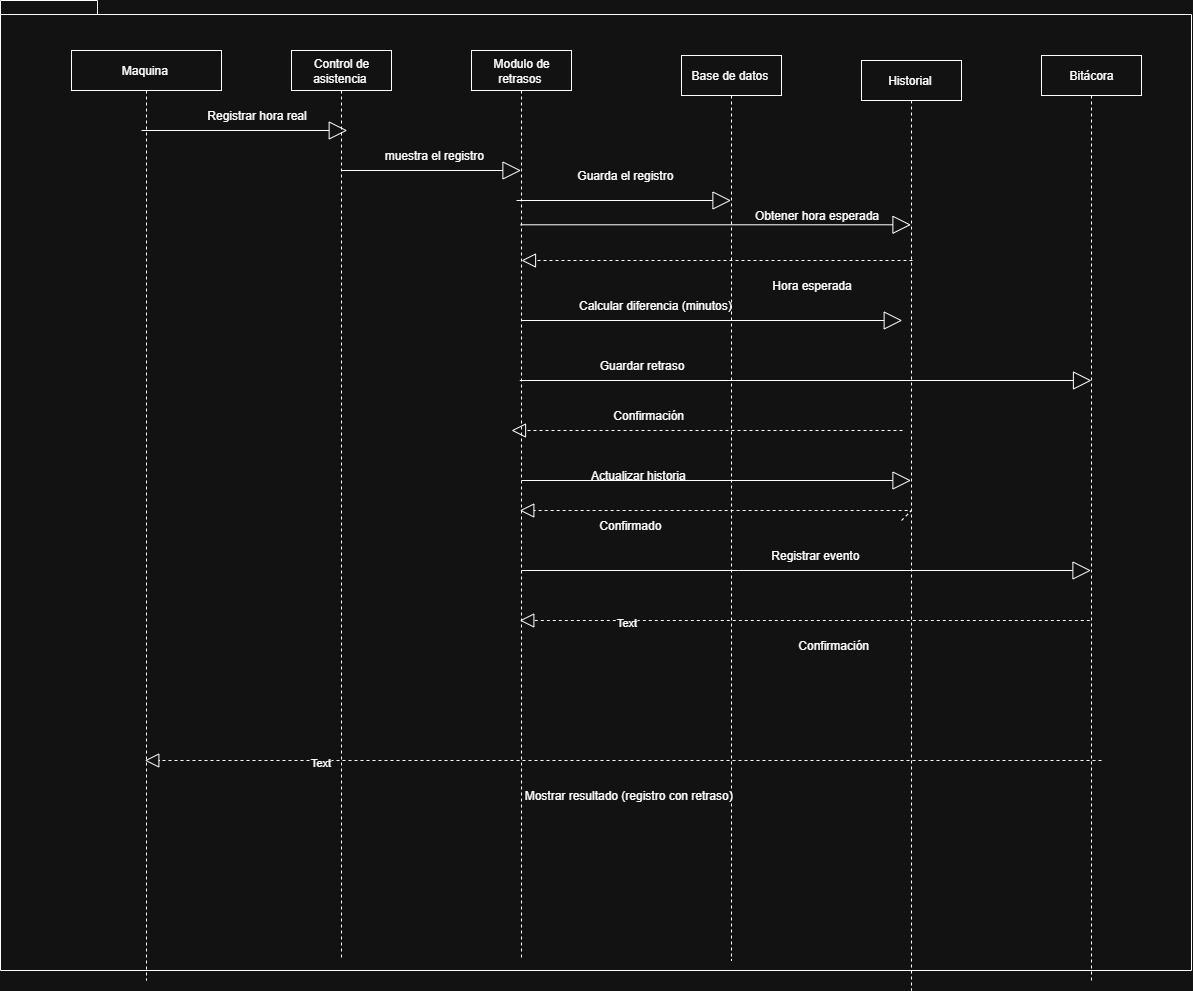
***Diagrama de secuencia 11.1 #***



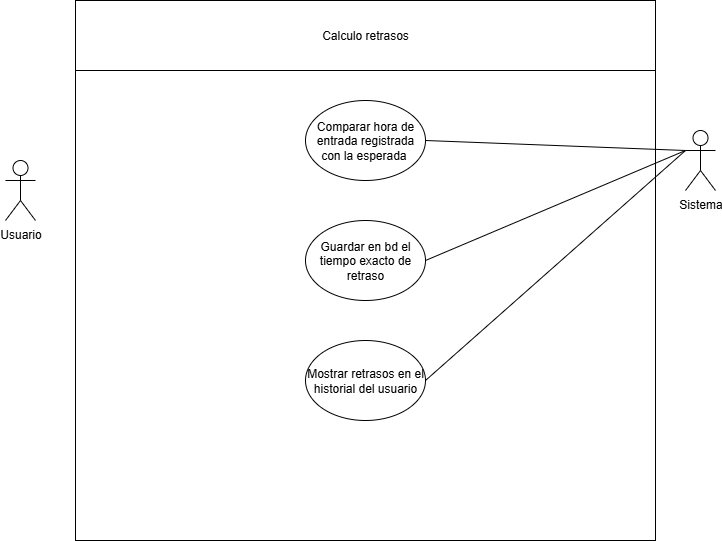
***Caso de uso 11.1 #***

******

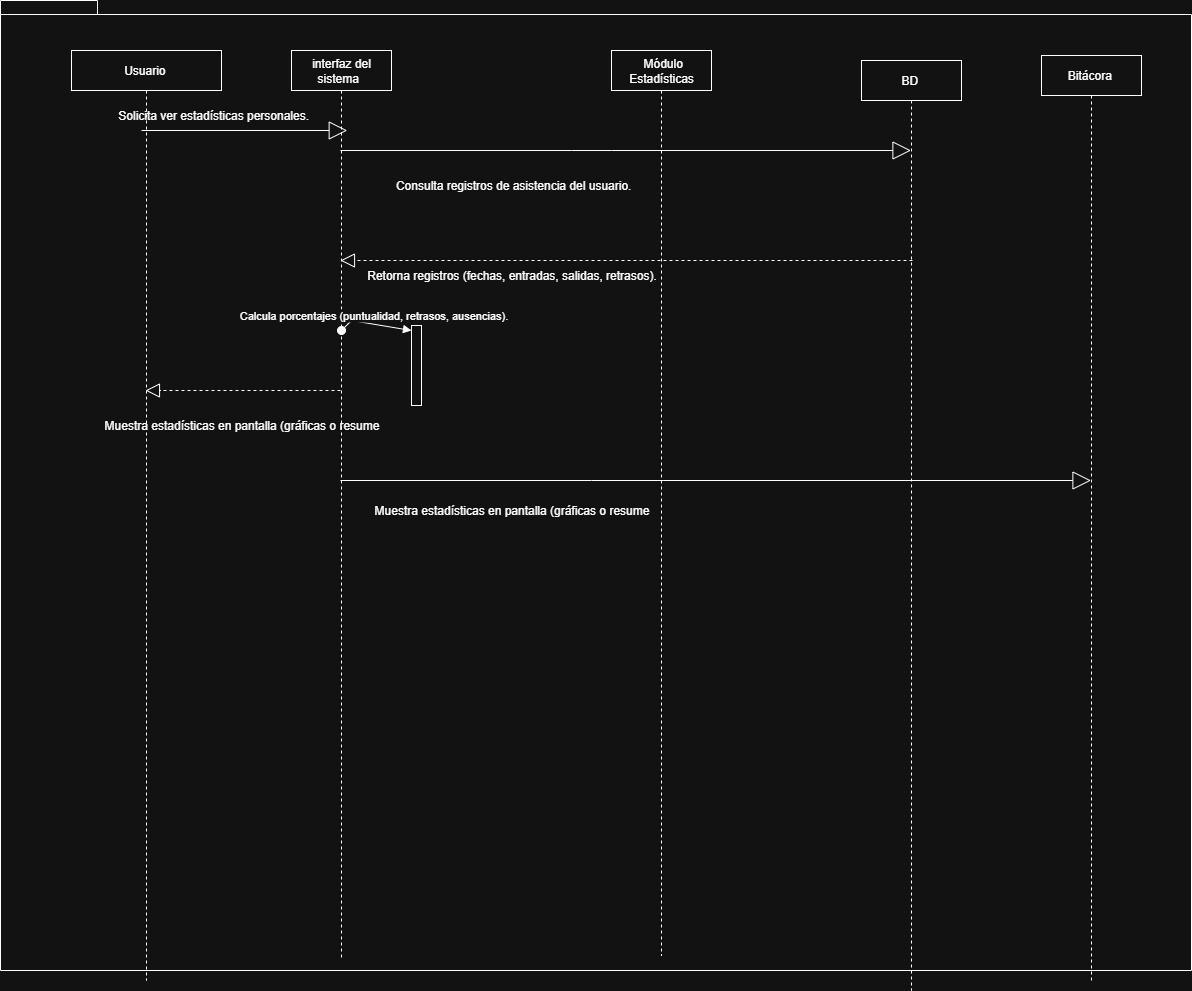
***Diagrama de secuencia 12 #***



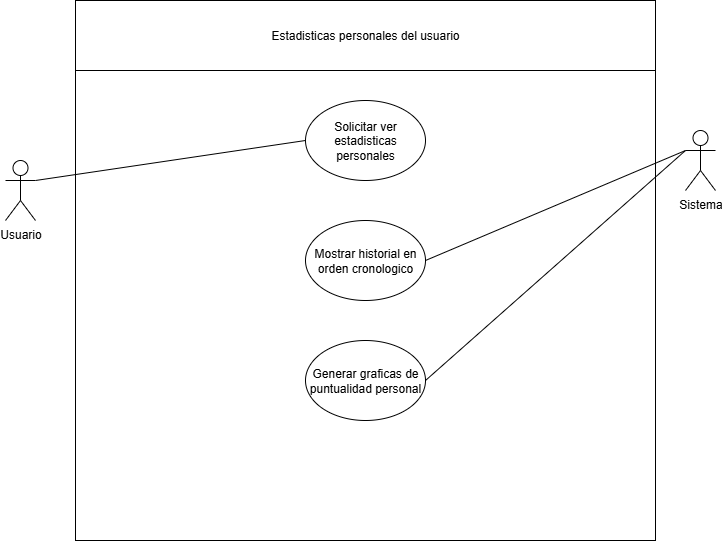
***Caso de uso 12 #***

******

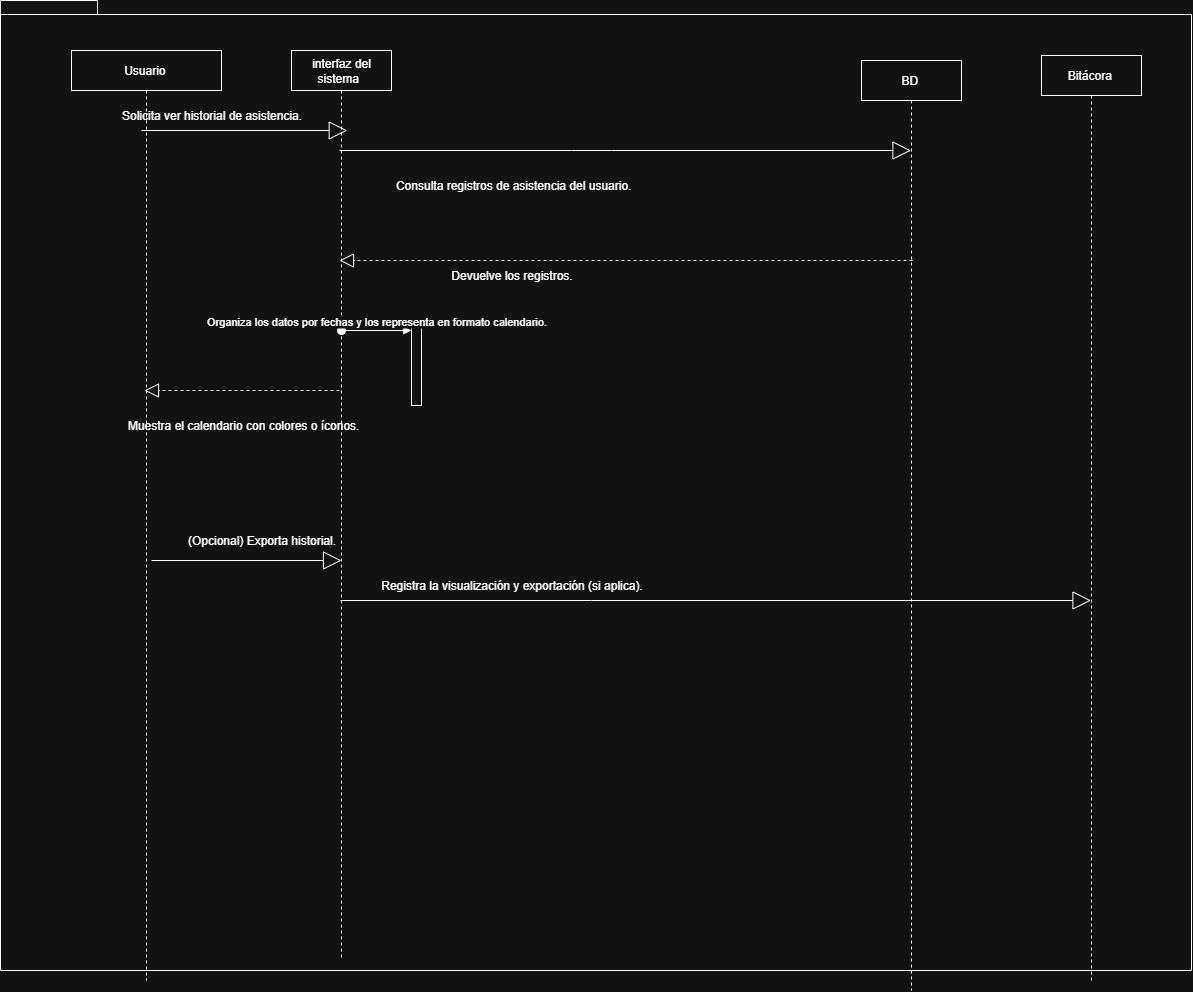
