

Especificación de los requerimientos

1. Funcionales

RF-01: El sistema debe permitir a los usuarios registrarse con RUT, correo electrónico, contraseña, confirmación de contraseña, nombre de usuario y dirección (región y comuna). Los roles son Usuario y Administrador.

RF-01.1: El sistema debe permitir a los usuarios iniciar sesión con correo electrónico y contraseña.

RF-01.2: El sistema debe validar que el correo electrónico ingresado tenga un formato válido, es decir contener una arroba seguida de un dominio.

RF-01.3: El sistema debe permitir al usuario definir una contraseña que cumpla con las políticas de seguridad, es decir tener una longitud mínima de 8 caracteres y contener al mínimo un número, una mayúscula y una minúscula.

RF-01.4: El sistema debe asignar permisos de acceso según el rol asociado (Usuario o Administrador).

RF-01.5: El sistema debe permitir al usuario desconectarse.

RF-02: El sistema debe permitir a los administradores visualizar y modificar los datos o el rol de un usuario.

RF-02.1: El sistema debe permitir a los administradores visualizar la lista de los usuarios y anuncios denunciados.

RF-02.2: El sistema debe permitir a los administradores suspender un usuario en caso de abuso.

RF-02.3: El sistema debe permitir a los administradores eliminar un anuncio si contiene contenido inapropiado.

RF-03: El sistema debe permitir al usuario proponer un producto a la donación. El anuncio asociado debe contener al mínimo un título, una descripción, un estado de desgaste, una imagen y un perímetro geográfico de recuperación del producto.

RF-03.1: El sistema debe permitir al usuario elegir entre los estados de desgaste siguientes: Nuevo, Como nuevo, Buen estado, Estado aceptable, Desgastado, A reparar.

RF-03.2: El sistema debe permitir al usuario agregar un máximo de 5 imágenes a cada anuncio.

RF-03.3: El sistema debe limitar la longitud del título ingresado a 50 caracteres.

RF-03.4: El sistema debe limitar la longitud de la descripción ingresada a 500 caracteres.

RF-03.5: El sistema debe permitir al autor de un anuncio modificar y eliminarlo.

RF-04: El sistema debe tener un sistema de mensajería para que los usuarios pongan ponerse en contacto.

RF-04.1: El módulo de mensajería debe permitir al usuario iniciar una conversación con otro usuario a través de un anuncio solamente.

RF-04.2: El módulo de mensajería debe permitir al usuario responder a una conversación existente.

RF-04.3: El módulo de mensajería debe permitir al usuario bloquear a otro usuario.

RF-04.4: El módulo de mensajería debe guardar un histórico de los mensajes entre dos usuarios. Este histórico no está limitado en el tiempo.

RF-04.5: El sistema debe enviar notificaciones push en caso de nuevos mensajes recibidos.

RF-05: El sistema debe permitir al usuario marcar un anuncio como favorito.

RF-05.1: El sistema debe permitir al usuario visualizar todos sus anuncios favoritos.

RF-05.2: El sistema debe permitir al usuario eliminar un anuncio de la lista de sus anuncios favoritos.

RF-06: El sistema debe permitir la búsqueda de productos con un título.

RF-07: El sistema debe permitir al usuario modificar sus datos personales.

RF-07.1: El sistema debe permitir al usuario eliminar su cuenta.

RF-08: El sistema debe permitir a los usuarios denunciar un anuncio (contenido inapropiado, fraude).

RF-09: El sistema debe enviar notificaciones push (nuevos mensajes).

II. No Funcionales

RNF-01: La aplicación debe ser compatible con los sistemas operativos Android 5.1+ e iOS 14.0+.

RNF-02: El sistema debe responder a cualquier acción crítica (registro, inicio de sesión, búsqueda de anuncios, envío de mensajes) en un tiempo máximo de 3 segundos bajo condiciones normales de red 4G/Wi-Fi.

RNF-03: La aplicación debe ser desarrollada en Ionic con Angular y TypeScript para garantizar mantenibilidad y reutilización de componentes.

RNF-04: La aplicación debe cumplir con las normas de accesibilidad WCAG 2.1 nivel AA (uso de lectores de pantalla, contraste, navegación por teclado, textos alternativos en imágenes).

RNF-05: La aplicación debe utilizar íconos apropiados y estandarizados (Material Design / iOS Human Interface Guidelines) para facilitar la comprensión de la interfaz.

RNF-06: El sistema debe proporcionar documentación técnica (arquitectura, API, base de datos) y documentación funcional (manual de usuario, manual de administrador).

RNF-07: El sistema debe proteger la API contra ataques de inyección SQL y XSS mediante validación de entradas y sanitización de datos.

RNF-08: El sistema debe implementar una configuración CORS segura que restrinja los orígenes permitidos según los dominios autorizados.

RNF-09: El sistema debe encriptar las contraseñas y datos sensibles utilizando el algoritmo bcrypt con un nivel de complejidad adecuado.

RNF-10: El sistema debe incluir un Dockerfile para el backend que permita su construcción y despliegue independiente.

RNF-10.1: La aplicación debe incluir un Dockerfile para el frontend que garantice su portabilidad y consistencia en diferentes entornos.

RNF-10.2: El sistema debe configurar un archivo docker-compose que orqueste los servicios de la API, la base de datos y el frontend.

RNF-10.3: El sistema debe permitir la ejecución de pruebas de despliegue local mediante Docker para validar la correcta integración de los servicios.

RNF-11: El sistema debe implementar autenticación basada en tokens JWT para los procesos de inicio de sesión y registro.

RNF-11.1: El sistema debe firmar los tokens JWT utilizando un algoritmo seguro (por ejemplo, HS256 o RS256) y una clave secreta robusta.

RNF-11.2: El sistema debe definir una expiración para los tokens JWT a fin de reducir riesgos de uso indebido.

RNF-11.3: El sistema debe validar los tokens JWT en cada solicitud que requiera autenticación para garantizar la seguridad de acceso a los recursos.