# 1.8 Requisitos iniciales

A continuación, se explican los requisitos iniciales de cada módulo que constituye el sistema.

## 1.8.1 Requisitos funcionales

### 1.8.1.1 Módulo de integración con sistemas centrales

REINT1. El sistema debe permitir la integración con el Sistema de Información Hospitalaria (HIS) existente.

REINT1.1. El sistema debe sincronizar en tiempo real los datos de los pacientes desde el HIS.

REINT1.2. El sistema debe permitir la actualización de los registros de los pacientes en el HIS.

REINT1.3. El sistema debe soportar la consulta de historiales médicos y citas desde el HIS.

REINT2. El sistema debe ofrecer una interfaz de programación de aplicaciones (API) para la comunicación bidireccional.

REINT2.1. El sistema debe permitir el envío de datos desde el sistema de teleasistencia al HIS a través de la API.

REINT2.2. El sistema debe permitir la recepción de datos desde el HIS al sistema de teleasistencia a través de la API.

REINT3. El sistema debe garantizar la seguridad de los datos compartidos entre sistemas.

REINT3.1. El sistema debe implementar cifrado de datos durante la transmisión.

REINT3.2. El sistema debe realizar autenticaciones seguras para acceder a la API.

REINT4. El sistema deberá permitir la sincronización en tiempo real los siguientes datos de los pacientes entre el sistema de teleasistencia y los sistemas centrales del contratante.

REINT4.1. Historiales clínicos.

REINT4.2. Citas previas.

REINT4.3. Citas futuras.

REINT4.4. Resultados de pruebas

REINT5. El sistema debe proporcionar registros de auditoría para todas las operaciones de intercambio de datos.

REINT5.1. El sistema debe registrar las operaciones de envío de datos al HIS.

REINT5.2. El sistema debe registrar las operaciones de recepción de datos desde el HIS.

### 1.8.1.2 Módulo de gestión de usuarios

REUSU1. El sistema debe permitir la creación de perfiles de usuario.

REUSU1.1 El sistema deberá permitir crear los perfiles para pacientes.

REUSU1.2 El sistema deberá permitir crear los perfiles para personal sanitario.

REUSU1.3. El sistema debe asignar un identificador único a cada perfil de usuario.

REUSU1.4. El sistema debe recoger información básica del perfil, incluyendo nombre, contacto.

REUSU 1.4.1. El sistema también deberá recoger el historial médico para los usuarios pacientes.

REUSU2. El sistema debe ofrecer funcionalidades para actualizar la información de los perfiles de usuario.

REUSU2.1. El sistema debe permitir a los usuarios modificar su información de contacto.

REUSU2.2. El sistema debe permitir al personal sanitario actualizar los detalles médicos de los perfiles de pacientes.

REUSU3. El sistema debe habilitar la búsqueda de perfiles de usuario utilizando varios criterios.

REUSU3.1. El sistema debe permitir la búsqueda por nombre.

REUSU3.2. El sistema debe permitir la búsqueda por identificador.

REUSU3.3. El sistema debe permitir la búsqueda por estado médico.

REUSU4. El sistema debe implementar medidas de seguridad para la protección de la información de los perfiles.

REUSU4.1. El sistema debe cifrar la información sensible almacenada en los perfiles de usuario.

REUSU4.2. El sistema debe restringir el acceso a la información médica a personal sanitario autorizado.

REUSU5. El sistema debe soportar la asignación de roles y permisos a los usuarios.

REUSU5.1. El sistema debe definir roles específicos para pacientes, personal sanitario, y administradores.

REUSU5.2. El sistema debe gestionar los permisos asociados a cada rol para acceder a funcionalidades específicas.

REUSU6. El sistema debe registrar y mantener un historial de todas las interacciones y cambios realizados en los perfiles de usuario.

REUSU7. El sistema debe proporcionar soporte para la gestión de consentimientos de los usuarios.

REUSU7.1. El sistema debe recopilar y almacenar el consentimiento del usuario para el tratamiento de datos personales y médicos.

REUSU7.2. El sistema debe permitir a los usuarios modificar o retirar su consentimiento en cualquier momento.

## 1.8.1.3 Módulo de sistemas de mensajería

REMEN1. El sistema debe permitir que pacientes autenticados inicien conversaciones con personal sanitario asignado.

