



SuperTransporte

 DOCUMENTO TÉCNICO OFICIAL

Software de Gestión de Usuarios SUPERINTENDENCIA DE TRANSPORTE

Manual de Instalación y Uso - Documento técnico y funcional para despliegue, administración y operación del sistema

Versión

1.0

Fecha

18 de marzo de 2026

Contenido

Instalación, configuración, buenas prácticas y guía de uso

- ❗ Este manual puede complementarse con capturas del sistema, diagramas de flujo y evidencias de operación según el entorno de despliegue.

Contenido

Introducción

Objetivos

Metodología y buenas prácticas implementadas

Arquitectura general de la solución

Instalación del sistema

Variables de entorno y explicación de campos

Uso funcional del software

Colección Postman entregable

Recomendaciones de operación y seguridad

Conclusión

1. Introducción

El presente manual describe de manera integral el proceso de instalación, configuración, despliegue y uso del Software de Gestión de Usuarios desarrollado para fortalecer la administración de accesos, usuarios, roles, contratos y solicitudes dentro de la entidad. La solución fue concebida para centralizar la gestión de identidades y permisos, reducir tareas manuales, mejorar la trazabilidad y reforzar los controles de seguridad sobre los sistemas institucionales.

Además de documentar la instalación técnica del backend y del frontend, este manual presenta las buenas prácticas de desarrollo aplicadas en la solución, la finalidad de cada variable de entorno, el proceso de inicialización del sistema y una guía funcional de los principales módulos. De esta manera, el documento sirve tanto para el equipo de tecnología responsable del despliegue como para las áreas administrativas y operativas que harán uso de la plataforma.

SECCIÓN 2

2. Objetivos

2.1 Objetivo general

Establecer una guía clara y estandarizada para instalar, configurar, desplegar y utilizar el Software de Gestión de Usuarios, asegurando una operación segura, controlada y alineada con las necesidades administrativas y tecnológicas de la entidad.

2.2 Objetivos específicos

- Describir los requisitos técnicos mínimos para la instalación del backend y del frontend.
- Explicar la finalidad de cada variable de entorno necesaria para poner en funcionamiento la solución.
- Documentar las buenas prácticas de programación y seguridad implementadas en el software.
- Orientar a los administradores y usuarios funcionales sobre el uso de los módulos principales del sistema.
- Facilitar el proceso de despliegue en ambientes de desarrollo, pruebas y producción.
- Promover una gestión más segura y eficiente de usuarios, contratos, accesos y roles institucionales.

3. Metodología y buenas prácticas implementadas

El desarrollo del software se realizó bajo un enfoque modular, seguro y escalable, adoptando buenas prácticas de programación orientadas a la mantenibilidad del código, la protección de la información y la facilidad de despliegue. A continuación se describen las principales medidas incorporadas en la solución.

3.1 Seguridad de credenciales y configuración

Variables de entorno

Uso de variables de entorno (.env) para evitar exponer credenciales sensibles dentro del código fuente.

Separación por ambiente

Separación de datos de configuración por ambiente, permitiendo definir valores distintos para desarrollo, pruebas y producción.

Control de versiones

Recomendación de no versionar archivos .env con credenciales reales dentro del repositorio.

3.2 Protección de contraseñas

Hash con bcrypt

Implementación de hash con bcrypt para el almacenamiento seguro de contraseñas.

Sin texto plano

Las credenciales no deben guardarse en texto plano, lo que reduce el riesgo ante accesos no autorizados a la base de datos.

Política de cambio

Se recomienda establecer políticas de cambio de contraseña para cuentas administrativas luego del despliegue inicial.

3.3 Acceso a datos y persistencia

ORM estructurado

Uso de ORM para interactuar con la base de datos de manera estructurada y mantenible.

Reducción de errores

Reducción del riesgo de errores manuales en consultas SQL y mejora en la legibilidad del código.

Consistencia

Facilidad para mantener entidades, relaciones y lógica de negocio de forma consistente.

3.4 Buenas prácticas adicionales



Separación de responsabilidades

Separación de responsabilidades entre módulos, servicios y controladores.



Validación de datos

Validación de datos de entrada antes de procesarlos.



Gestión de roles y permisos

Gestión de roles y permisos para restringir funcionalidades según el perfil del usuario.



Registro y monitoreo

Registro y monitoreo de eventos relevantes para trazabilidad y auditoría.

