

Gestión Integral de Guardias y Asistencia (GIGA)

Laboratorio de Desarrollo de Software
Curso 2025



Instituto de Desarrollo
Económico e Innovación

Aguila Tayra
Alvarado Micaela
Criniti Teresa
Frers Pamela
García Cristian
Gomez Antonaz Leandro

Entrega parcial
xx/xx/xxxx

ÍNDICE

INTRODUCCIÓN	4
ESPECIFICACIÓN DE REQUERIMIENTOS	5
Introducción y ámbito del sistema	5
Definiciones, siglas y abreviaturas	6
Referencias	6
Descripción general	7
Funciones del producto	7
Características de los usuarios	8
Restricciones	9
Requisitos específicos	10
Requisitos funcionales	10
Módulo de Gestión de Usuarios	10
Módulo de Control de asistencia y novedades	10
Módulo de Gestión de guardias	11
Módulo de Generación de Reportes	11
Módulo informativo sobre el Convenio Colectivo	12
Módulo de generación de correos para notificación de novedades	12
Módulo de Seguridad y Acceso	12
Módulo Auditoría	13
Requisitos no funcionales (RNF)	13
CRONOGRAMA DE TRABAJO	14
Visión general	14
Cronograma por requerimientos	14
METODOLOGÍA DE DESARROLLO	15
Resumen de la metodología elegida	15
Adecuación de la metodología	15
HERRAMIENTAS UTILIZADAS	16
Análisis	17
Descripción de Actores	17
Diagrama de Casos de Uso	18
Casos de uso	19
Diagramas	28
Diagrama sobre Plus 20% y 40%	28
Diagrama de la gestión de asistencias	28
Diagrama de gestión del cronograma	29
Matriz de trazabilidad	30
Requerimientos Funcionales (RF) y Casos de uso (CU)	30

Casos de Uso (CU) y Actores	31
Diseño	32
Diagrama Entidad-Relación	32
Diagrama de Clases	32
Diseño de pantallas	34
SOBRE LAS ITERACIONES	38
ITERACIÓN 1	38
ITERACIÓN 2	39
SOBRE LOS ENTREGABLES	1
Aplicaciones y plataformas que forman al sistema	1
Requerimientos técnicos para la instalación	1
PRESENTACIÓN VISUAL PARA APROBAR FINAL	1

INTRODUCCIÓN

En la actualidad, la carga y control de horas guardias del personal que pertenece a la Secretaría de Protección Civil se realiza de manera manual por los usuarios administrativos. Este procedimiento presenta diversas dificultades que afectan la eficacia, precisión y transparencia del proceso, entre lo que se destaca:

- Errores humanos al registrar horas guardias, por ejemplo agentes que se encuentran usufructuando licencias (enfermedad personal, enfermedad familiar, franco compensatorio, entre otros).
- Cálculos incorrectos del total de horas trabajadas por agente o por dirección.
- Dependencia de una herramienta interna desarrollada en Excel con VBA, que si bien agiliza el cálculo, presenta importantes limitaciones:
 - Instalación manual en cada equipo donde se utilice.
 - Ausencia de sincronización en tiempo real entre distintas computadoras de una misma dirección.
 - Compatibilidad condicionada por la arquitectura del sistema (x86 o x64).
 - Dificultad de uso para usuarios sin conocimientos de Excel avanzado.
 - Falta de acceso individual por parte de cada agente para consultar su asistencia y horas guardias.

Asimismo, el Convenio Colectivo de Trabajo aprobado el 18/11/2022 mediante la Resolución n° 425 del Ministerio de Trabajo y Empleo incorpora nuevos incisos para la justificación de inasistencias. No obstante, gran parte del personal desconoce estas disposiciones, lo que genera confusión y errores en la gestión administrativa.

En este proyecto se propone el desarrollo de un sistema moderno y centralizado que reemplace las planillas manuales y las herramientas aisladas, permitiendo mejorar la eficiencia administrativa, reducir errores y garantizar la transparencia en el cálculo de horas guardias, guardias y asistencia.

ESPECIFICACIÓN DE REQUERIMIENTOS

Introducción y ámbito del sistema

El sistema propuesto, denominado *Gestión Integral de Guardias y Asistencia* (GIGA), surge como respuesta a las dificultades actuales en la gestión de asistencia, guardias, y horas guardias del personal de la Secretaría de Protección Civil.

El objetivo principal del sistema es reemplazar este procedimiento manual por una plataforma web moderna, segura y escalable, que permita centralizar la información, garantizar transparencia en los cálculos y brindar acceso a todos los actores involucrados en tiempo real.

El ámbito de aplicación abarca a todo el personal operativo y administrativo de la Secretaría de Protección Civil, incluyendo Agentes, Agentes avanzados, Jefaturas, Directores y Administradores.

Asimismo, el sistema será multiplataforma, accesible desde computadoras, tablets y teléfonos móviles con conexión a internet, favoreciendo la sincronización de datos en tiempo real y la reducción de la carga administrativa.

Definiciones, siglas y abreviaturas

GIGA: Gestión Integral de Guardias y Asistencia.

Convenio Colectivo: Convenio Colectivo aprobado por Res. 425/22 del 18/11/2022, donde se regula licencias y ausencias (actualmente vigente)

Planilla: Documento que resume asistencia, tareas y horas trabajadas.

VBA: Visual Basic for Applications, lenguaje de macros utilizado en Excel.

Multiplataforma: Capacidad de funcionar en distintos dispositivos y sistemas operativos.

Gestión: En el presente documento siempre que se hable de requerimientos, cada vez que se haga referencia a la gestión de datos se entenderá en el marco de las operaciones CRUD (Create, Read, Update, Delete), es decir, la creación, consulta, actualización y eliminación de la información correspondiente. Además la gestión será completa si el usuario tiene permisos para cada operación.

HTTPS: Hypertext Transfer Protocol Secure es una versión segura de HTTP que cifra las comunicaciones entre un navegador web y un sitio web para proteger los datos del usuario.

Hash: Un hash es una secuencia única de letras y números generada por un algoritmo matemático a partir de cualquier dato o documento, sin importar su tamaño.

Auditoría: Registro de modificación de datos.

Corpus Cerrado: En nuestro contexto hace referencia a que la IA solo va a tener acceso y va a basar sus respuestas **únicamente** en el convenio colectivo de trabajo cargado.

Referencias

Resolución N.º 425/22 del Ministerio de Trabajo y Empleo (18/11/2022).

Guía de estilo Springer Engineering para referencias bibliográficas.

Manual de buenas prácticas en desarrollo web ágil – Blog de Atlassian.

Documentación oficial de Django: <https://docs.djangoproject.com>

Artículo técnico sobre sistemas de gestión de RRHH: IEEE Xplore, 2021.

Descripción general

Funciones del producto

Se propone el desarrollo de un sistema web moderno, seguro y escalable que centralice la gestión de guardias, horarios, asistencia y recursos humanos, superando las limitaciones de los métodos actuales.

El sistema contempla los siguientes módulos y funcionalidades principales:

- Gestión de Usuarios
 - Alta, baja, modificación y consulta de usuario.
 - Administración de datos personales, historial de asistencia y guardias.
 - Asignación de roles y permisos en función de las estructuras organizacionales actuales.
- Control de asistencia y novedades
 - Registro diario de asistencia.
 - Registro de licencias, ausencias justificadas y permisos especiales.
- Gestión de guardias
 - Generación del cronograma de guardias del mes.
 - Aprobación del cronograma.
 - Cálculo automático de horas de guardias, considerando normativa vigente.
- Generación de reportes
 - Individuales: resumen mensual por agente (asistencia, horas trabajadas y guardias), con posibilidad de consultas por períodos específicos.
 - Por área: listados de personal con detalle y tipo de guardia y posibilidad de consultas por períodos específicos.
- Módulo informativo sobre el Convenio Colectivo
 - Acceso simple y claro al Convenio Colectivo de Trabajo.
- Generación de correos para notificación de novedades.

El sistema funcionará con roles y permisos de usuarios, los cuales serán asignados en función de los roles de cada usuario y las responsabilidades que le competen a cada uno.

Características de los usuarios

El sistema Gestión Integral de Guardias y Asistencia (GIGA) está diseñado para ser utilizado por diferentes usuarios dentro de la Secretaría de Protección Civil. Cada usuario responde a un rol y permisos que conllevan diferentes grados de responsabilidad, por consiguiente las funcionalidades y el nivel técnico requerido también varían.