***Diagrama de secuencias 13 #***

******

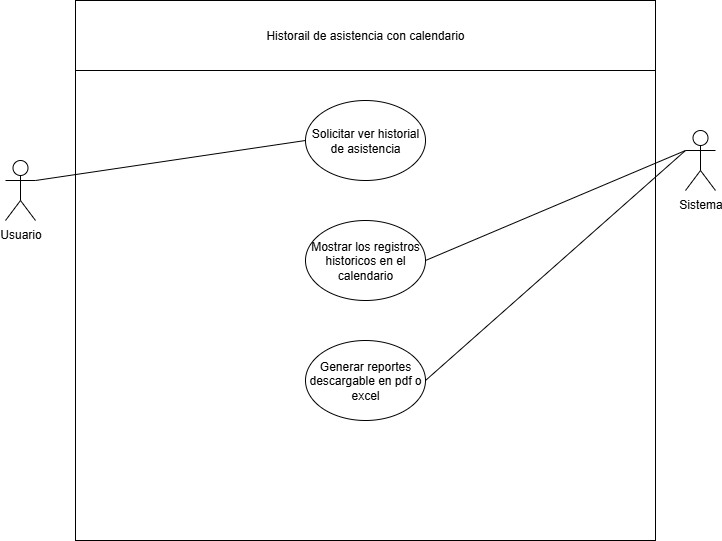
***Caso de uso 13 #***

******

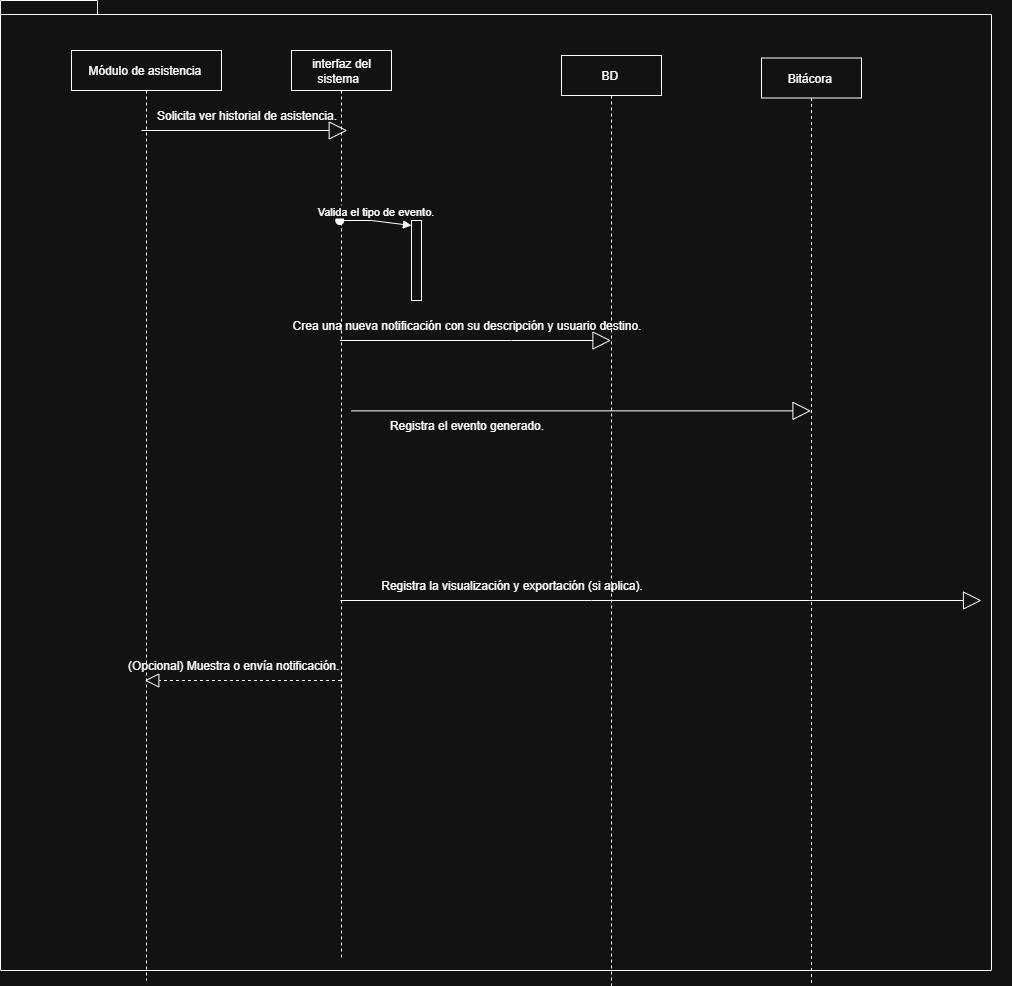
***Diagrama de secuencias 14 #***

******

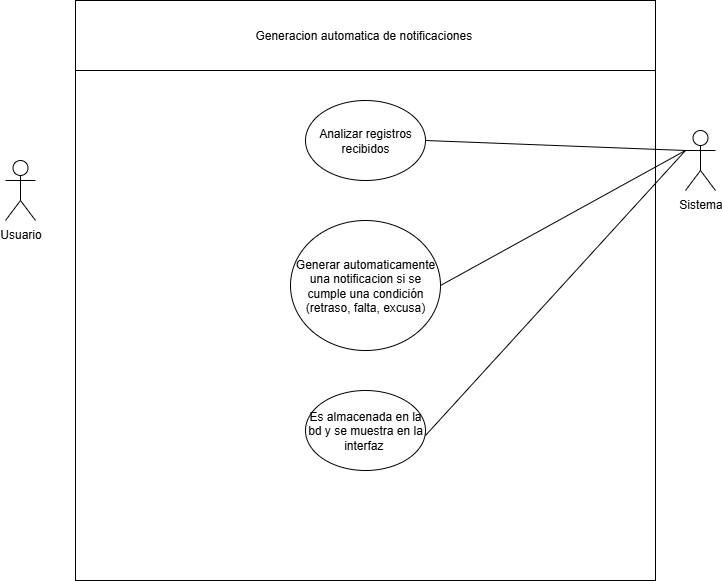
***Caso de usos 14 #***

******

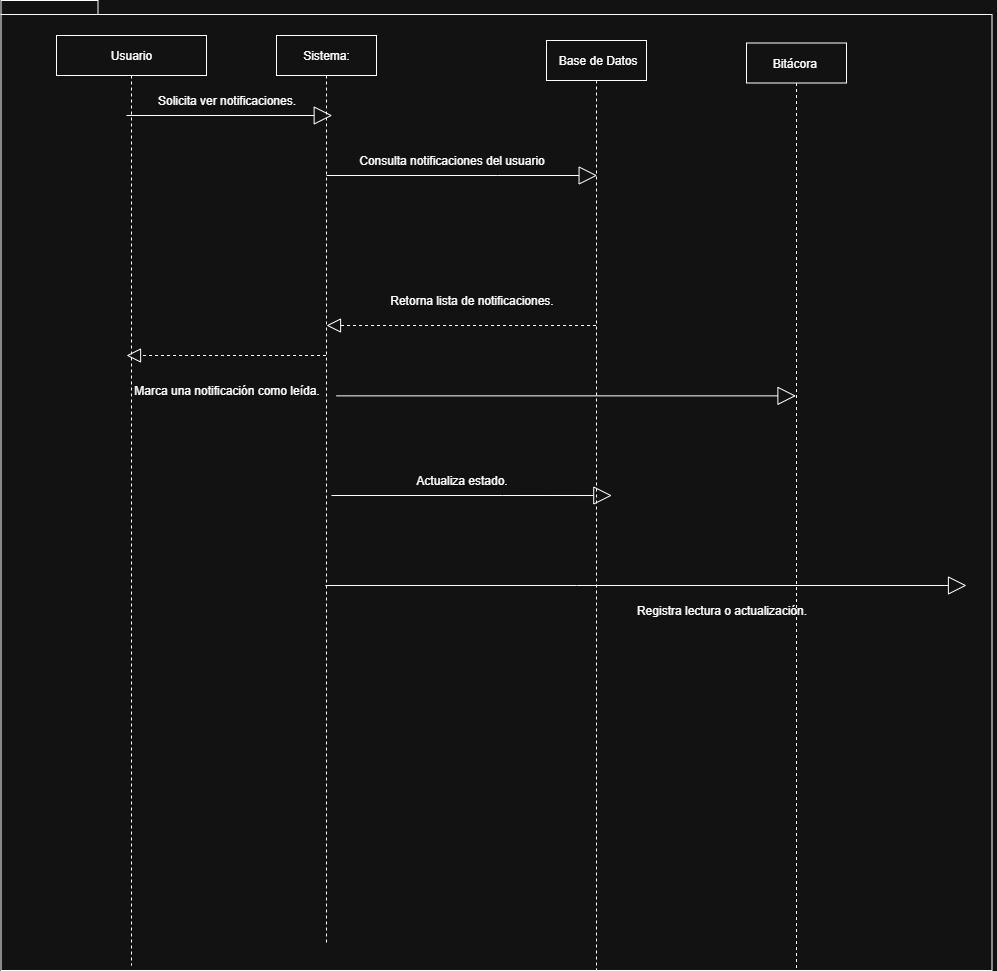