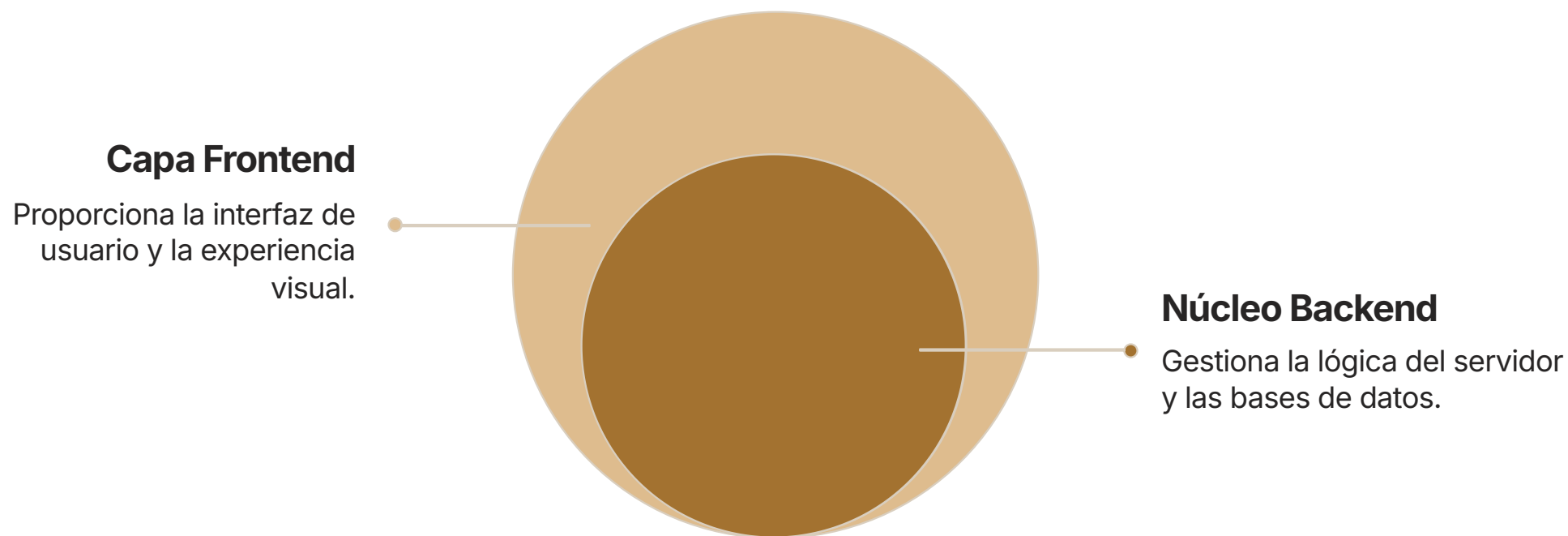


Integraciones futuras

Preparación de la aplicación para integraciones posteriores con correo institucional y directorios corporativos como LDAP.

4. Arquitectura general de la solución

La solución está compuesta por un backend desarrollado con NestJS y un frontend desarrollado con Next.js. Esta combinación permite disponer de una arquitectura moderna, robusta y escalable, adecuada para aplicaciones empresariales que requieren modularidad, seguridad y facilidad de mantenimiento.



4.1 Ventajas de NestJS en el backend



Arquitectura modular

Arquitectura modular que facilita la organización del proyecto por dominios o funcionalidades.



Soporte nativo para TypeScript

Soporte nativo para TypeScript, mejorando tipado, mantenibilidad y detección temprana de errores.



Inyección de dependencias

Inyección de dependencias para una estructura más limpia y desacoplada.