Los perfiles de usuario en el sistema se estructuran de forma jerárquica e incremental respetando las estructuras organizacionales. En ese sentido, el **Agente** constituye el nivel más básico de acceso, limitado a la consulta de su propia información. A partir de allí, cada rol superior incorpora las capacidades del anterior.

- Agentes
 - Acceso a consulta de su información personal: asistencia registrada, guardias asignadas y horas guardias calculadas.
 - Pueden notificar errores o solicitar aclaraciones mediante el módulo de notificación.
- Agente avanzado
 - Carga de asistencia y novedades de los agentes del área (parte diario).
- Jefaturas
 - Cuentan con acceso a funciones de gestión de guardias y registro de licencias y ausencias.
 - Generan reportes individuales o por área, y supervisan la información de los agentes bajo su responsabilidad.
- Directores
 - Aprobación del cronograma de guardias.
 - Aprobación de las guardias realizadas en el mes.
- Administradores
 - Tienen acceso completo al sistema, incluyendo la administración de usuarios, la definición de roles, la supervisión integral de guardias y la generación de reportes globales.
 - Se encargan de mantener actualizada la estructura organizacional (direcciones, jefaturas y agentes).

En resumen, el sistema debe adaptarse a un público con experiencia básica tecnológica, ofreciendo interfaces simples e intuitivas para quienes ejercen tareas de gestión y administración.

Restricciones

El sistema Gestión Integral de Guardias y Asistencia (GIGA) debe contemplar una serie de restricciones que delimitan su desarrollo y operación, garantizando cumplimiento normativo, seguridad y accesibilidad.

1. Seguridad en el acceso

- El sistema debe implementar mecanismos de autenticación segura y cifrado de datos (ej. HTTPS, hash de contraseñas) para proteger la información sensible de los usuarios.
- Además, cada usuario sólo podrá acceder a las funciones que le permitan sus permisos, garantizando que las acciones sensibles estén restringidas al rol correspondiente.

2. Accesibilidad multiplataforma

- El sistema debe ser accesible desde dispositivos con conexión a internet (computadoras, tablets y smartphones) mediante navegadores web modernos, versiones superiores a Chrome 72+, Firefox 65+, Safari 12.1+ (macOS) / 12.2+ (iOS), Edge 79+ (Chromium) y Samsung Internet 9.2+.

3. Usabilidad para todo el personal

- La interfaz debe ser intuitiva y de fácil uso.

4. Integridad y trazabilidad de la información

- Toda creación, modificación o eliminación de registros de asistencia, y guardias (horas y días) deberá quedar registrada en el sistema, incluyendo usuario responsable, fecha y hora y operación realizada para garantizar transparencia y trazabilidad.

Requisitos específicos

Requisitos funcionales

Módulo de Gestión de Usuarios

RF01 – Gestión de agentes

- Usuario: Administrador.
- Descripción: El sistema debe permitir el alta, baja y modificación de agentes, registrando datos personales, legajo, puesto y asignación de áreas.

Módulo de Control de asistencia y novedades

RF02 – Registro de asistencia diaria

- Usuario: Agente
- Descripción: El sistema debe permitir la carga de marcas de ingreso y egreso. El sistema valida horarios y ventanas de tolerancia antes de aceptar la marca.

RF03 – Control de asistencia diaria

- Usuario: Agente Avanzado.
- Descripción: Puede visualizar y corregir las marcas de ingreso y egreso de su equipo inmediato, especialmente en situaciones de contingencia. El sistema debe validar que los registros respeten los horarios establecidos para cada agente.

RF04 – Gestión de licencias y novedades

- Usuario: Agente Avanzado.
- Descripción: Puede cargar licencias y novedades de los agentes junto con la documentación respaldatoria correspondiente.

Módulo de Gestión de guardias

RF05 - Generación del cronograma de guardias

- Usuario: Jefatura.
- Descripción: Puede generar el cronograma mensual de asignación de guardias a los agentes del área. En el caso de rechazo por parte del Director, deberá modificar el cronograma hasta conseguir la aprobación.

RF06 - Aprobación del cronograma

- Usuario: Director.
- Descripción: Puede aprobar o rechazar el cronograma de guardias.

RF07 – Cálculo automático de horas de guardias

- Usuario: Sistema
- Descripción: El sistema debe calcular de forma automática las horas de guardias, asignando el plus correspondiente (ver diagrama en sección Diseño).
 - Plus del 40%: Se otorga a todos los agentes pertenecientes al área operativa que hayan realizado al menos 8 horas guardias en el período y a aquellos agentes administrativos que hayan realizado 32 horas o más.
 - Plus del 20%: Se otorga a los agentes del área operativa que hayan realizado menos de 8 horas guardias y a los agentes de otras áreas que hayan realizado de 0 a 31 horas guardias.

Módulo de Generación de Reportes

RF08 – Generación de reportes

- Usuario: Director.
- Descripción: Puede generar reportes por rangos de fechas, área, tipo de guardia o por agente en formato PDF o Excel.

Módulo informativo sobre el Convenio Colectivo

RF09 - Consultar Convenio con IA

- Usuario: Agente.
- Descripción: El sistema permitirá realizar consultas en lenguaje natural sobre el Convenio Colectivo de Trabajo usando un componente de IA con corpus cerrado al documento oficial cargado en el sistema. La IA no podrá consultar internet ni otras fuentes. Las respuestas serán cortas y concretas.

Módulo de generación de correos para notificación de novedades

RF10 – Notificaciones automáticas

- Usuario: Sistema
- Descripción: El sistema generará una notificación automática por correo electrónico para notificar errores y consultas.

RF11 – Notificaciones

- Usuario: Agente
- Descripción: Puede generar una notificación por correo electrónico desde el sistema para la corrección de datos (personales o de guardias).

Módulo de Seguridad y Acceso

RF12 – Autenticación y roles de usuario

- Usuario: Todos
- Descripción: El usuario accede mediante usuario y contraseña a las funciones que le han sido otorgadas.

RF13 – Gestión de contraseñas

- Usuario: Todos
- Descripción: Los usuarios pueden modificar su contraseña o recuperarla, la cual será enviada a su correo institucional.

Módulo Auditoría

RF14 – Registro de auditoría

- Usuario: Sistema
- Descripción: El sistema registra toda creación, modificación o eliminación de registros de asistencia, y guardias (horas y días), incluyendo usuario responsable, fecha, hora y operación realizada.

RF15 - Consulta de auditoría

- Usuario: Jefatura
- Descripción: Puede consultar el historial de cambios.

Requisitos no funcionales (RNF)

- RNF01 – Rendimiento: el sistema debe soportar al menos 200 usuarios concurrentes sin degradación significativa de la respuesta.
- RNF02 – Seguridad: la comunicación debe realizarse bajo protocolo HTTPS con certificados válidos.
- RNF03 – Disponibilidad: el sistema debe estar operativo al menos el 99% del tiempo.
- RNF04 – Portabilidad: la aplicación debe funcionar en navegadores modernos sin necesidad de plugins adicionales. Versiones superiores a Chrome 72+, Firefox 65+, Safari 12.1+ (macOS) / 12.2+ (iOS), Edge 79+ (Chromium) y Samsung Internet 9.2+.
- RNF05 – Escalabilidad: el diseño debe permitir la incorporación futura de nuevos módulos.
- RNF06 – Mantenibilidad: el sistema debe permitir actualizaciones con impacto mínimo en usuarios.
- RNF07 – Documentación: El sistema contará con un manual de usuario y un manual técnico.

CRONOGRAMA DE TRABAJO

Visión general

Actividad / Semana	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Def. del tema del trabajo	•	•														
Especif. requerimientos		•	•	•												
Def. de metodología			•	•	•											
Análisis y diseño					•	•	•	•	•	•	•	•				
Desarrollo y codificación								•	•	•	•	•	•	•	•	
Validación										•				•	•	
Entrega		•		•	•					•		•				•

Cronograma por requerimientos

[illegible]

METODOLOGÍA DE DESARROLLO

Resumen de la metodología elegida

La metodología seleccionada para el desarrollo de este software se plantea como una combinación entre el enfoque en cascada y el ágil. Dado el tiempo limitado para su implementación, los sprints se organizarán de forma semanal, concentrando la mayor carga de trabajo durante los fines de semana. Asimismo, si las tareas previstas para un sprint se completan antes de la fecha establecida, se avanzará con las correspondientes al sprint siguiente. Para la planificación, asignación y seguimiento de las tareas utilizaremos Trello, lo que permitirá una mejor organización y visibilidad del progreso del proyecto.