***Diagrama de secuencias 15 #***



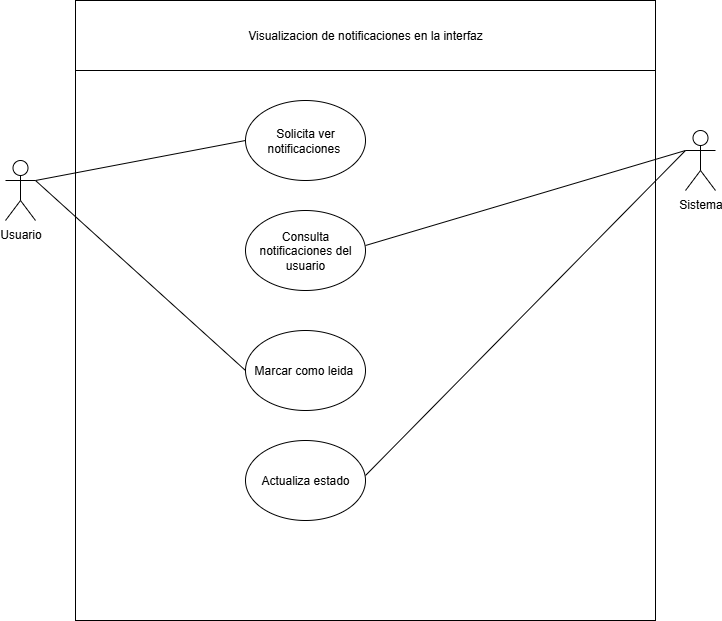
***Caso de uso 15 #***

******

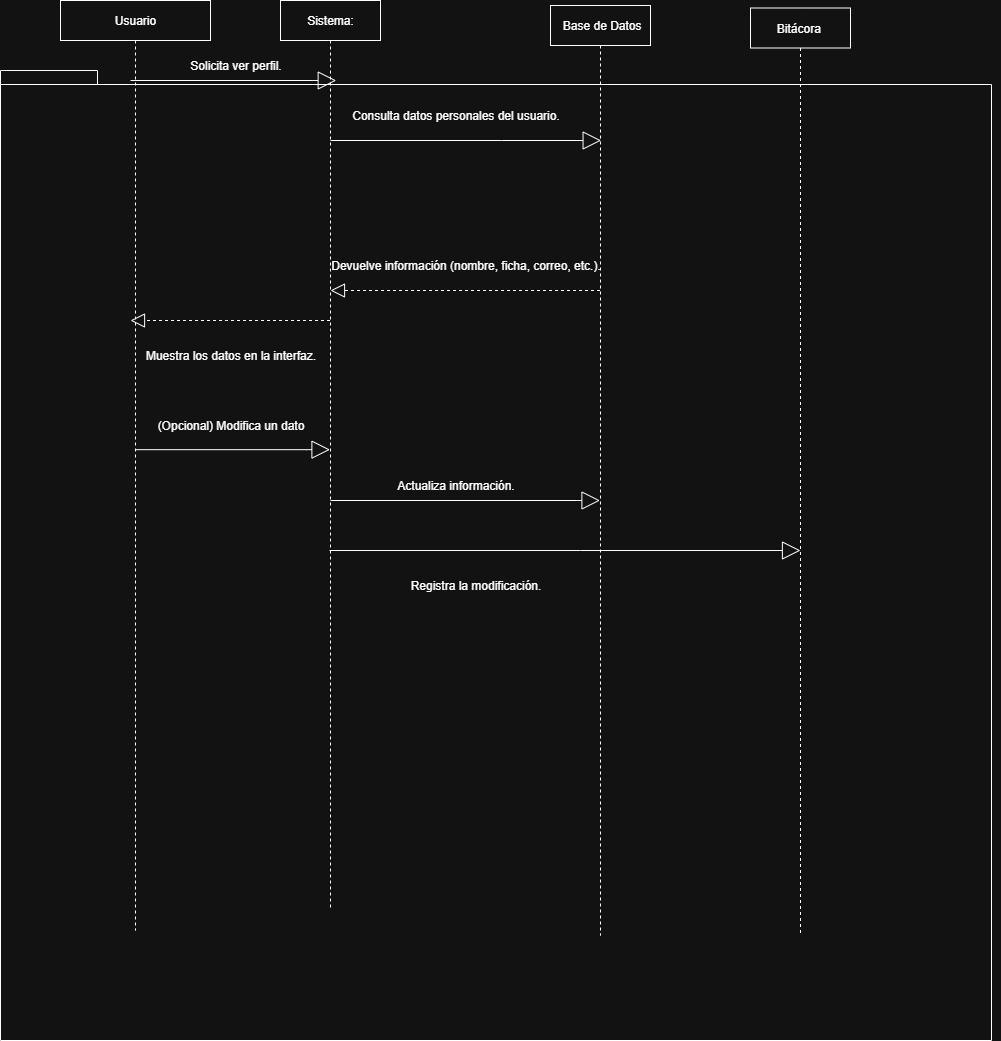
***Diagrama de secuencias 15.1 #***



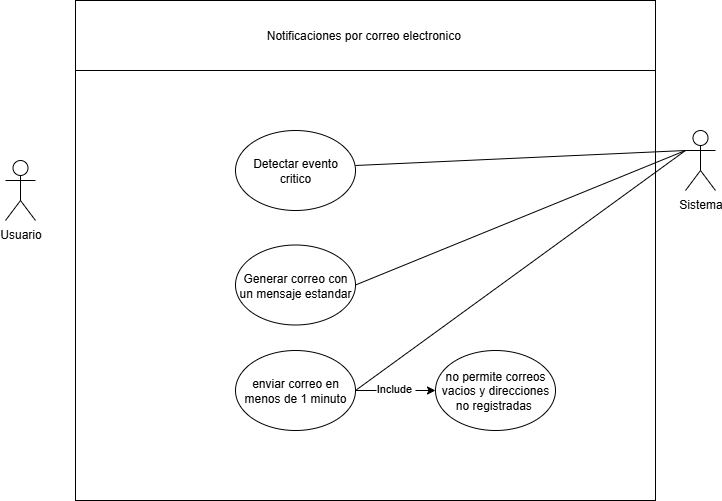
***Caso de uso 15.1 #***

******

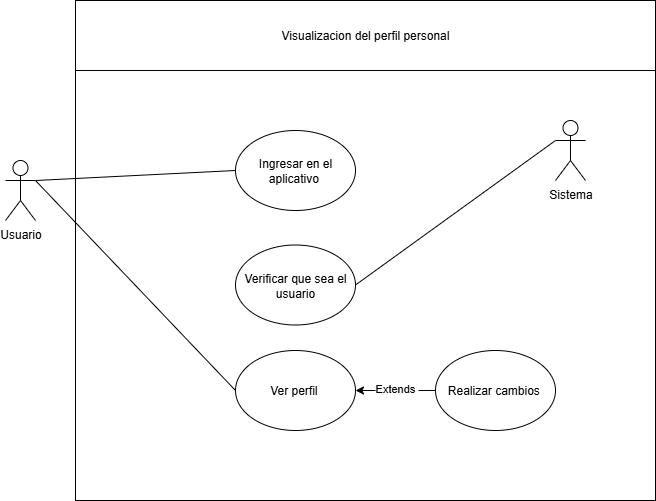