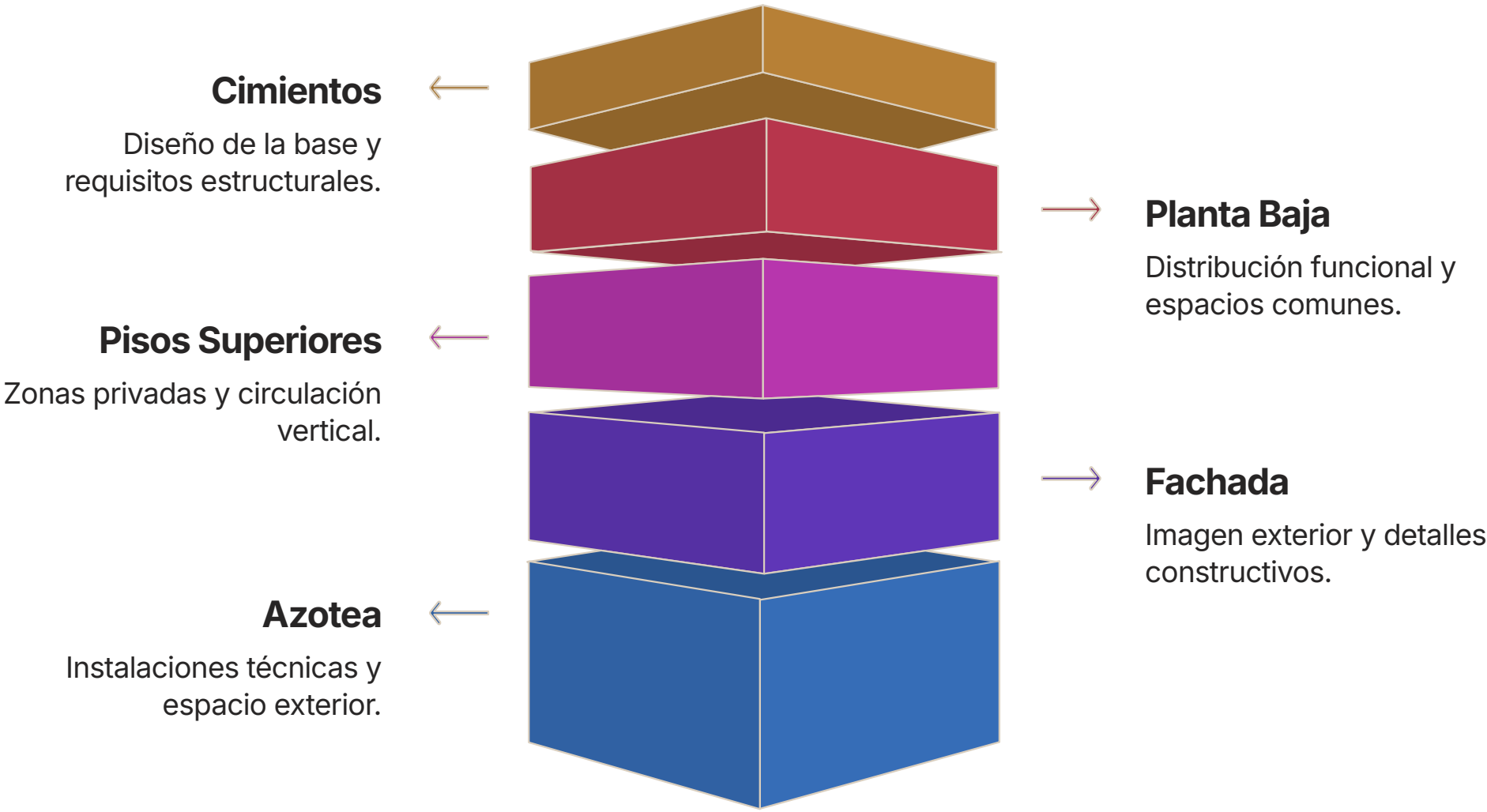
Guards, pipes e interceptors

Facilidad para implementar controladores, servicios, guards, pipes e interceptors orientados a seguridad y validación.



APIs empresariales escalables

Adecuado para APIs empresariales escalables y mantenibles.



4.2 Ventajas de Next.js en el frontend



Framework moderno basado en React

Framework moderno basado en React con estructura organizada y alta productividad.



Renderizado eficiente

Soporte para renderizado eficiente y optimización del rendimiento.



Rutas y componentes reutilizables

Manejo claro de rutas y componentes reutilizables.



Paneles administrativos corporativos

Buena experiencia para construir paneles administrativos y aplicaciones web corporativas.



Configuración por ambiente

Facilidad para configuración por ambiente mediante variables de entorno.

- ❗ En conjunto, ambas tecnologías permiten desarrollar una plataforma alineada con necesidades institucionales, con capacidad de crecer, integrar nuevos módulos y fortalecer el control sobre la gestión de usuarios y accesos.

5. Instalación del sistema

Antes de iniciar la instalación, se recomienda contar con un servidor o equipo que disponga de acceso a internet para descarga de dependencias, permisos para crear bases de datos y capacidad para ejecutar servicios Node.js. El despliegue puede realizarse en ambientes locales, de pruebas o de producción, ajustando las variables de entorno correspondientes.

Ambiente local

Desarrollo y pruebas en equipo local con variables de entorno de desarrollo.

Ambiente de pruebas

Entorno de QA con configuración diferenciada para validación funcional.