Adecuación de la metodología

La metodología se adecuó al proyecto y al equipo de trabajo considerando las limitaciones de tiempo y los recursos disponibles. Se adoptó un enfoque mixto, combinando aspectos del modelo en cascada —para garantizar una estructura ordenada de las etapas principales— con prácticas ágiles, que permiten flexibilidad y adaptación continua.

En este marco, los sprints se definieron de una semana de duración, ajustándose al ritmo del equipo, que concentra la mayor parte del trabajo durante los fines de semana. Este esquema no solo responde a la disponibilidad horaria de los integrantes, sino que también permite un avance sostenido. Además, se incorporó Trello como herramienta de gestión colaborativa, lo que facilitó la asignación de tareas, la visualización del progreso y la comunicación entre los miembros.

De esta manera, la metodología no se aplicó de forma rígida, sino que fue adaptada a la dinámica real del equipo. A su vez, el equipo adoptó prácticas ágiles —como el adelanto de tareas del sprint siguiente en caso de completar antes las planificadas—, demostrando capacidad de adaptación y aprovechando al máximo el tiempo disponible.

HERRAMIENTAS UTILIZADAS

Las tecnologías a usar son:

- Svelte
- Django
- Python
- GitHub
- Postgres
- Trello: Para organizar las tareas del proyecto, desde la parte de diseño hasta la parte de desarrollo.
- BPMN
- Figma

Análisis

En esta etapa de análisis se van a identificar las funcionalidades requeridas y los actores involucrados. Este análisis se basó en los requerimientos funcionales y no funcionales definidos; la problemática identificada y la necesidad de acceso, control y trazabilidad de datos por parte de distintos perfiles de usuarios.

Descripción de Actores

Actor	Agente	A1
Descripción	Personal operativo de la Secretaría de Protección Civil. Son los usuarios que realizan tareas de campo o guardias.	
Características	Consulta datos personales, asistencia, guardias y horas guardias. Accede al Convenio Colectivo. Reporta errores o novedades mediante el módulo de notificaciones. Visualiza licencias usufructuadas y asignación de plus.	

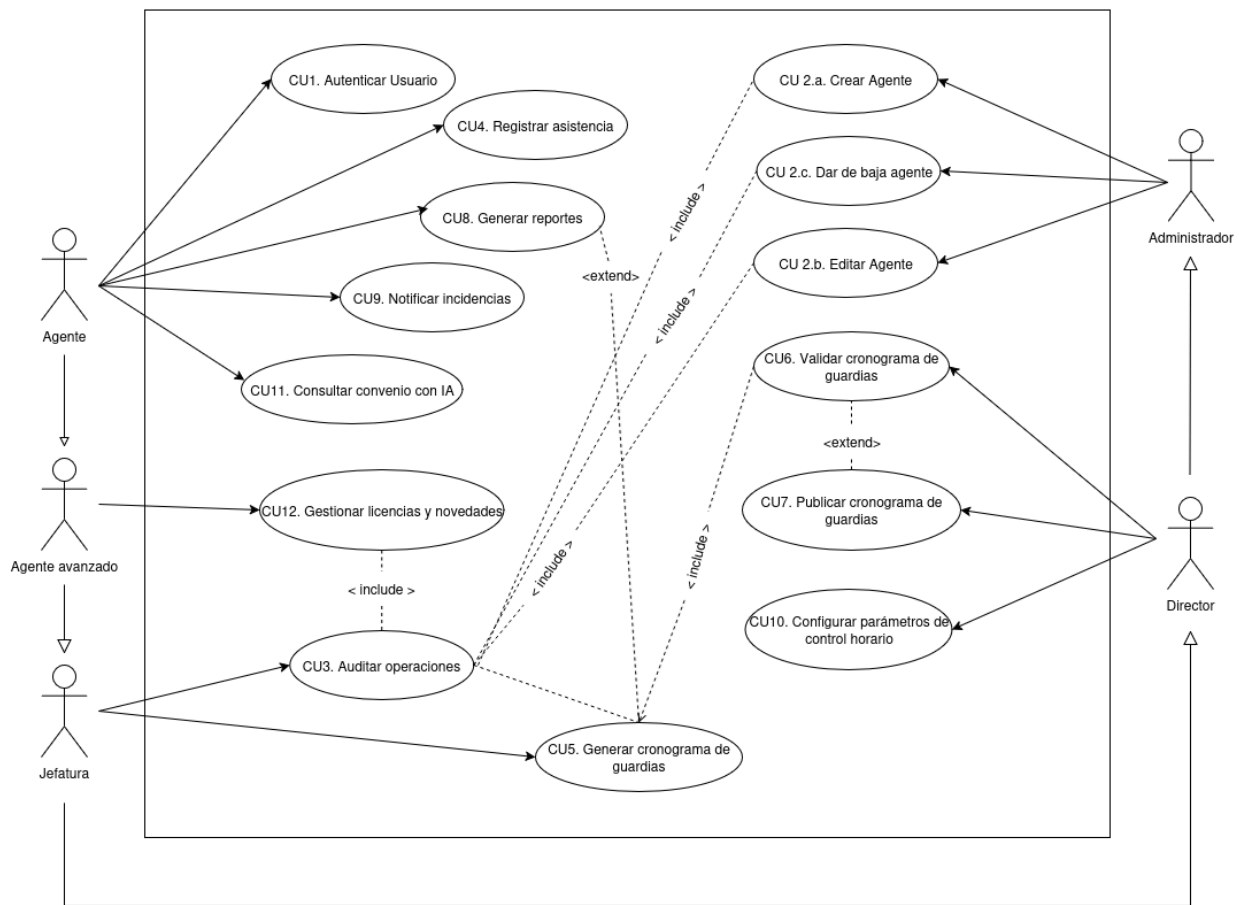
Actor	Agente Avanzado	A2
Descripción	Personal operativo de la Secretaría de Protección Civil. Son los usuarios que realizan tareas de campo o guardias con funciones adicionales.	
Características	Carga la asistencia y novedades de los agentes del área (parte diario).	

Actor	Jefatura	A3
Descripción	Responsables jerárquicos de supervisar agentes y asignar guardias.	
Características	Asigna guardias y gestiona personal bajo su dirección. Genera cronogramas de guardias.	

Actor	Director	A4
Descripción	Aprueban horas guardias y acepta licencias.	
Características	Aprueba o rechaza horas guardias. Genera reportes por agente o dirección.	

Actor	Administrador	A5
Descripción	Usuario con rol de superusuario o responsable del sistema. Tiene acceso completo a todas las funcionalidades.	
Características	Crea, da de baja y/o modifica cuentas de usuario. Otorgar permisos a usuarios. Supervisar el buen funcionamiento del sistema.	

Diagrama de Casos de Uso



La flecha que une los actores en el diagrama anterior, representan la Herencia entre los diferentes actores; como se definió anteriormente, el Agente Avanzado hereda las funcionalidades del agente, así como el Director hereda las funcionalidades de Jefatura.

Casos de uso

CU N° 1	Autenticar usuario
Actor primario:	Agente / Jefatura / Administrador
Stakeholders:	Usuarios finales; Seguridad; Administrador del sistema
Pre condiciones:	El usuario debe tener una cuenta registrada
Post condiciones:	El sistema otorga acceso a las funcionalidades según el rol.
Escenario Principal:	<ol style="list-style-type: none"> 1. El usuario selecciona 'Iniciar sesión'. 2. Ingresa credenciales (usuario y contraseña). 3. El sistema valida credenciales y estado de cuenta. 4. El sistema redirige al tablero principal mostrando las funcionalidades disponibles según el rol asignado.
Extensiones:	<ol style="list-style-type: none"> 2.a. Recuperar contraseña <ol style="list-style-type: none"> 2.a.1- El usuario selecciona "Olvidé mi contraseña". 2.a.2- El sistema envía enlace de recuperación al correo institucional. 2.a.3- El usuario establece una nueva contraseña. 2.a.4- El sistema confirma el cambio y registra el evento en auditoría. 2.a.5- El usuario vuelve al paso 2. 3.a. Credenciales inválidas <ol style="list-style-type: none"> 3.a.1-El sistema muestra un mensaje de error "Usuario o contraseña inválidos". 3.a.2- El sistema regresa al paso 2. 4.a. El usuario selecciona la opción "Cerrar sesión".