***Diagrama de secuencias 16 #***



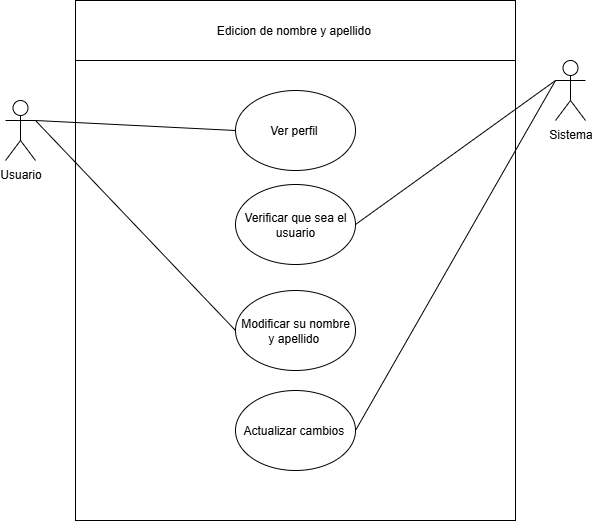
***Caso de uso 16 #***

******

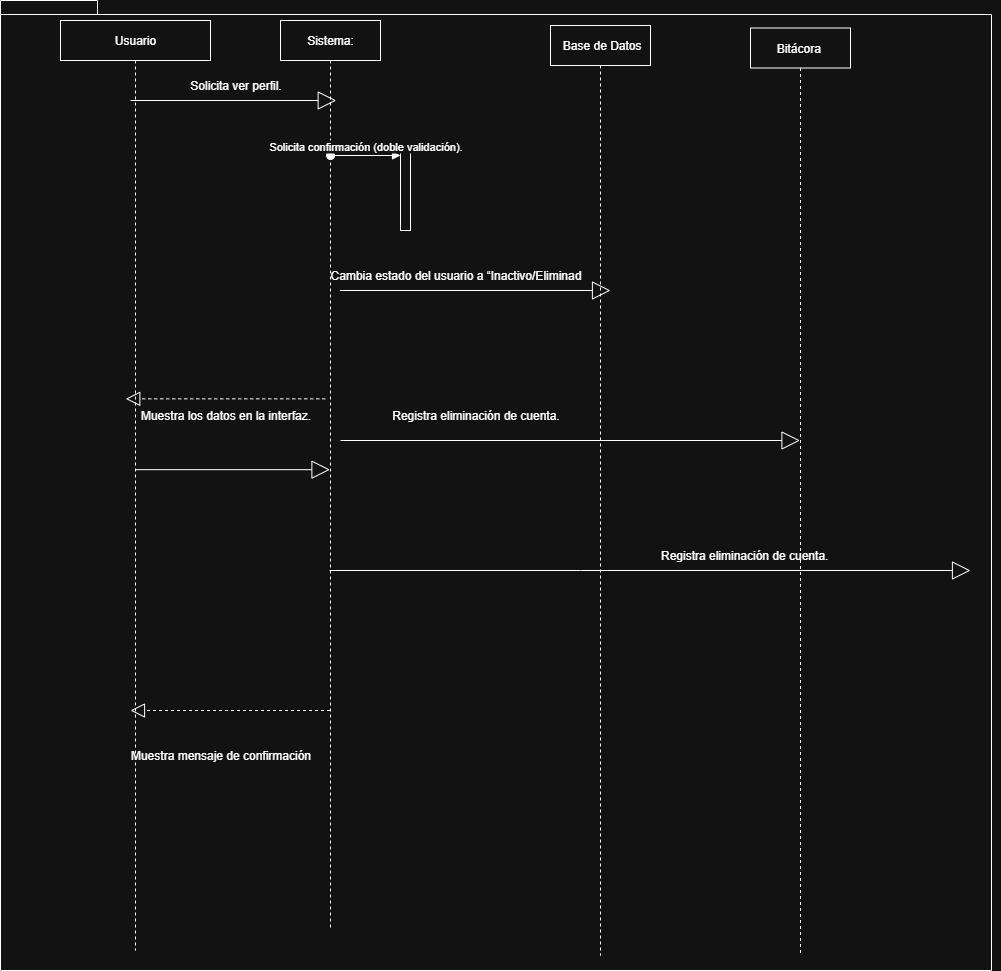
***Caso de uso 17 #***

******

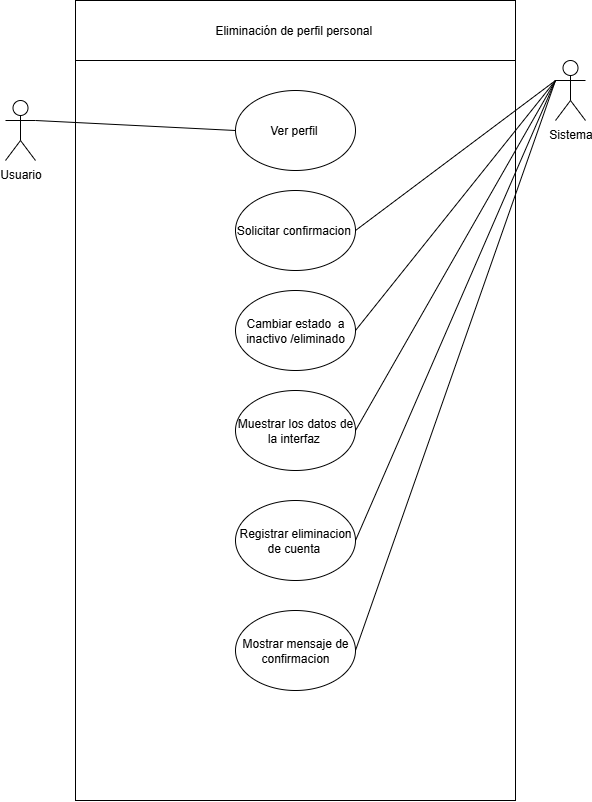
***Caso de uso 18 #***

******

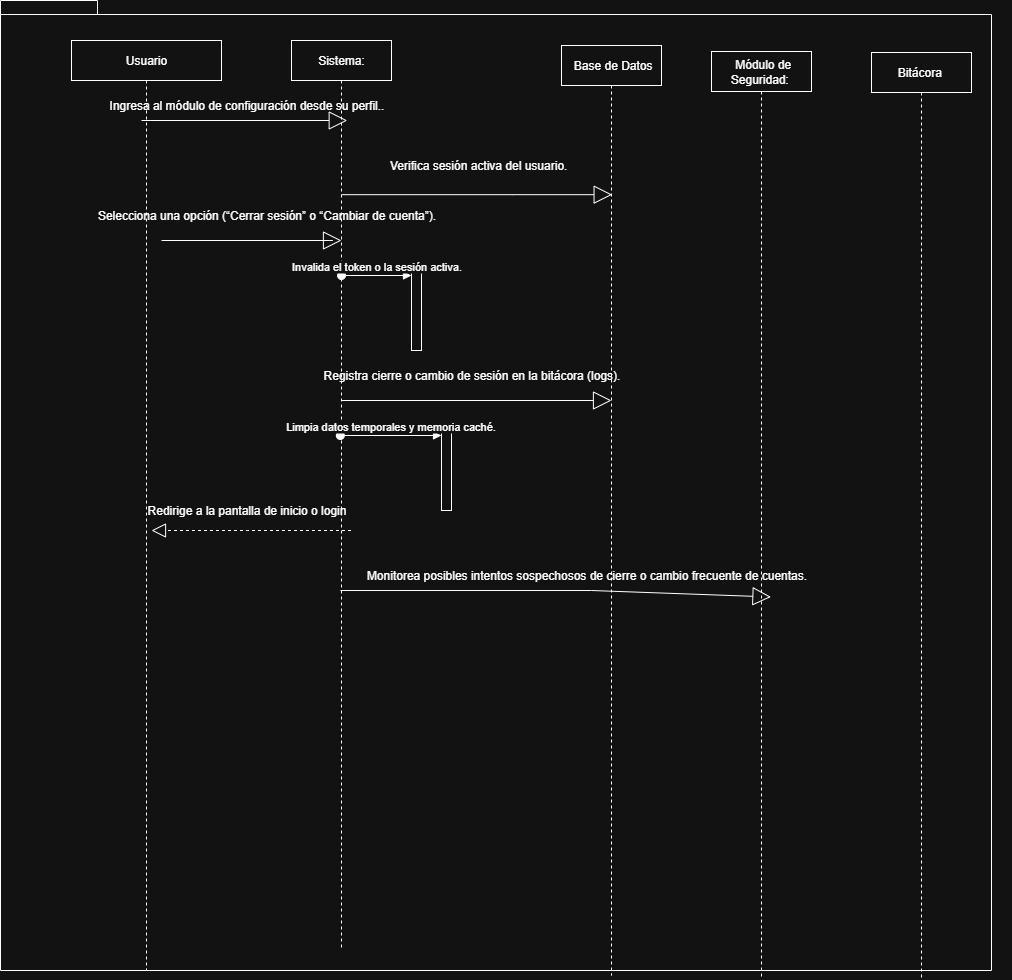
***Diagrama de secuencias 19 #***



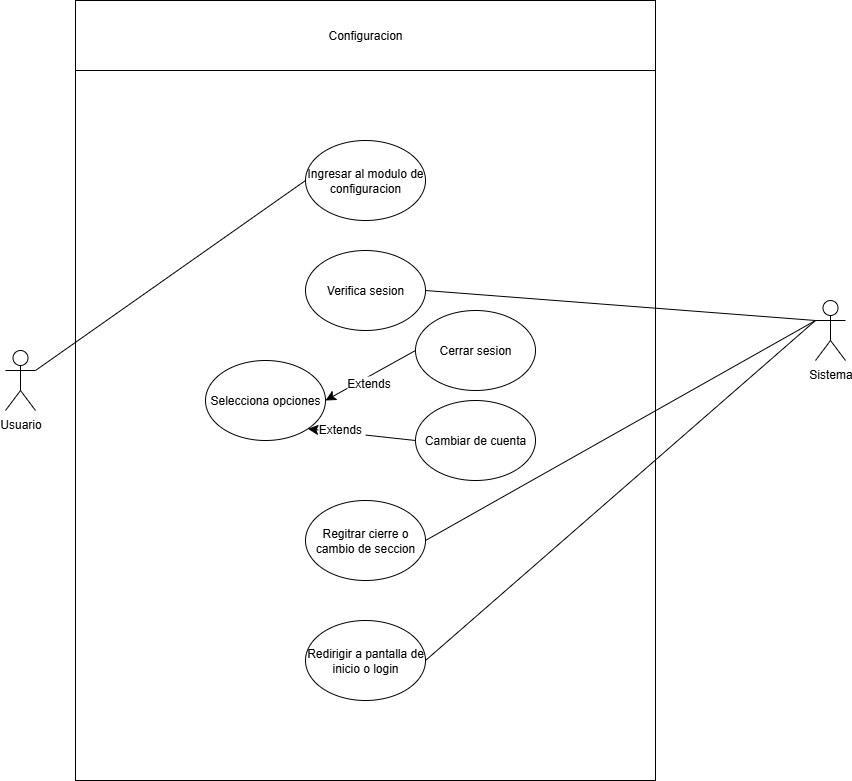