Ambiente de producción

Despliegue final con credenciales y configuración de producción segura.

5.1 Backend (NestJS) - Requisitos previos



Node.js LTS

Node.js instalado en versión LTS recomendada.



npm

npm disponible para la instalación de dependencias.



MySQL

Motor de base de datos MySQL instalado y accesible.



Correo SMTP

Acceso a una cuenta de correo SMTP para el envío de notificaciones.



Código fuente

Código fuente del backend entregado en el paquete del proyecto.

Backend - Pasos de instalación del Backend



Ubicar el proyecto

Ubicar el proyecto backend en el servidor o equipo de despliegue.



Instalar dependencias

Instalar las dependencias ejecutando el comando `npm install` dentro de la carpeta del backend.



Crear base de datos

Crear la base de datos MySQL que será utilizada por la aplicación.



Configurar .env

Configurar el archivo `.env` con los valores del entorno de despliegue.



Ejecutar seeder

Ejecutar el seeder inicial mediante el comando `npm run seed`.



Levantar la aplicación

Levantar la aplicación en ambiente de desarrollo o compilarla para producción según corresponda.

Backend — Ejemplo de archivo .env para Backend

Una vez configurado el archivo .env, el backend podrá conectarse a la base de datos y al servicio de correo utilizado para alertas y notificaciones. Los valores deben ajustarse de acuerdo con el servidor, puertos y credenciales definidos por la entidad.

```
APP_HOST = localhost
APP_PORT = 3052
BASE_URL = http://localhost:3050
```

```
DB_DIALECT = mysql
DB_HOST =
DB_PORT =
DB_DATABASE =
DB_USERNAME =
DB_PASSWORD =
```

```
MAIL_SERVER=smtp.hostinger.com
MAIL_PORT=465
MAIL_USER=""
MAIL_PASSWORD=""
```

```
ALLOWED_EMAIL_DOMAINS=@supertransporte.gov.co
```

Backend - Seeder inicial

El sistema incluye un seeder que puede ejecutarse mediante el siguiente comando:

```
npm run seed
```

Este proceso crea un usuario inicial de pruebas con perfil administrador, con los siguientes datos de acceso:

Nombre	test
Correo	test@gmail.com
Contraseña	Darkmoon132@
Rol	Administrador

 Por seguridad, se recomienda cambiar esta contraseña inmediatamente después de la primera puesta en marcha en un entorno real.

Backend - Compilación para producción

Para generar la versión compilada del backend en ambiente de producción, se debe ejecutar el siguiente comando:

```
npm run build
```

- ☑ Este comando prepara el proyecto para su despliegue en producción, generando los archivos necesarios para una ejecución optimizada.

5.2 Frontend (Next.js)

El frontend del sistema fue construido con Next.js. Para su instalación, se recomienda contar igualmente con Node.js y npm. Después de copiar el proyecto al entorno de trabajo, se deben instalar las dependencias y configurar su respectivo archivo .env para apuntar al backend correspondiente.

Pasos de instalación del frontend



Ubicar el proyecto

Ubicar el proyecto frontend en el servidor o equipo local.



Instalar dependencias

Instalar dependencias con el comando `npm install`.



Crear archivo .env

Crear el archivo .env del frontend con las variables requeridas por el proyecto, por ejemplo la URL pública del backend.



Verificar conectividad

Verificar la conectividad con la API antes de publicar el sistema.



Compilar o ejecutar

Compilar o ejecutar el frontend según el entorno definido por el equipo técnico.

Ejemplo referencial de variable principal en frontend:

```
NEXT_PUBLIC_ENCRYPTION_KEY = key_encryptado
```

```
NEXT_PUBLIC_BACK_URL = https://backiam.vialcode.dev/api
```

- ✓ El nombre exacto de las variables del frontend puede variar según la implementación entregada. No obstante, el objetivo principal es asegurar que la interfaz apunte al backend correcto en cada ambiente.

SECCIÓN 6

6. Variables de entorno y explicación de campos

Las variables de entorno permiten parametrizar la aplicación sin modificar el código fuente. Esto facilita el despliegue entre ambientes y reduce la exposición de información sensible. A continuación se explica la finalidad de cada campo suministrado para el backend.