CU N° 2.a	Crear agente
Actor primario:	Administrador
Stakeholders:	RR. HH.; Jefatura; Agentes.
Pre condiciones:	El usuario debe estar autenticado;
Post condiciones:	Agente creado y registrado en el sistema; evento registrado en la auditoría.
Escenario Principal:	<ol style="list-style-type: none"> 1. El usuario selecciona la opción "Crear agente". 2. El usuario ingresa los datos personales, cargo y área. 3. El sistema valida formato y unicidad de los datos (legajo/DNI). 4. El usuario confirma la creación. 5. El sistema guarda el nuevo agente, registra auditoría y muestra confirmación.
Extensiones:	<ol style="list-style-type: none"> 3.a. Correo/DNI duplicado <ol style="list-style-type: none"> 3.a.1- El sistema rechaza la acción y solicita corrección. 3.a.2- El usuario corrige los datos y vuelve al paso 2. 5.a. Enviar invitación/restablecer contraseña <ol style="list-style-type: none"> 5.a.1- El sistema envía correo de acceso inicial y registra auditoría.

CU N° 2.b	Editar agente
Actor primario:	Administrador
Stakeholders:	RR.HH.; Jefaturas; Agentes
Pre condiciones:	El usuario debe estar autenticado; el agente debe existir en el sistema.
Post condiciones:	Datos del agente actualizados; evento registrado en la auditoría.
Escenario Principal:	<ol style="list-style-type: none"> 1. El usuario busca y selecciona un agente por nombre, legajo o área. 2. El usuario modifica los datos personales, cargo o área. 3. El sistema valida coherencia y unicidad de los cambios. 4. El usuario confirma los cambios. 5. El sistema guarda la actualización, registra auditoría y muestra confirmación.
Extensiones:	<ol style="list-style-type: none"> 2.a. Intento de degradar al único Administrador <ol style="list-style-type: none"> 2.a.1- El Sistema impide la acción por política de mínimos. 2.a.2- El Administrador mantiene el rol o agrega otro administrador antes de degradar. 3.a. Legajo o DNI duplicado <ol style="list-style-type: none"> 3.a.1- El sistema rechaza la acción y solicita corrección. 3.a.2- El usuario corrige los datos y vuelve al paso 2. 3.b. Duplicado de correo/DNI <ol style="list-style-type: none"> 3.b.1- El Sistema rechaza y solicita corrección. 3.b.2- El Administrador corrige y vuelve al paso 2.

CU N° 2.c	Dar de baja agente (baja lógica)
Actor primario:	Administrador
Stakeholders:	RR.HH.; Jefaturas; Agentes
Pre condiciones:	El usuario debe estar autenticado; el agente debe existir en el sistema.
Post condiciones:	Agente dado de baja; accesos revocados; evento registrado en la auditoría.
Escenario Principal:	<ol style="list-style-type: none"> 1. El usuario selecciona la opción "Dar de baja agente". 2. El sistema muestra advertencia con el alcance de la baja. 3. El usuario confirma la acción. 4. El sistema marca al agente como dado de baja, registra auditoría y muestra confirmación.
Extensiones:	<ol style="list-style-type: none"> 2.a. El agente tiene guardias u horas pendientes <ol style="list-style-type: none"> 2.a.1- El sistema bloquea la baja y muestra un mensaje "Deben resolverse las dependencias". 2.a.2- El usuario gestiona las dependencias y vuelve al paso 3. 2.b. El Usuario es el único Administrador activo <ol style="list-style-type: none"> 2.b.1- El Sistema bloquea la baja hasta que exista al menos otro Administrador activo.

CU N° 3	Auditar operaciones
Actor primario:	Jefatura/ Director/ Administrador.
Stakeholders:	Dirección; Auditoría interna; Seguridad; Agentes
Pre condiciones:	Usuario autenticado con permisos de auditoría; registros auditables ya existen en el sistema.
Post condiciones:	Registros visualizados y/o exportados; evento registrado en auditoría.
Escenario Principal:	<ol style="list-style-type: none"> 1. El Usuario selecciona la opción “Auditoría” en el sistema. 2. El Usuario define criterios de búsqueda (fechas, usuario, tipo de operación). 3. El Sistema valida los filtros y busca en los registros. 4. El Sistema muestra la lista de operaciones coincidentes (quién, qué, cuándo). 5. El Usuario revisa los resultados. 6. El Usuario exporta los registros si lo requiere. 7.El Sistema genera archivo de exportación y registra el evento en la auditoría
Extensiones:	<ol style="list-style-type: none"> 3.a. Sin resultados para filtros 3.a.1- El sistema muestra el mensaje: “No se encontraron registros”. 3.a.2- El usuario ajusta criterios y vuelve al paso 2.

CU N° 4	Registrar asistencia
Actor primario:	Agente/ Agente Avanzado/ Jefatura / Director / Administrador
Stakeholders:	Agentes; Jefaturas; RR.HH.
Pre condiciones:	El usuario debe estar autenticado; calendario y reglas de control horario vigentes.
Post condiciones:	Marcas de asistencia registradas o corregidas; parte diario actualizado; evento registrado en la auditoría.
Escenario Principal:	<ol style="list-style-type: none"> 1. El usuario selecciona la opción “Registrar asistencia”. 2. El usuario marca el ingreso o el egreso. 3. El sistema valida la marca contra horarios y ventanas de tolerancia. 4. El sistema genera o actualiza el parte diario correspondiente. 5. La jefatura revisa incidencias. 6. El sistema guarda los datos, registra la acción en la auditoría y muestra confirmación.
Extensiones:	<ol style="list-style-type: none"> 3.a. Marca fuera de ventana 3.a.1- El sistema muestra una alerta y solicita justificación. 3.a.2- El usuario ingresa la justificación. 3.a.3- El sistema guarda la información y registra auditoría. 5.a. Falta de marca o doble marca detectada 5.a.1- El sistema genera una alerta en el parte diario. 5.a.2- La jefatura corrige la asistencia desde su panel. 5.a.3- El sistema actualiza el registro y deja trazabilidad en auditoría.

CU N° 5	Generar cronograma de guardias
Actor primario:	Jefatura / Director / Administrador
Stakeholders:	Agentes; RR.HH.; Dirección
Pre condiciones:	El usuario debe estar autenticado; existen agentes y reglas vigentes de horarios/feriados/topes.
Post condiciones:	Cronograma generado para el período; evento registrado en la auditoría.
Escenario Principal:	<ol style="list-style-type: none"> 1. La jefatura selecciona el período a planificar. 2. La jefatura asigna horas y días de guardia a los agentes de su área. 3. El sistema valida solapamientos, feriados y topes legales. 4. El sistema genera el cronograma en estado Borrador y muestra alertas pendientes (si las hubiera). 5. La jefatura guarda el borrador para su envío a validación. 6. El sistema registra la acción en auditoría y marca el cronograma como “Listo para validar”.
Extensiones:	<ol style="list-style-type: none"> 3.a. Inconsistencias detectadas (solapamientos/topes/feriados) <ol style="list-style-type: none"> 3.a.1- El sistema muestra las alertas. 3.a.2- La jefatura corrige asignaciones y vuelve al paso.

CU N° 6	Validar cronograma de guardias
Actor primario:	Director / Administrador
Stakeholders:	Jefatura; Agentes; RR.HH.
Pre condiciones:	Cronograma en estado “Listo para validar”; usuario autenticado con permisos de validación.
Post condiciones:	Cronograma aprobado y listo para publicación; evento registrado en la auditoría.
Escenario Principal:	<ol style="list-style-type: none"> 1. El director abre el cronograma pendiente de validación. 2. El director revisa el resumen (período, dotación, totales, alertas resueltas). 3. El sistema verifica que no existan alertas bloqueantes. 4. El director aprueba el cronograma. 5. El sistema cambia el estado a Aprobado, bloquea ediciones de jefatura y registra auditoría.
Extensiones:	<ol style="list-style-type: none"> 3.a. Alertas bloqueantes vigentes <ol style="list-style-type: none"> 3.a.1- El sistema informa las incidencias. 3.a.2- El director cancela la validación; la jefatura corrige en CU-U06 y reenvía a validación. 4.a. Rechazar cronograma <ol style="list-style-type: none"> 4.a.1- El director rechaza el cronograma indicando el motivo. 4.a.2- El sistema notifica a jefatura y cambia el estado a “Requiere correcciones” para que vuelva a CU-U06.