***Caso de uso 19 #***

******

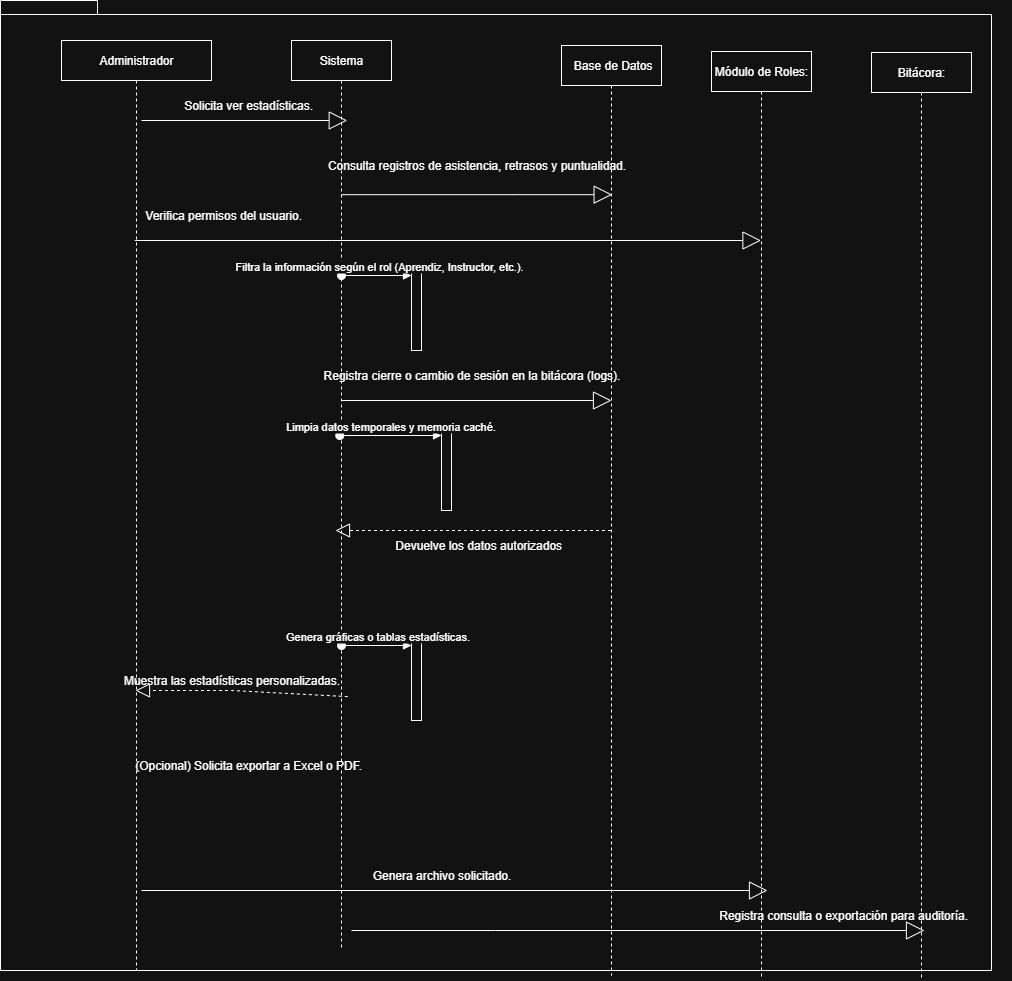
***Diagrama de secuencias 20 #***



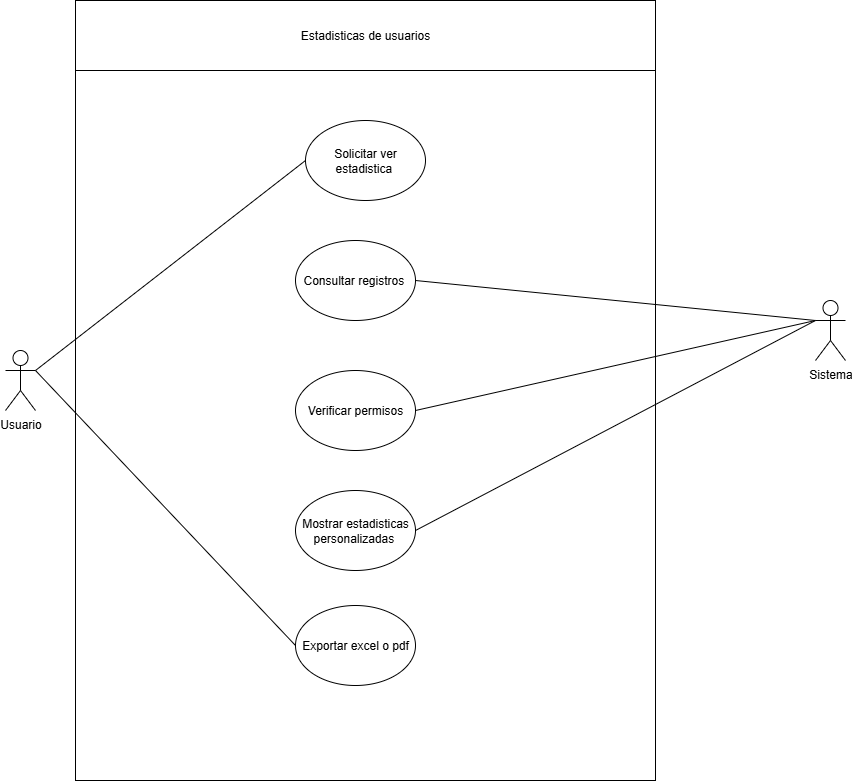
***Caso de uso 20 #***

******

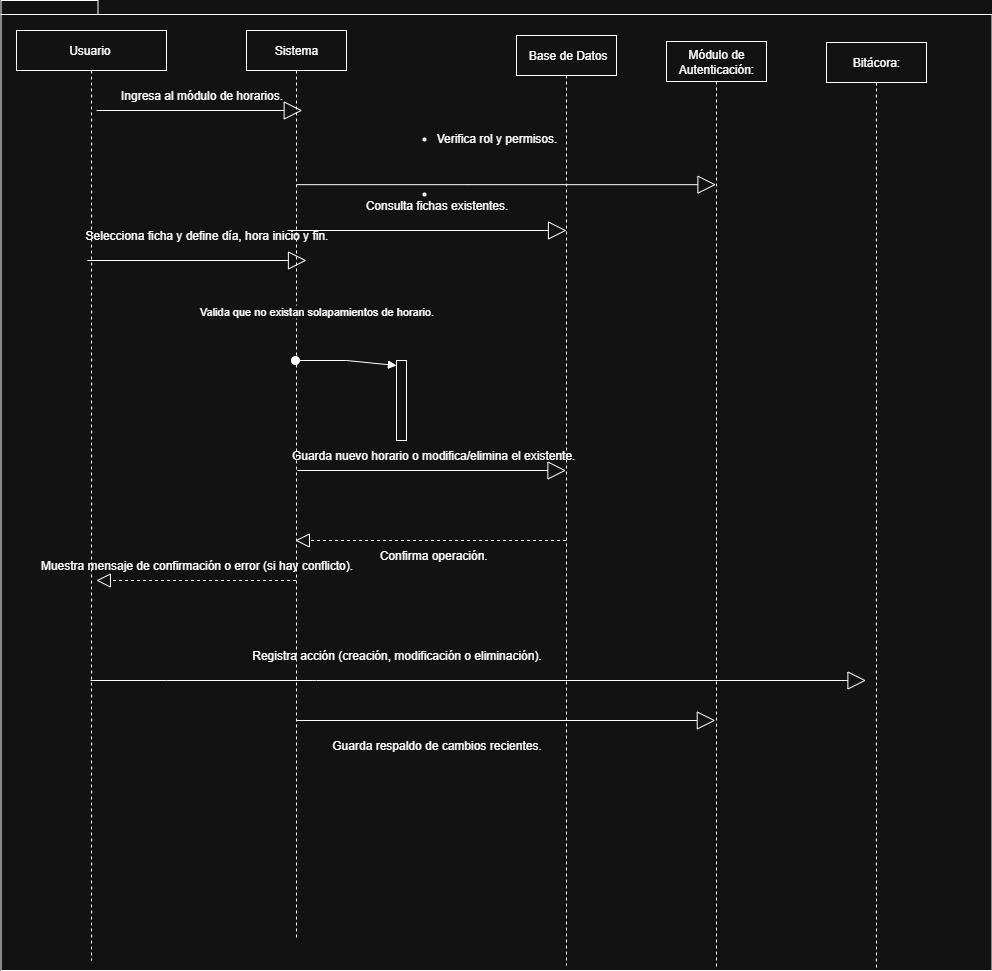
***Diagrama de secuencias 21 #***



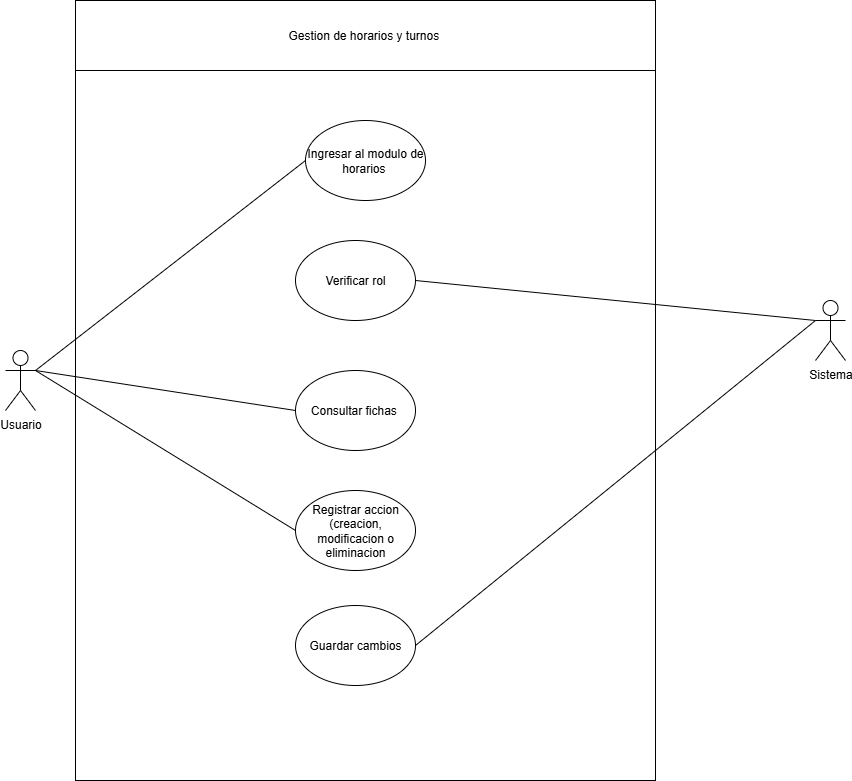