6. Variables de entorno - Aplicación y Base de datos

Variable	Tipo	Descripción
APP_HOST	Aplicación	Host o interfaz en la que escuchará el backend. En entornos locales suele utilizarse localhost.
APP_PORT	Aplicación	Puerto en el que se ejecutará el backend.
BASE_URL	Aplicación	URL base pública o de referencia utilizada por la aplicación para accesos, enlaces o consumo desde el frontend.
DB_DIALECT	Base de datos	Motor o dialecto de base de datos utilizado por la aplicación. En este caso: mysql.
DB_HOST	Base de datos	Dirección del servidor donde se encuentra la instancia MySQL.
DB_PORT	Base de datos	Puerto de conexión del servicio MySQL.
DB_DATABASE	Base de datos	Nombre de la base de datos que utilizará la aplicación.
DB_USERNAME	Base de datos	Usuario con permisos para conectarse a la base de datos.
DB_PASSWORD	Base de datos	Contraseña del usuario de la base de datos.

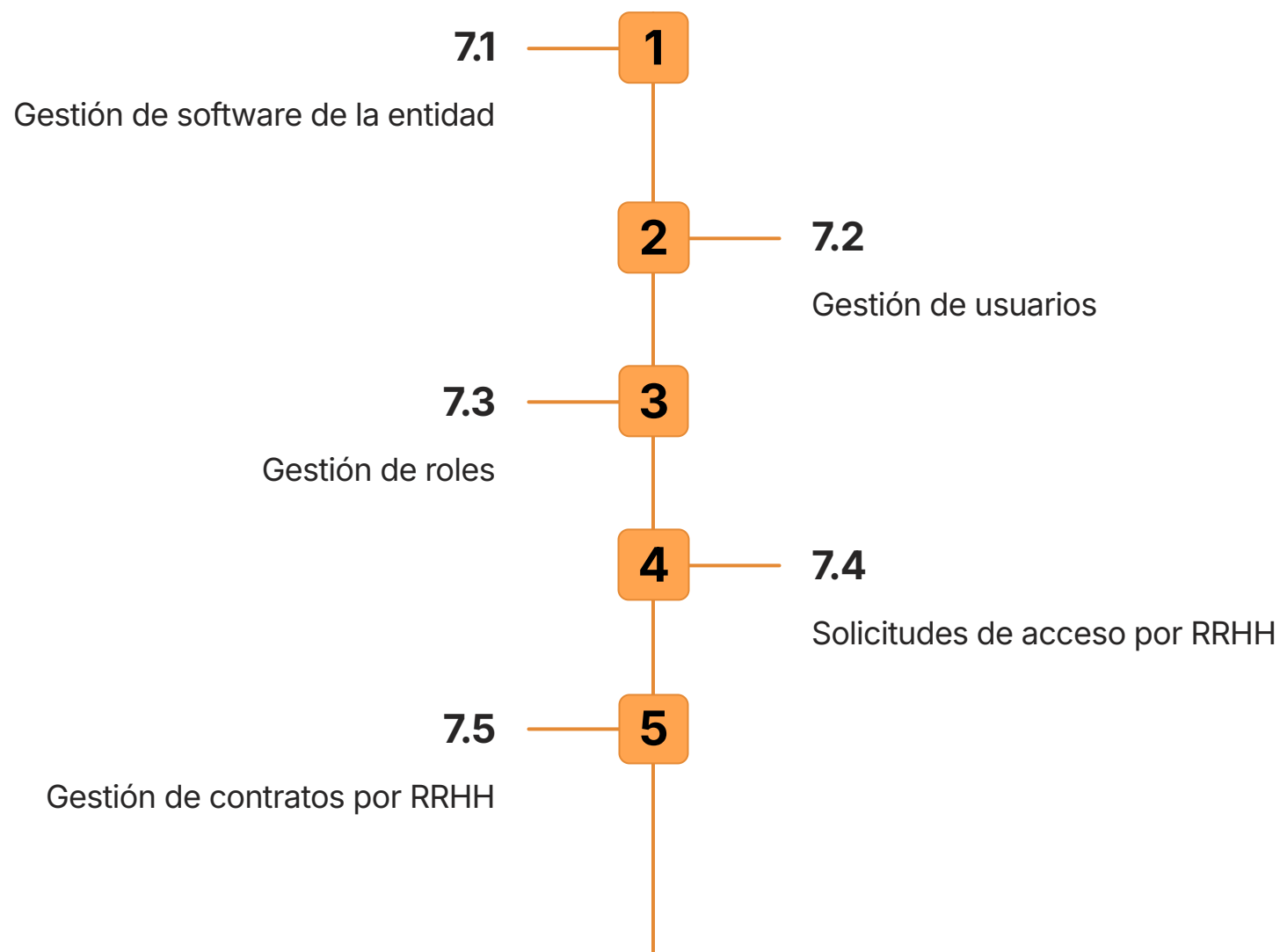
6. Variables de entorno — Correo y Restricción