REMEN1.1. El sistema debe permitir el envío de mensajes de texto por parte de pacientes autenticados.

REMEN1.2. El sistema debe permitir a los pacientes adjuntar y enviar imágenes.

REMEN1.3. El sistema debe permitir a los pacientes adjuntar y enviar documentos médicos.

REMEN2. El sistema debe permitir al personal sanitario iniciar conversaciones con pacientes basándose en necesidades de seguimiento médico.

REMEN2.1. El sistema debe permitir el envío de mensajes de texto por parte del personal sanitario.

REMEN2.2. El sistema debe permitir al personal sanitario adjuntar y enviar imágenes.

REMEN2.3. El sistema debe permitir al personal sanitario adjuntar y enviar documentos médicos.

REMEN3. El sistema debe almacenar el historial de todas las conversaciones.

REMEN3.1. El sistema debe asegurar el acceso al historial de conversaciones para pacientes autenticados.

REMEN3.2. El sistema debe asegurar el acceso al historial de conversaciones para el personal sanitario.

REMEN4. El sistema debe encriptar los mensajes.

REMEN5. El sistema debe clasificar los mensajes por categorías.

REMEN5.1. El sistema debe permitir la filtración de conversaciones por categorías para pacientes.

REMEN5.2. El sistema debe permitir la filtración de conversaciones por categorías para el personal sanitario.

REMEN6. El sistema debe permitir al personal sanitario enviar notificaciones y mensajes grupales a pacientes específicos.

REMEN7. El sistema debe proporcionar opciones de configuración de privacidad y notificaciones.

REMEN7.1. El sistema debe permitir a los pacientes configurar sus preferencias de notificación.

REMEN7.2. El sistema debe permitir al personal sanitario configurar sus preferencias de notificación.

REMEN8. El sistema deberá comprobar que los usuarios están autenticados antes de realizar ninguna operación.

## 1.8.1.4 Módulo de app de avisos y mensajería

REAPP1. El sistema debe permitir a los usuarios autenticados enviar y recibir mensajes de texto a través de la aplicación.

REAPP2. El sistema deberá permitir al personal médico enviar recordatorios a los pacientes.

REAPP3. El sistema debe habilitar la recepción de avisos de salud personalizados y recordatorios de citas para los usuarios autenticados.

REAPP3.1. El sistema debe permitir a los usuarios configurar preferencias para los tipos de avisos y recordatorios que desean recibir.

REAPP3.2. El sistema debe asegurar la entrega de avisos y recordatorios en los horarios establecidos por el usuario o el personal sanitario.

REAPP4. El sistema debe proporcionar una función de notificaciones push para informar a los usuarios.

REAPP4.1 Las notificaciones push deberán poder informar sobre nuevos mensajes.

REAPP4.2 Las notificaciones push deberán poder informar sobre avisos.

REAPP5. El sistema debe permitir a los usuarios enviar archivos dentro de los mensajes.

REAPP6. El sistema debe garantizar la seguridad y privacidad de las comunicaciones.

REAPP6.1 El sistema deberá cifrar los mensajes.

REAPP6.2 El sistema deberá cifrar los archivos compartidos.

REAPP7. El sistema debe incluir opciones para que los usuarios gestionen su perfil dentro de la aplicación.

REAPP7.1 Los usuarios podrán actualizar su información personal.

REAPP7.2 Los usuarios podrán actualizar sus preferencias de contacto.

REAPP8. El sistema debe soportar un sistema de ayuda dentro de la aplicación para asistir a los usuarios en la resolución de dudas.

## 1.8.1.5 Módulo de sistema de geoposicionamiento

REGEO1. El sistema debe permitir la geolocalización en tiempo real de los vehículos de emergencia.

REGEO2. El sistema deberá almacenar los perfiles de vehículos de emergencia.

REGEO2.1 El sistema deberá almacenar el código de identificación del vehículo.

REGEO2.2 El sistema deberá almacenar el código de identificación del conductor.

REGEO2.3 El sistema deberá almacenar la matrícula del vehículo.

REGEO3. El sistema deberá almacenar los datos de la ubicación de los vehículos de emergencia en un histórico.

REGEO4. El sistema debe cifrar los datos de geolocalización durante su transmisión y almacenamiento.

## 1.8.1.6 Módulo de dashboard de seguimiento

REDASH1. El sistema debe proporcionar un panel de control en tiempo real que mostrará los siguientes datos.