***Caso de uso 21 #***

******

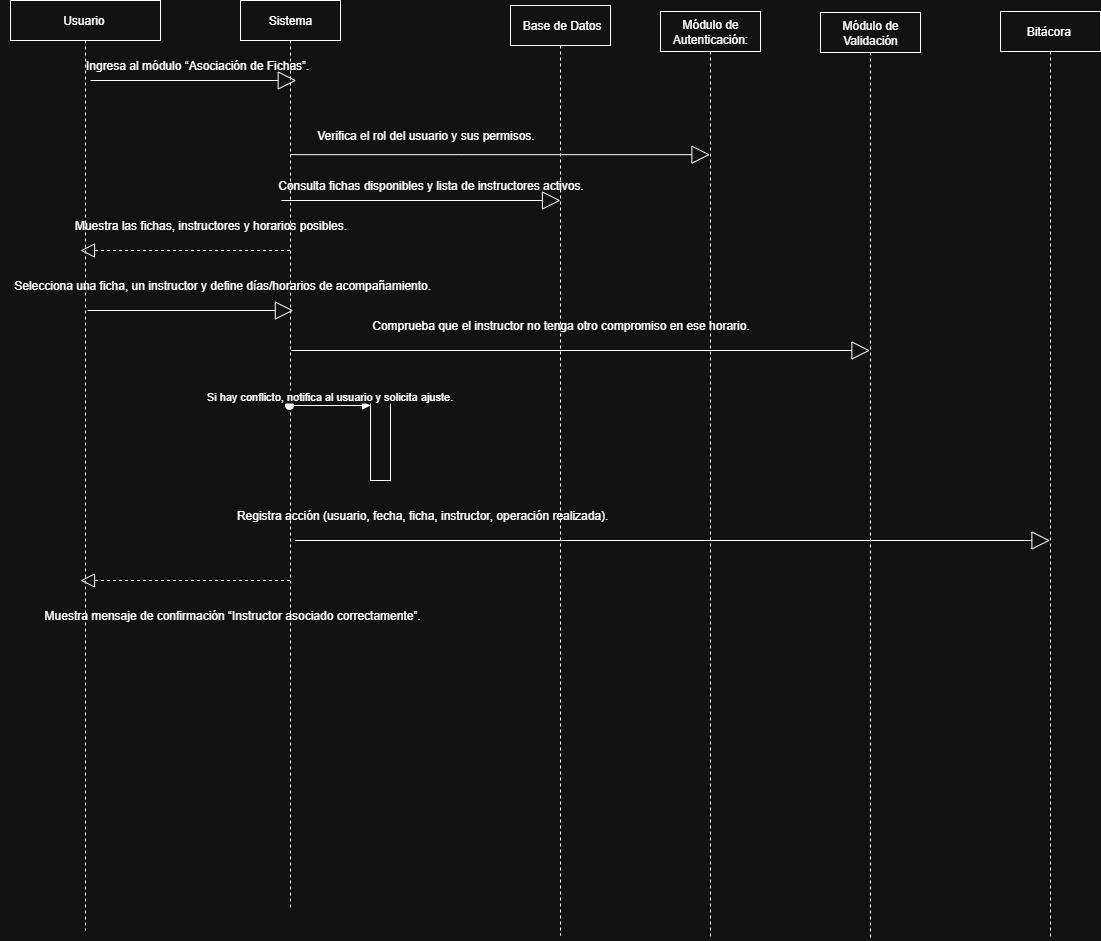
***Diagrama de secuencias 22 #***

******

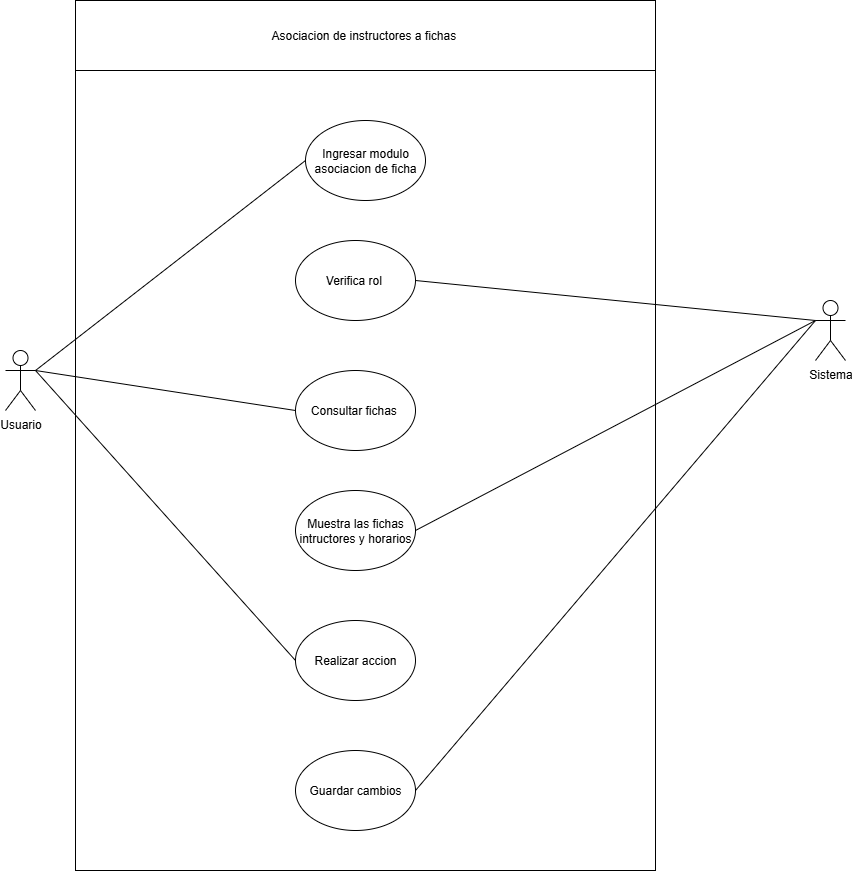
***Caso de uso 22 #***

******

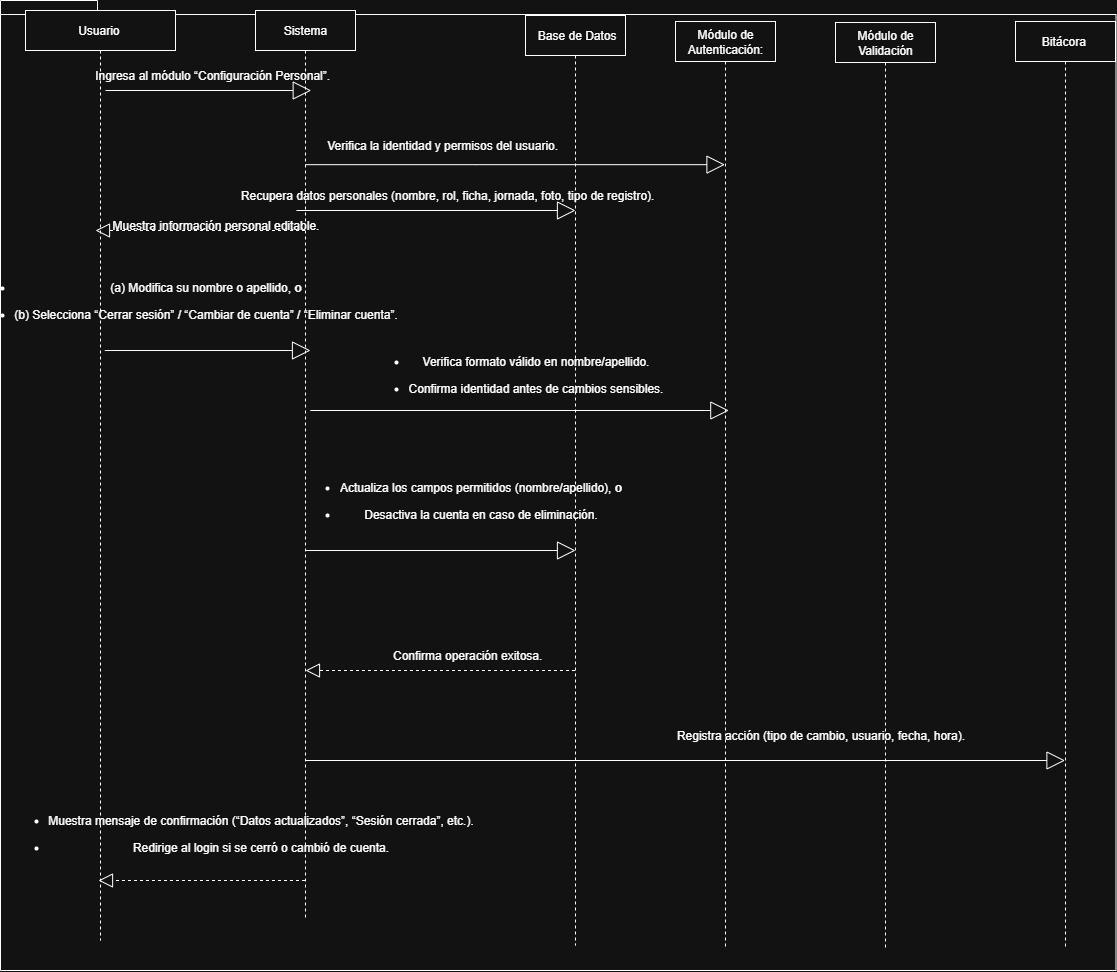
***Diagrama de secuencias 23 #***

******

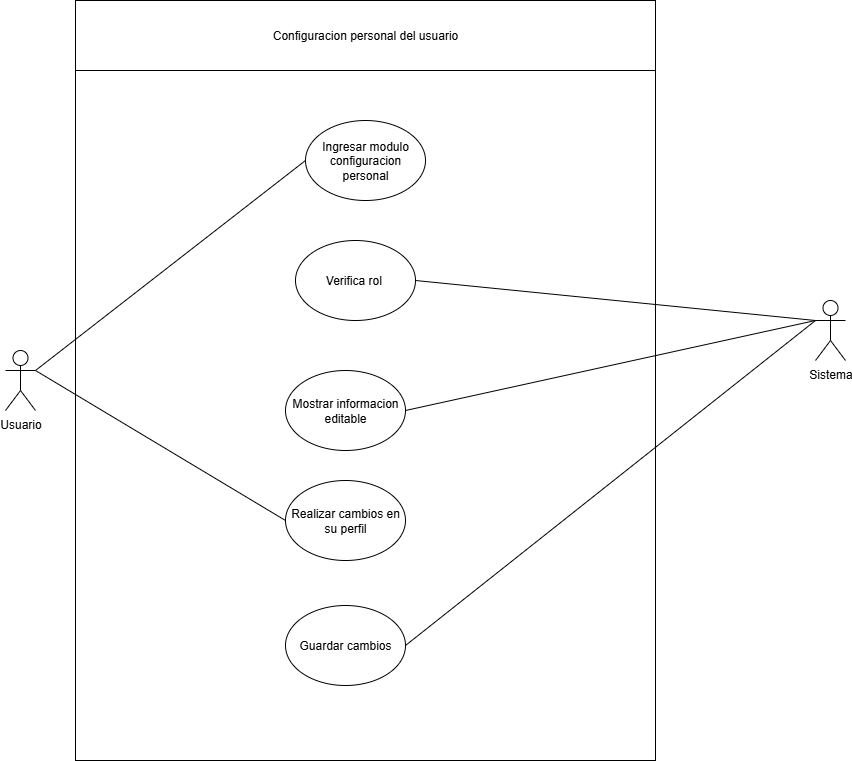