Variable	Tipo	Descripción
MAIL_SERVER	Correo	Servidor SMTP encargado del envío de correos de notificación y alertas.
MAIL_PORT	Correo	Puerto del servicio SMTP. En el ejemplo entregado se utiliza 465.
MAIL_USER	Correo	Cuenta de correo autorizada para el envío de mensajes desde la plataforma.
MAIL_PASSWORD	Correo	Contraseña o credencial asociada a la cuenta SMTP.
ALLOWED_EMAIL_DOMAINS	Restricción	Dominio permitido para el registro de usuarios. En este caso se restringe a cuentas @supertransporte.gov.co para evitar registros con correos no institucionales.

 La variable ALLOWED_EMAIL_DOMAINS tiene un propósito de control de acceso. Su función es permitir el registro únicamente de cuentas pertenecientes al dominio institucional autorizado, ayudando a prevenir registros de correos externos y fortaleciendo el gobierno de identidades.

7. Uso funcional del software

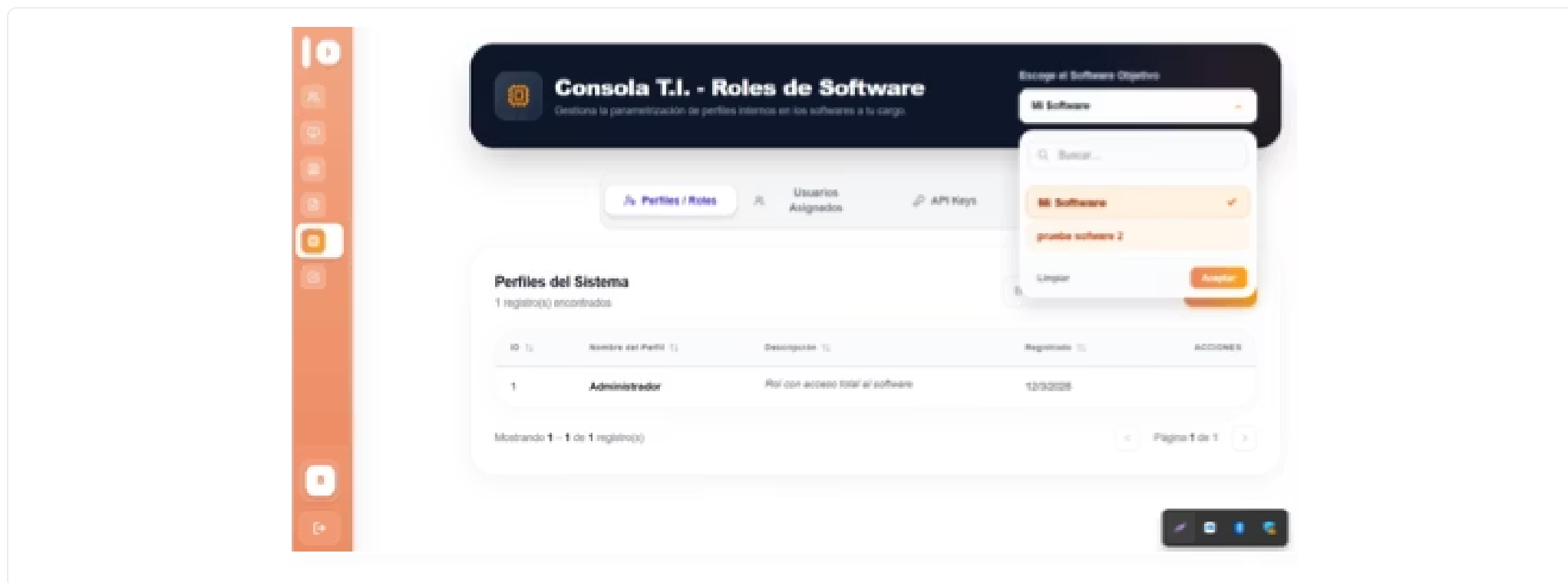
El Software de Gestión de Usuarios fue diseñado para apoyar la administración y la seguridad de la gestión de usuarios dentro de la entidad. A nivel funcional, la plataforma permite centralizar procesos que normalmente se ejecutan de forma dispersa, manual o sin una trazabilidad completa. A continuación se describen los módulos y capacidades principales del sistema.