REDASH1.1. Las alertas activas.

REDASH1.2. La ubicación de los vehículos de emergencia.

REDASH1.3. Los datos de los pacientes.

REDASH2. El sistema debe permitir al personal de emergencia filtrar los datos del dashboard.

REDASH2.1. Por tipo de alerta.

REDASH2.2 Por tipo de paciente.

REDASH2.3 Por estado del vehículo de emergencia.

REDASH3. El sistema debe integrar datos de geoposicionamiento, permitiendo la visualización de mapas detallados con las ubicaciones actuales.

REDASH3.1 El sistema debe mostrar las ubicaciones de los vehículos de emergencia.

REDASH3.2 El sistema debe mostrar las ubicaciones de los pacientes.

## 1.8.1.7 Módulo de app de gestión de emergencias

REEMER1. El sistema debe permitir al personal de emergencia recibir alertas de usuarios en tiempo real.

REEMER2. El sistema debe habilitar la visualización de la información de contacto y médica esencial del usuario que emite una alerta para una rápida evaluación.

REEMER2.1. El sistema debe mostrar automáticamente la información médica crítica del usuario en alerta.

REEMER2.1.1 Alergias.

REEMER2.1.2 Condiciones preexistentes.

REEMER2.2. El sistema debe proporcionar acceso rápido a los contactos de emergencia del usuario.

REEMER3. El sistema debe permitir al personal de emergencia comunicarse directamente con el usuario.

REEMER4. El sistema deberá permitir al personal de emergencia comunicarse con los conductores de los vehículos de emergencia.

REEMER5. El sistema debe permitir la asignación y gestión de recursos de emergencia para responder a las alertas.

REEMER5.1. El sistema debe permitir la asignación de vehículos de emergencia a incidentes específicos.

REEMER5.2. El sistema debe permitir al personal de emergencia registrar el estado de los recursos asignados.

REEMER5.2.1 En ruta.

REEMER5.2.2 En el lugar.

REEMER5.2.3 Disponible.

REEMER5.2.4 Ocupado.

REEMER6. El sistema debe ofrecer un historial de las alertas y su respuesta de emergencia.

REEMER7. El sistema debe cifrar las comunicaciones durante las emergencias.

## 1.8.1.8 Módulo de middleware de mensajería

REMIDMES1. El sistema debe permitir la comunicación entre los siguientes modulos.

REMIDMES1.1 La gestión de usuarios.

REMIDMES1.1 El dashboard de seguimiento.

REMIDMES1.1 El sistema de geoposicionamiento.

REMID2. El sistema debe asegurar la seguridad de los mensajes, implementando cifrado de extremo a extremo.

## 1.8.1.9 Módulo de middleware de geoposicionamiento

REMIDGEO1. El sistema debe permitir la comunicación entre los siguientes modulos.

REMIDGEO1.1 El sistema de geoposicionamiento.

REMIDGEO1.1 El dashboard de seguimiento.

REMGEO2. El sistema debe soportar la integración con datos provenientes de GPS.

REMGEO3. El sistema debe asegurar la seguridad de los datos de geoposicionamiento, implementando cifrado de extremo a extremo.

## 1.8.2 Requisitos no funcionales

RNF1. El sistema debe estar disponible en constante funcionamiento, con una disponibilidad del 99.9% fuera de los periodos programados de mantenimiento.

RNF2. El sistema de tratamiento de datos tiene que seguir el reglamento general de protección de datos. (RGDP)

RNF3. La aplicación móvil para los clientes debe ser compatible con Android y IOS.

RNF4. El módulo de integración con sistemas centrales debe soportar el estándar de interoperabilidad de salud HL7.

RNF5. Los tiempos de respuesta de los sistemas integrados deberán ser menores a 500 milisegundos.

RNF6. Tras 30 minutos de uso, los usuarios deberán estar completamente familiarizados con todas las funciones de la aplicación móvil.

RNF7. Debe cumplir con los estándares de accesibilidad web WCAG 2.1 nivel AA como mínimo, asegurando que el sistema sea utilizable por personas con distintas capacidades.

RNF8. Todos los datos transmitidos y almacenados deben ser cifrados utilizando estándares de cifrado actuales.

RNF9. El sistema debe implementar autenticación de dos factores para el acceso de usuarios críticos.