***Caso de uso 23 #***

******

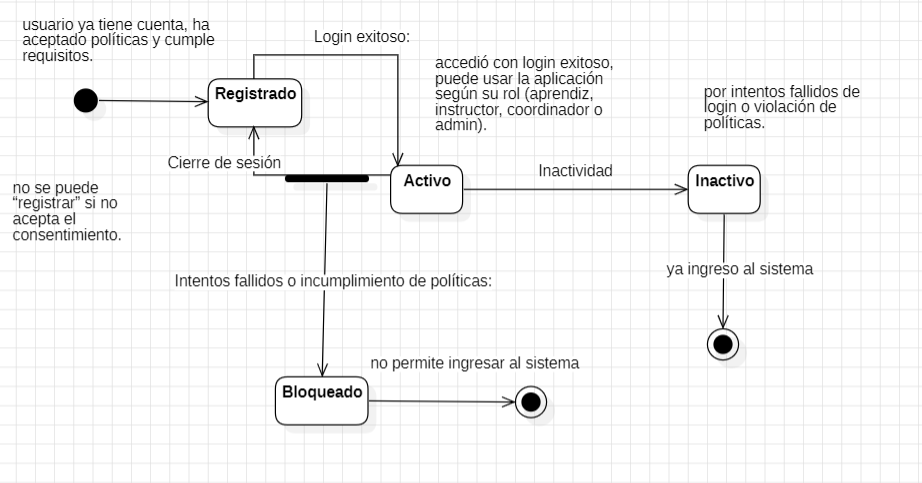
***Diagrama de secuencias 24 #***



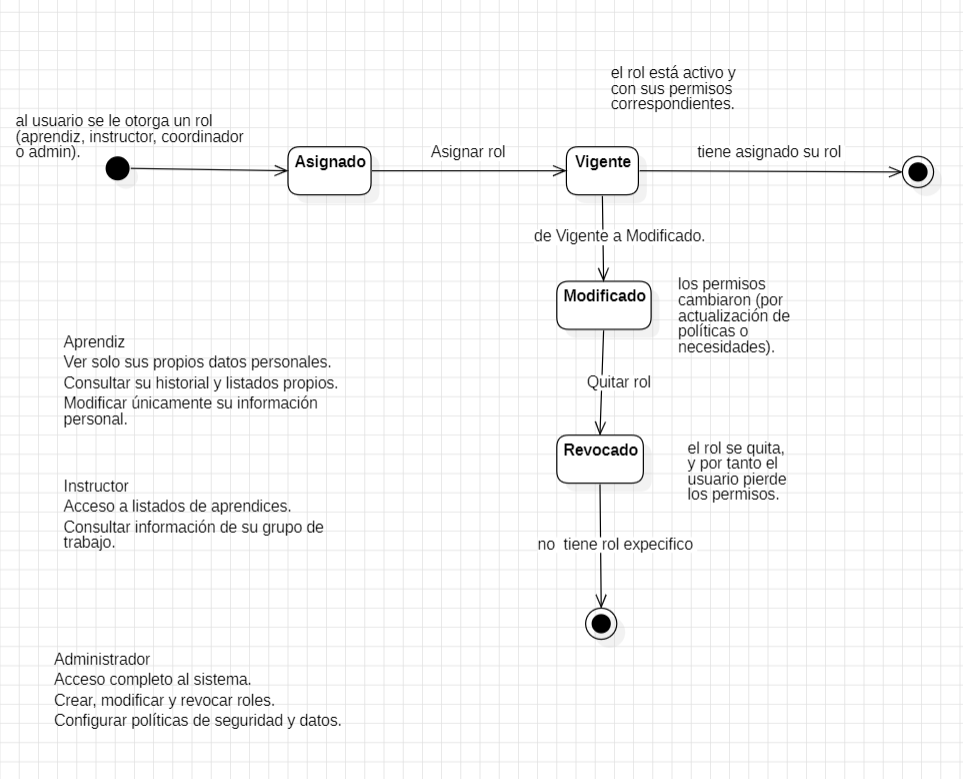
***Caso de uso 24 #***

******

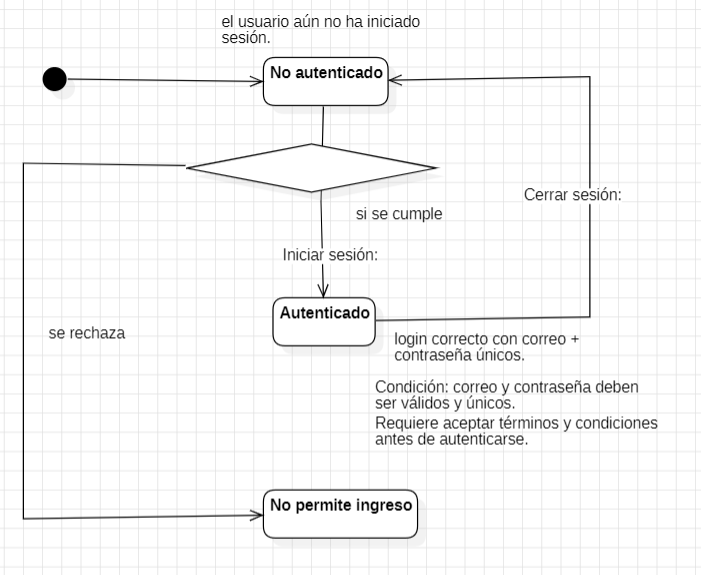
***Diagrama se transacción estados***

***1) Usuario***

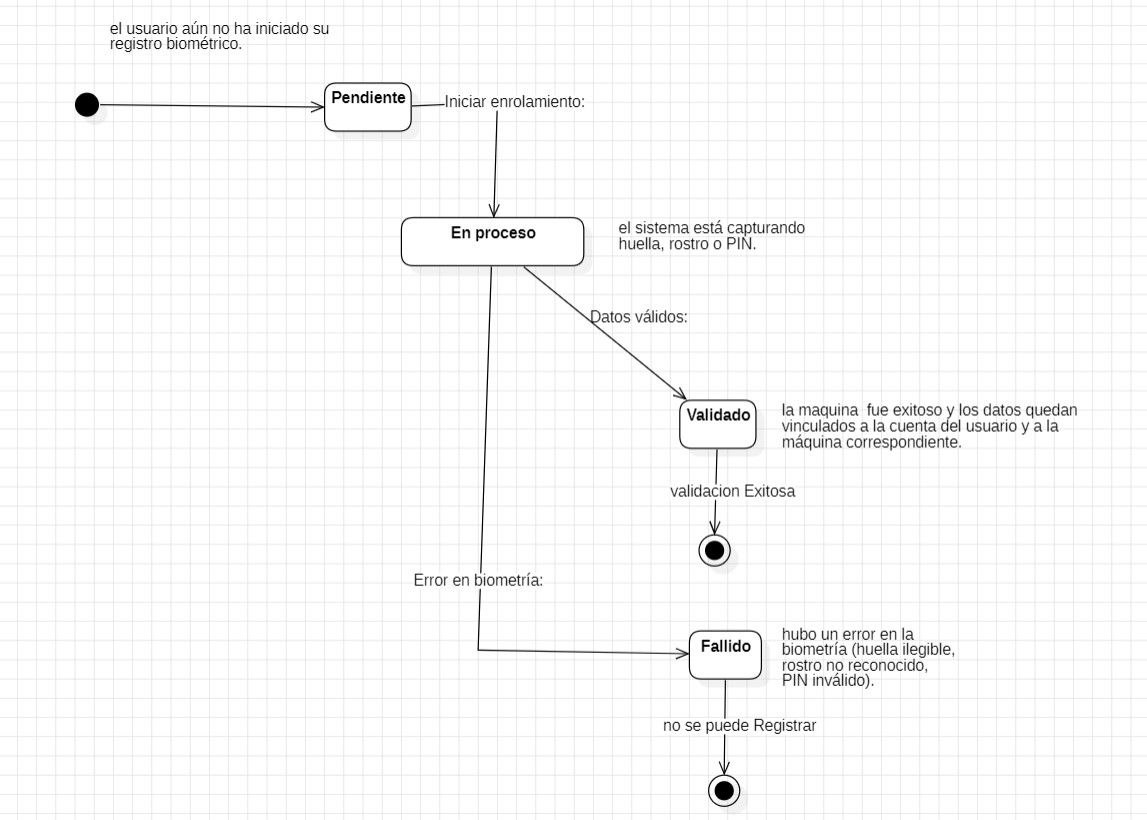