7.1 Gestión de software de la entidad

Permite registrar, organizar y administrar los sistemas o plataformas institucionales que serán controlados desde la solución. Este módulo sirve como base para relacionar usuarios, roles, solicitudes y accesos sobre cada software administrado.

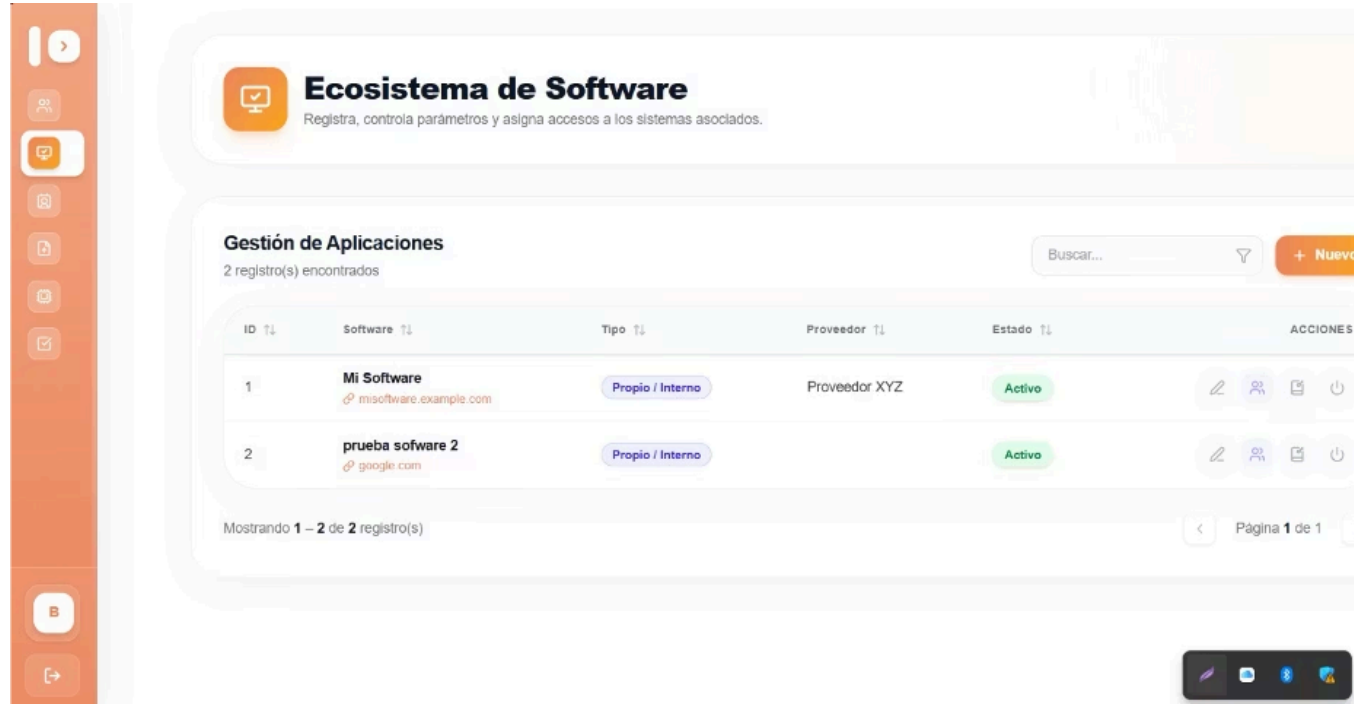
Evidencia sugerida: 7.1 Gestión de software de la entidad



7.2 Gestión de usuarios

Facilita la creación, consulta, edición y seguimiento de usuarios vinculados a la institución, centralizando su información básica y su relación con contratos, accesos y estados dentro de la plataforma.