CU N° 7	Publicar cronograma de guardias
Actor primario:	Director / Administrador
Stakeholders:	Jefatura; Agentes; RR.HH.; Administración
Pre condiciones:	Cronograma en estado Aprobado; usuario autenticado con permisos de publicación.
Post condiciones:	Cronograma publicado; guardias asignadas a cada agente; notificaciones emitidas; auditoría registrada.
Escenario Principal:	<ol style="list-style-type: none"> 1. El director selecciona el cronograma aprobado para publicar. 2. El sistema muestra el resumen final (período, agentes afectados, totales). 3. El director confirma la publicación. 4. El sistema cambia el estado a Publicado, asigna las guardias a cada agente y bloquea ediciones según política. 5. El sistema envía notificaciones a jefatura y agentes y registra auditoría.
Extensiones:	<ol style="list-style-type: none"> 2.a. Cambios no validados detectados <ol style="list-style-type: none"> 2.a.1- El sistema advierte que hay modificaciones pendientes de validación. 2.a.2- El director cancela la publicación y devuelve a CU-U06. 5.a. Fallo parcial en notificaciones <ol style="list-style-type: none"> 5.a.1- El sistema completa la publicación, marca destinatarios con error y ofrece reintento de envío.

CU N° 8	Generar reportes
Actor primario:	Agente/ Agente Avanzado / Jefatura / Director / Administrador
Stakeholders:	Agentes; Jefaturas; RR.HH.; Dirección
Pre condiciones:	Usuario autenticado; permisos adecuados para el alcance del reporte.
Post condiciones:	Reporte visualizado y/o exportado; evento registrado en la auditoría.
Escenario Principal:	<ol style="list-style-type: none"> 1. El usuario selecciona la opción “Generar reporte”. 2. El usuario aplica filtros según el tipo de información que necesita (fechas, agente, área, dirección, tipo de novedad). 3. El sistema valida los filtros y consulta la información solicitada. 4. El sistema muestra la vista previa del reporte con los resultados. 5. El usuario revisa el reporte. 6. El usuario exporta el reporte a PDF o Excel. 7. El sistema genera el archivo, lo entrega y registra el evento en la auditoría.
Extensiones:	<ol style="list-style-type: none"> 2.a. Reporte individual (Agente) <ol style="list-style-type: none"> 2.a.1-El usuario Agente solicita su propio historial. 2.a.2- El sistema genera el reporte personal y lo muestra. 2.b. Reporte por equipo/área (Jefatura) <ol style="list-style-type: none"> 2.b.1- El usuario Jefatura aplica filtros por su equipo. 2.b.2- El sistema genera el reporte de agentes bajo su responsabilidad. 2.c. Reporte por dirección (Director/Administrador) <ol style="list-style-type: none"> 2.c.1- El usuario Director o Administrador aplica filtros por dirección y rango de fechas. 2.c.2- El sistema genera el reporte consolidado. 3.a. Sin resultados <ol style="list-style-type: none"> 3.a.1- El sistema muestra el mensaje “No se encontraron registros”. 3.a.2- El usuario ajusta filtros y vuelve al paso 2. 3.b. Demasiados resultados (sobrecarga) <ol style="list-style-type: none"> 3.b.1- El sistema propone segmentar por períodos o aplicar filtros más específicos.

CU N° 9	Notificar incidencias
Actor primario:	Agente / Agente Avanzado / Jefatura / Director / Administrador
Stakeholders:	Agentes; Jefaturas; Soporte; Administración
Pre condiciones:	Usuario autenticado; destinatario disponible en la organización.
Post condiciones:	Notificación generada y enviada; evento registrado en la auditoría.
Escenario Principal:	<ol style="list-style-type: none"> 1. El usuario selecciona la opción “Notificar” en su panel. 2. El sistema abre un formulario de contacto con el correo del destinatario preconfigurado. 3. El usuario completa el mensaje con el detalle de la incidencia. 4. El usuario envía la notificación. 5. El sistema genera el correo electrónico, lo envía al destinatario y registra la acción en la auditoría.
Extensiones:	<ol style="list-style-type: none"> 1.a. Si es Agente, selecciona el botón “Contactar Jefatura”. 1.b. Si es Jefatura, selecciona el botón “Contactar Agente” y elige destinatario. 2.a. Destinatario no disponible (sin jefe asignado o agente dado de baja). <ol style="list-style-type: none"> 2.a.1- El sistema muestra un mensaje de error: “No existe destinatario válido”. 2.a.2- El usuario cancela o selecciona otro destinatario. 5.a. Fallo en el envío del correo. <ol style="list-style-type: none"> 5.a.1- El sistema informa que la notificación no pudo enviarse. 5.a.2- El usuario puede reintentar el envío o guardar el mensaje como borrador.

CU N° 10	Configurar parámetros de control horario
Actor primario:	Administrador / Director
Stakeholders:	Direcciones; Jefaturas; RR.HH.; Seguridad
Pre condiciones:	Usuario autenticado; políticas y límites previamente definidos.
Post condiciones:	Parámetros de control horario actualizados y auditados.
Escenario Principal:	<ol style="list-style-type: none"> 1. El usuario administrador accede a la opción "Parámetros de control horario". 2. El usuario define o ajusta los valores globales (horarios, tolerancias, ventanas de marcación, reglas de plus). 3. El sistema valida que los parámetros sean coherentes y estén dentro de los rangos permitidos. 4. El usuario confirma la configuración. 5. El sistema guarda los parámetros, actualiza la vigencia y registra la acción en la auditoría.
Extensiones:	<ol style="list-style-type: none"> 3.a. Valor fuera de rango o solapado <ol style="list-style-type: none"> 3.a.1- El sistema rechaza la configuración y muestra un mensaje de error: "<i>Valor fuera de rango/solapado</i>". 3.a.2- El usuario corrige y vuelve al paso 2. 3.b. Inconsistencias en reglas de plus <ol style="list-style-type: none"> 3.b.1- El sistema bloquea la acción y muestra un mensaje con detalles y sugerencias. 3.b.2- El usuario corrige y vuelve al paso 2. 3.c. Necesidad de retrotraer cambios <ol style="list-style-type: none"> 3.c.1- El sistema conserva una copia de la configuración anterior. 3.c.2- El usuario puede restaurar la versión anterior si es necesario. 5.a. Impacto en horarios vigentes <ol style="list-style-type: none"> 5.a.1- El sistema detecta que los cambios afectan horarios en uso. 5.a.2- El sistema solicita confirmación de fecha de efectividad. 5.a.3- El usuario confirma la fecha y el sistema programa la aplicación.

CU N° 11	Consultar convenio con IA
Actor primario:	Agente / Agente Avanzado / Jefatura / Director / Administrador
Stakeholders:	RR.HH.; Auditoría;
Pre condiciones:	Usuario autenticado; versión vigente del Convenio cargada e indexada; permisos de lectura.
Post condiciones:	Respuesta mostrada con citas al Convenio; evento registrado en auditoría.
Escenario Principal:	<ol style="list-style-type: none"> 1. El usuario abre "Consulta del Convenio". 2. El usuario ingresa una pregunta en lenguaje natural. 3. El sistema procesa la consulta usando el índice del Convenio (sin internet?). 4. El sistema muestra la respuesta basándose en el convenio cargado.
Extensiones:	<ol style="list-style-type: none"> 1.a. Convenio no indexado o versión desactualizada <ol style="list-style-type: none"> 1.a.1- El sistema indica que debe cargarse el convenio. 1.a.2- El Administrador va a CU-U11 (parámetros globales) y ejecuta "Actualizar Convenio" (flujo de carga). 3.a. Pregunta fuera de alcance <ol style="list-style-type: none"> 3.a.1- El sistema detecta que no hay soporte en el Convenio. 3.a.2- El sistema responde: "Esta pregunta no se encuentra en el Convenio cargado; intente con términos del documento."