***2) Rol y permisos***



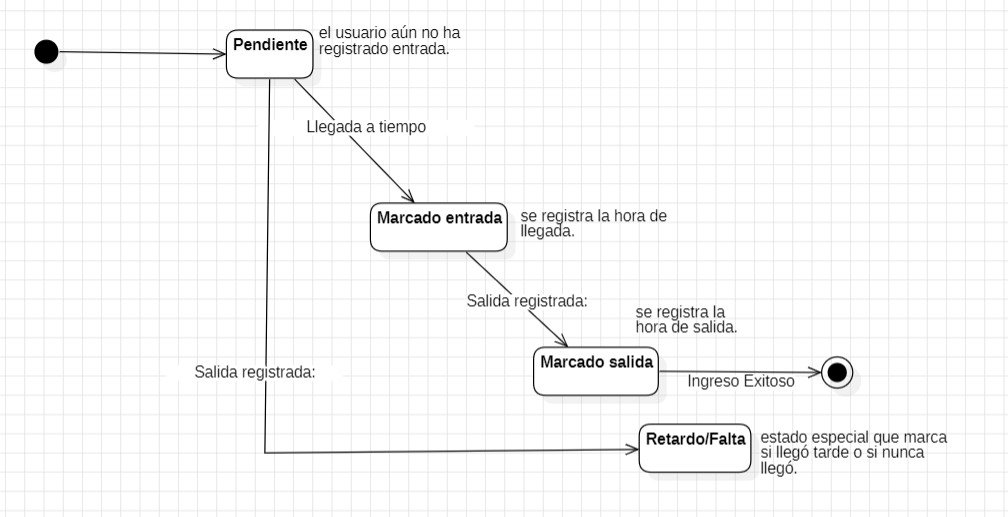
***3) Sesión del sistema***



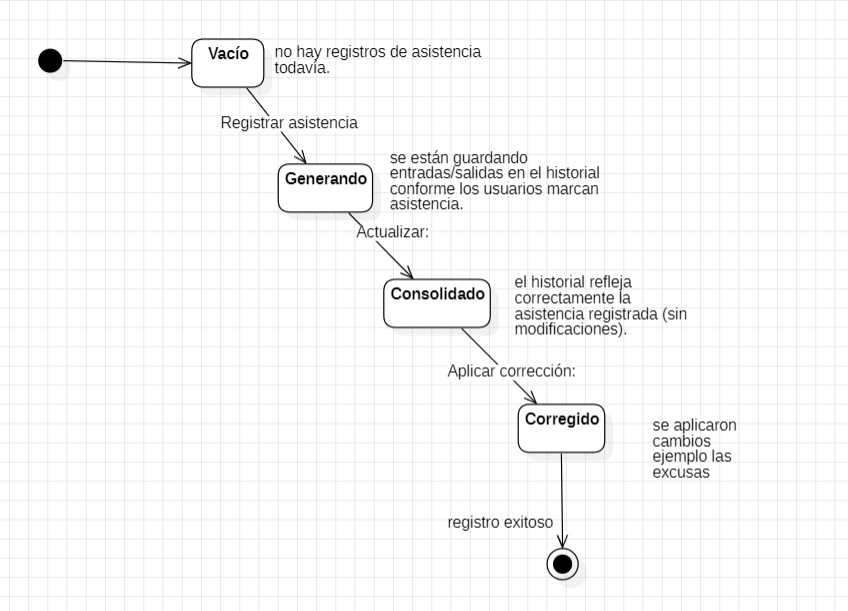
***4) biométrico***



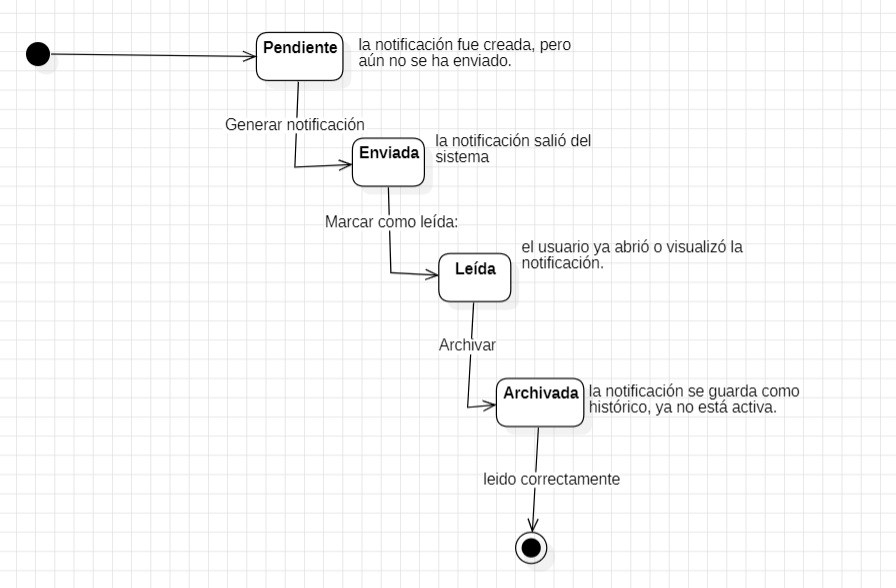
***5) Asistencia (entrada/salida)***



***6) Historial de asistencia***



***8) Notificación***



***9) Configuración***