CU N° 12	Gestionar licencias y novedades
Actor primario:	Agente avanzado / Jefatura / Director / Administrador
Stakeholders:	Agentes; Jefaturas; RR.HH.;
Pre condiciones:	Usuario autenticado; agente válido en el sistema.
Post condiciones:	Licencia/novedad registrada con documentación adjunta; evento registrado en la auditoría.
Escenario Principal:	<ol style="list-style-type: none"> 1. El usuario selecciona la opción "Cargar licencia/novedad". 2. El usuario ingresa los datos básicos: Tipo de licencia/novedad (enfermedad, estudio, franco, etc), fecha de inicio y fin, y observaciones opcionales. 3. El usuario adjunta la documentación respaldatoria (ej. certificado médico). 4. El sistema valida que las fechas sean coherentes y que el archivo sea del formato permitido(pdf, jpg, png). 5. El usuario confirma la carga. 6. El sistema guarda el registro, asocia la documentación adjunta y registra auditoría.
Extensiones:	<ol style="list-style-type: none"> 2.a. Fechas inválidas (inicio mayor a fin) <ol style="list-style-type: none"> 2.a.1- El sistema muestra un mensaje de error: "Rango de fechas inválido". 2.a.2- El usuario corrige y vuelve al paso 2. 3.a. Archivo no permitido <ol style="list-style-type: none"> 3.a.1- El sistema muestra un mensaje de error: "Formato de archivo no válido (solo pdf/jpg/png)". 3.a.2- El usuario selecciona un archivo válido y vuelve al paso 3.

Diagramas

Diagrama sobre Plus 20% y 40%

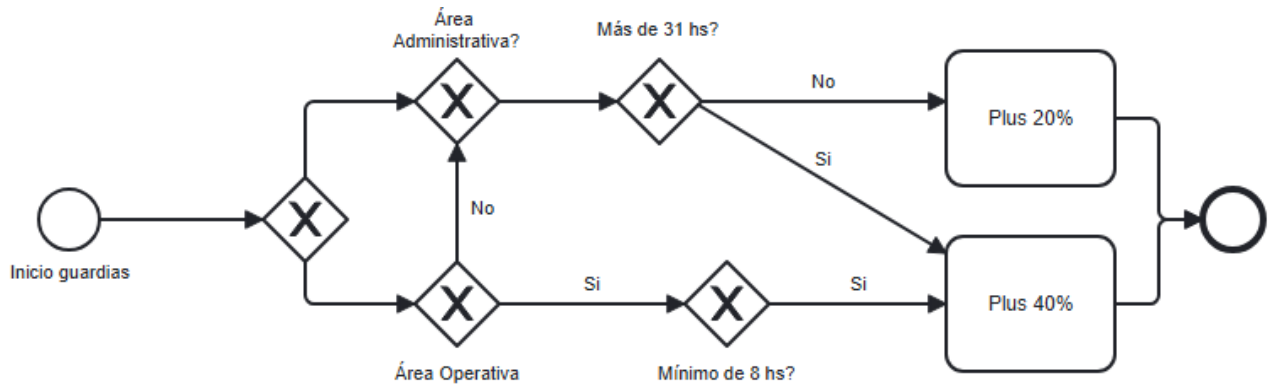


Diagrama de la gestión de asistencias

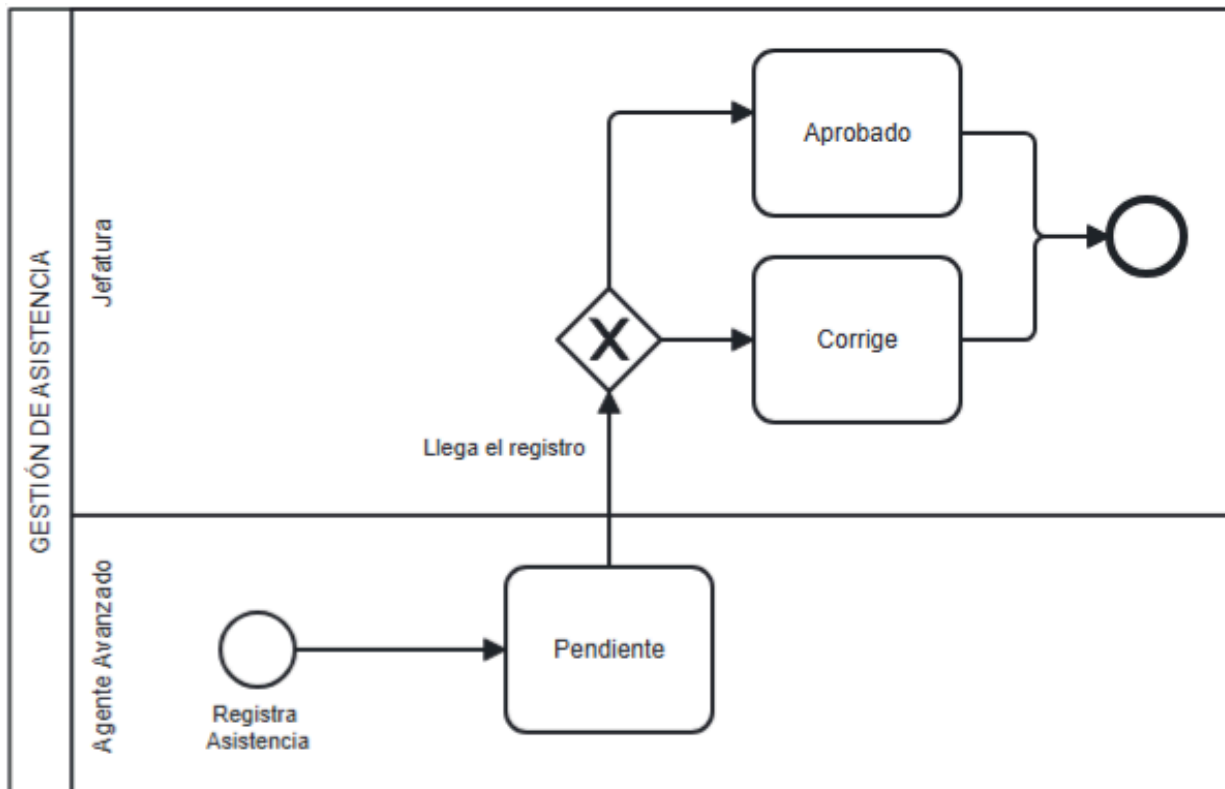
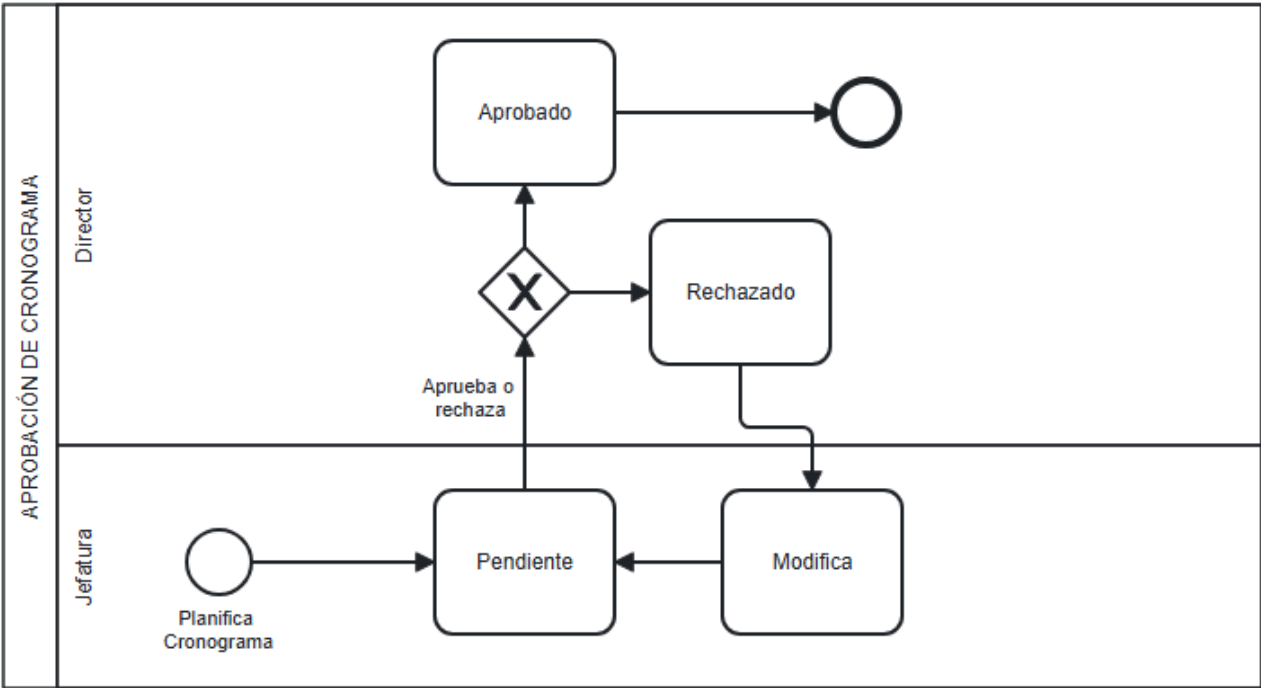


Diagrama de gestión del cronograma



Matriz de trazabilidad

Requerimientos Funcionales (RF) y Casos de uso (CU)

	CU1	CU2.a	CU2.b	CU2.c	CU3	CU4	CU5	CU6	CU7	CU8	CU9	CU10	CU11	CU12
RF01		x	x	x										
RF02						x								
RF03						x								
RF04														x
RF05							x							
RF06								x						
RF07							x	x	x					
RF08										x				
RF09													x	
RF10									x					
RF11											x			
RF12	x													
RF13	x	x												
RF14	x	x	x	x	x	x	x	x	x	x	x	x	x	x
RF15							x							

Casos de Uso (CU) y Actores

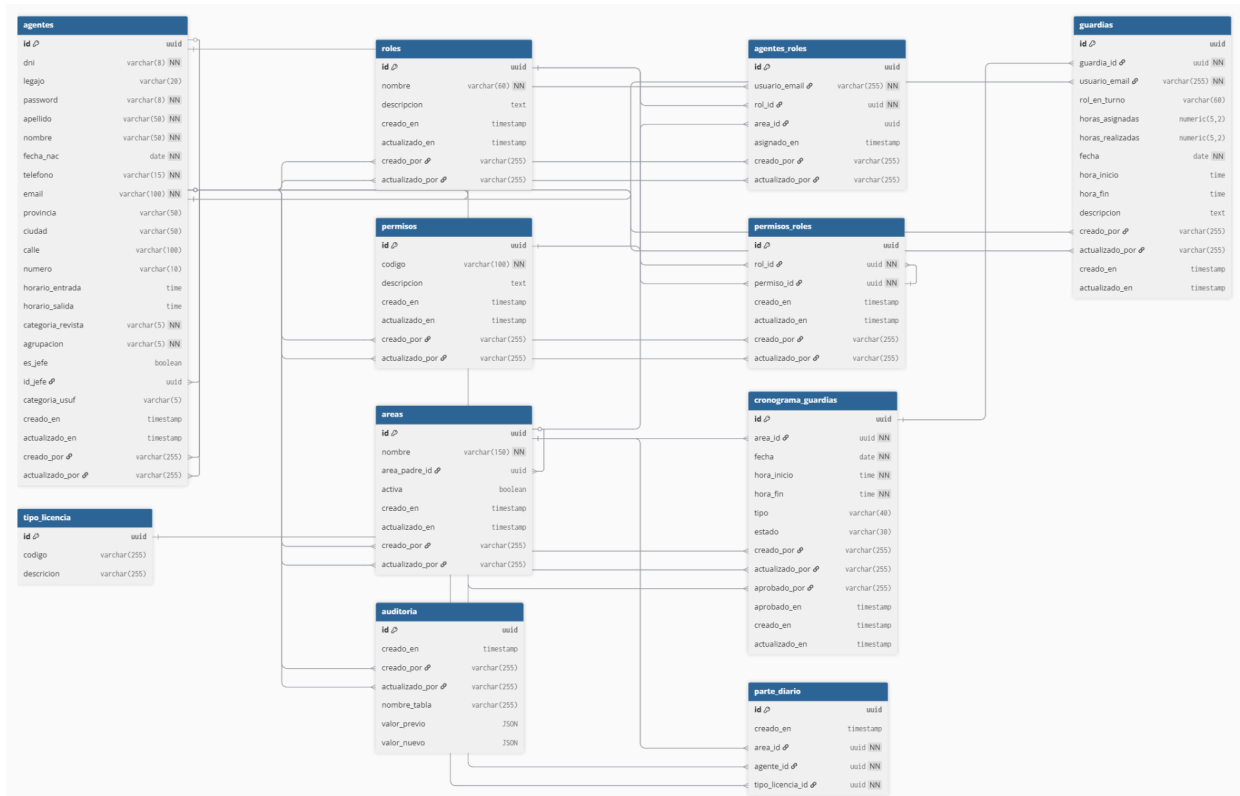
Casos de uso	Actores	Agente	Agente Avanzado	Jefatura	Director	Administrador
CU1	Autenticar Usuario	x	x	x	x	x
CU2.a	Crear Agente					x
CU2.b	Editar Agente					x
CU2.c	Dar de baja Agente					x
CU3	Auditar Operaciones			x	x	x
CU4	Registrar asistencia		x	x	x	x
CU5	Generar cronograma de guardias			x	x	x
CU6	Validar cronograma de guardias				x	x
CU7	Publicar cronograma de guardias				x	x
CU8	Generar reportes		x	x	x	x
CU9	Notificar incidencias	x	x	x	x	x
CU10	Configurar parámetros de control horario				x	x
CU11	Consultar convenio con IA	x	x	x	x	x
CU12	Gestionar Licencias y novedades		x	x	x	x

Diseño

Documentación técnica de las etapas desarrolladas. Incluirá los diagramas realizados durante el análisis y el diseño, y las principales pantallas de la aplicación.

Diagrama Entidad-Relación

Para ver donde se diseñó el diagrama, el enlace se encuentra vinculado con la imagen presentada a continuación:




 [GIGA-light.pdf](#)

Diagrama de Clases

A continuación, se presentan las capturas de los diagramas de clases generados con la herramienta PlantUML en Visual Studio Code (VSCode).

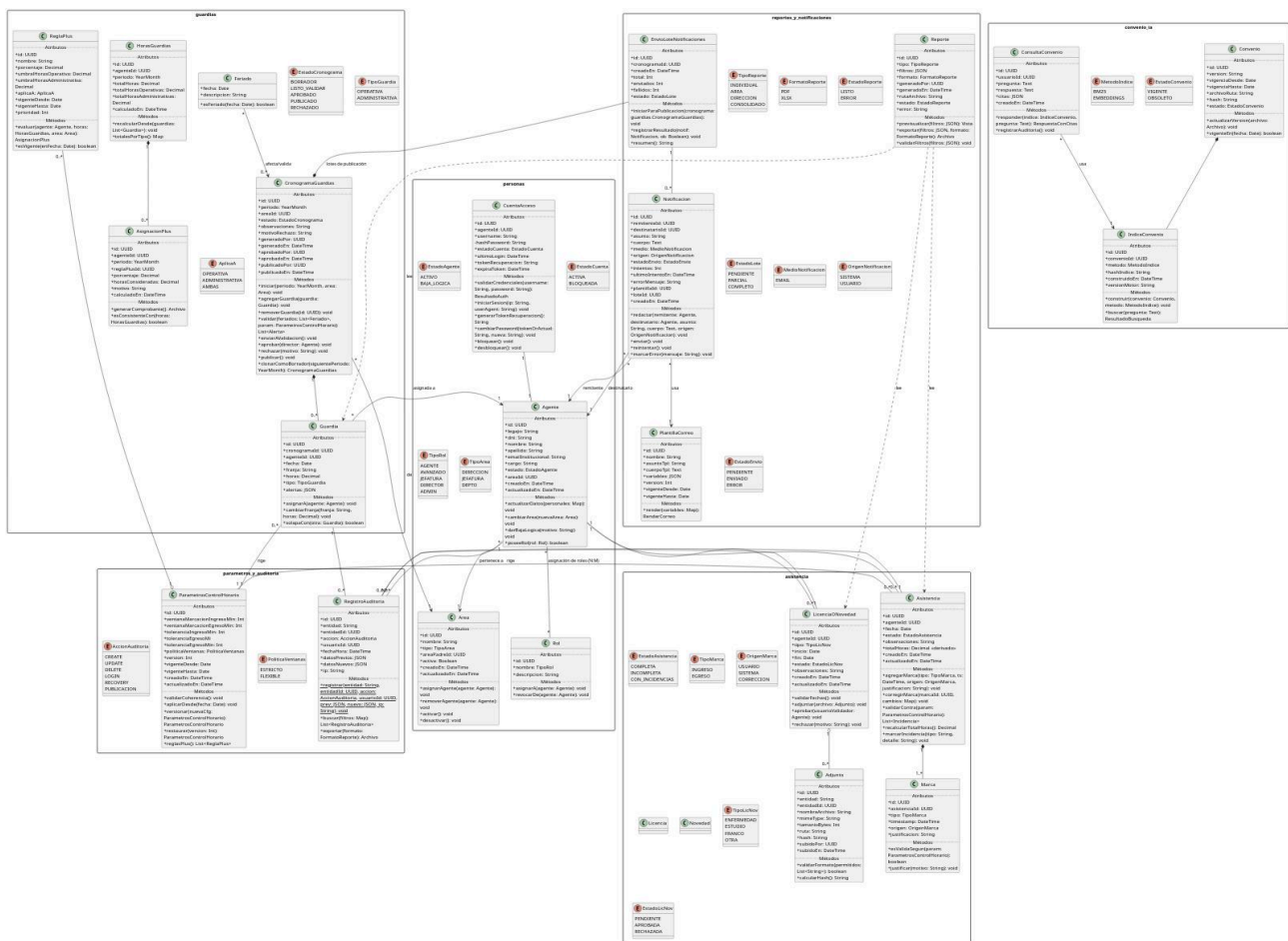


diagrama de clases.jpg

Diseño de pantallas

Propósito: Punto de entrada a la app. Permite iniciar sesión y, sin autenticarse, consultar a la IA sobre el Convenio Colectivo de Trabajo (CCT).

Estado: usuario no autenticado (no se muestra nombre ni rol).

Indicaciones visuales

- Nombre de la app, logo de la Secretaría de Seguridad Vial en la banda superior y logo de la Secretaría de Protección Civil y leyenda © 2025 UNTDF en el pie en toda la app.

Página de inicio:



Home de la app: Esta pantalla muestra las opciones del menú en función de los permisos que tenga el usuario.



Interfaz al acceder a algunas de las opciones del menú.



Interfaz Mis Dato, donde el agente podrá visualizar su ficha personal y su actividad de **asistencia** y **guardias** del mes seleccionado (en la imagen: **septiembre 2025**).

Interfaz Asistencia, donde el agente podrá consultar y cargar el **Parte Diario de Asistencia** de los agentes del área (si su rol y permisos asignados se lo permiten) y visualizar el estado mensual por día.




Observatorio Vial

Seleccionar Mes
Para Visualizar
Asistencia

Septiembre 2025		L	M	Mi	J	V	S	D	L	M	Ju.	J	V	S	D	L	M	Vi.	J	V	S	D	L	M	Sa.	J	V	S	D	L	M
Agente	Legajo	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Frers Pamela	27803459/00																														
Pérez Juan	12345678/00																														

Gestión de Parte Diario

Agente	Legajo	Fecha	Hora Entrada	Hora Salida	Novedad
			_____	_____	

Guardar
Parte de Diario del
AgenteModificar
Parte de Diario del
Agente

Pantalla Principal



Cerrar Sesión

SOBRE LAS ITERACIONES

En este capítulo se desarrolló el seguimiento por fechas e iteraciones donde se detalla cómo fue el avance de nuestro grupo con respecto al desarrollo del software GIGA.

Las etapas fueron:

- Definición del tema (Iteración 1)
- Selección de metodología (Iteración 1)
- Análisis de requerimientos (Iteración 1 y 2)
- Diseño de casos de uso (Iteración 2)
- Selección de herramientas
- Diseño de clases y DB
- Modelado del sistema
- Desarrollo
- Testing
- Entrega de Documento Final

(Posteriormente migrar esto a un ANEXO y presentar en esta sección más resumidamente)

ITERACIÓN 1

Fecha: 11/08

Tareas:

- Creación de grupo de whatsapp.
- Proponer temas para realizar la app.

Fecha 12/08

- Debatar sobre dos temas propuestos: Stalke.ar y GIGA, el primero trataba de buscar datos de personas a solicitud del cliente.
- Nos enteramos que necesitábamos un integrante más para conformar el grupo.

Fecha 13/08

- Después de buscar información sobre [Stalke.ar](https://stalke.ar) íbamos a tener muchos problemas legales, así que decidimos hacer GIGA.
- Entrevistamos a Cristian y Leandro que estaban sin grupo y los sumamos al equipo.
- Añadimos a Cristian y a Leandro al grupo de WhatsApp.
- Comenzó debate de si avanzar con la propuesta GIGA o los nuevos integrantes tenían otras ideas.
- Decidimos juntarnos el viernes 15 en un domicilio para conocer a los nuevos integrantes y terminar de conformar el equipo de trabajo.

Fecha: 15/08

- Primera reunión en domicilio con el equipo completo.
- Debatisimos y se decidió continuar con la propuesta GIGA.
- Escribimos la propuesta de GIGA y la refinamos.

Fecha: 17/08

- Seguimos refinando la propuesta.
- Entrega de propuesta.

Fecha 19/08

- ENTREGA DE PROPUESTA: Exposición de la propuesta en clase.
- Aprobación de la propuesta por parte del profesor.
- Definición de roles para las etapas.

Fecha 20/08

- Empezamos a escribir el SRS.
- Creación del github.

Fecha 22/08

- descargamos el iEEE830 y el manual SRS para guiarnos.

Fecha 23/08

- Cena de investigación con otros grupos, para hacer comparación de proyectos objetivos de alcance y obtener cual es desarrollo que esperan hacer.

Fecha del 25/08 al 28/08

- Continuamos escribiendo el SRS.
- Finalización de definición de requerimientos funcionales y no funcionales.

Fecha 29/08

- Se pulieron los requerimientos y se definieron los actores para proceder con los casos de uso.
- Comenzamos a plantear los casos de uso.
- Creación del Tablero en Trello.

ITERACIÓN 2

Fecha 31/8

- Agrega definición de niveles de acceso.
- Se vuelven a pulir los requerimientos considerando los niveles de acceso.
- Se definieron los casos de uso en función de los niveles de acceso.

Fecha 1/9

- Revisión de documentación y alineación de requerimientos y casos de uso.
- Creación del boceto del diagrama de Casos de uso.

Fecha 2/9

- ENTREGA DE DOCUMENTOS DE REQUERIMIENTOS: Revisión del material con el Docente (aún los requisitos no se revisaron).
- Desarrollo del diagrama representativo del PLUS 20% Y 40%.
- Avance con diagrama de casos de uso.

Fecha 3/9

- Debate sobre el alcance de la aplicación.
- Acuerdo sobre nuevo alcance del sistema a desarrollar.

Fecha 5/9

- Reunión grupal y presencial, para definir nuevos cambios y plasmarlos en la documentación.
- Como resultado del encuentro se redefinieron los alcances del proyecto, funciones, características de usuario, restricciones y requerimientos funcionales y no funcionales.
- Queda pendiente corrección de diagramas, planillas y casos de uso.

fecha 16/9

- Entrega de documento con Requerimientos.
- Se traza plan de trabajo para proxima entrega (26/9).

fecha 18/9

- Definición final de los casos de uso.
- Presentación de Diagrama de casos de uso.

fecha 20/9

- Se creó archivo .puml para la creación de diagrama de clases.
- Presentación en el archivo de documentación.
- Queda pendiente el traslado a subcarpeta dentro del repositorio.

fecha 21/09

- Se crearon algunas pantallas de la app.
- Se importaron al documento en preparación con una breve descripción a modo de manual de usuario.

fecha 26/09

- Reunión para refinar modelo entidad-relación, y definición de pantallas.

fecha 15/10

- se armo la estructura del proyecto en funcion de los diagramas de clases y el diagrama de entidad-relacion presentado en este documento
- se preparo el front y el back con las configuraciones minimas para poder empezar a hacer el proyecto
 - se creo la carpeta front donde estara desarrollado el frontend de nuestra aplicacion con el framework Svelte + Javascript.

- se creo la carpeta back donde se desarrollara el backend de nuestra aplicacion con Django + Python + Postgres
- Se crearon los readme para poder tener la guia basica para poder instalar el proyecto y comenzar con el desarrollo del proyecto.
- Ademàs se creo la carpeta documentacion donde se presenta el diagrama de clases y el diagrama de la base de datos.
-

SOBRE LOS ENTREGABLES

Los entregables durante las ITERACIÓN 1,2 ... Fueron el avance en el desarrollo de este documento, por lo que los primeros entregables están contenidos en este mismo documento.

Aplicaciones y plataformas que forman al sistema

Requerimientos técnicos para la instalación

Descripción técnica de los requerimientos y pasos necesarios para la instalación del software desarrollado.

Copia del software desarrollado al menos en un 80% de su funcionalidad, según los requerimientos definidos para dicho trabajo.

PRESENTACIÓN VISUAL PARA APROBAR FINAL

[Esta sección es requerida para aprobar la materia, no para la regularidad]