Evidencia sugerida: 7.2 Gestión de usuarios



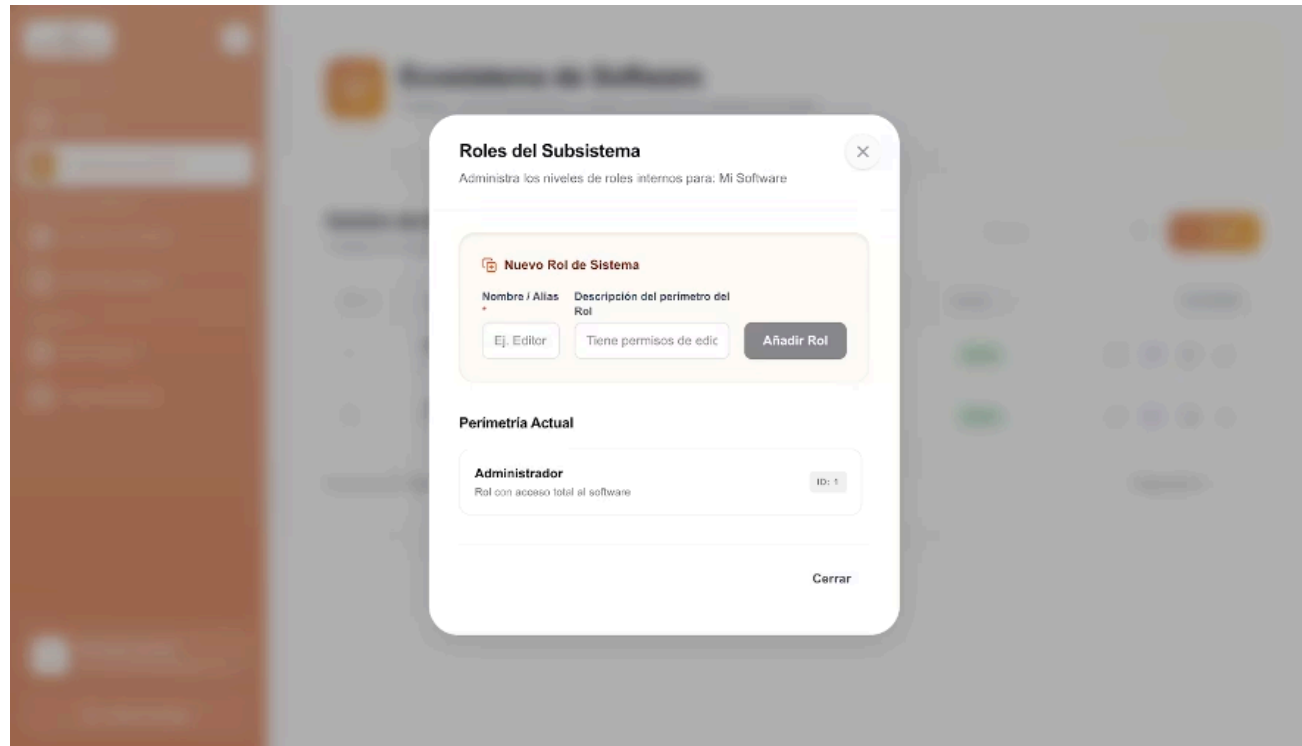
The screenshot displays a web application interface for managing software. On the left is a vertical orange sidebar with icons for home, users, applications, settings, reports, and a search function. The main content area is titled 'Ecosistema de Software' with a subtitle 'Registra, controla parámetros y asigna accesos a los sistemas asociados.' Below this is a section for 'Gestión de Aplicaciones' showing '2 registro(s) encontrados'. It includes a search bar, a '+ Nuevo' button, and a table with columns: ID, Software, Tipo, Proveedor, Estado, and ACCIONES. The table lists two items: 'Mi Software' (misoftware.example.com) and 'prueba software 2' (google.com), both marked as 'Propio / Interno' and 'Activo'. At the bottom, it shows 'Mostrando 1 - 2 de 2 registro(s)' and 'Página 1 de 1'. A mobile status bar is visible at the very bottom.

ID	Software	Tipo	Proveedor	Estado	ACCIONES
1	Mi Software misoftware.example.com	Propio / Interno	Proveedor XYZ	Activo	[Edit] [Add User] [Add Role] [Power]
2	prueba software 2 google.com	Propio / Interno		Activo	[Edit] [Add User] [Add Role] [Power]

7.3 Gestión de roles

Permite administrar perfiles de acceso y permisos de acuerdo con las responsabilidades de cada usuario. Esto contribuye a aplicar el principio de mínimo privilegio y a controlar mejor las acciones autorizadas dentro del sistema.

Evidencia sugerida: 7.3 Gestión de roles



7.4 Solicitudes de acceso por parte de Recursos Humanos

El sistema permite que el área de Recursos Humanos integre o solicite acceso para usuarios a los diferentes sistemas institucionales, mejorando la coordinación con el área de tecnología y manteniendo trazabilidad sobre cada requerimiento.

Evidencia sugerida: 7.4 Solicitudes de acceso por parte de Recursos Humanos

The screenshot displays a web application interface for managing software requests. On the left is an orange sidebar with navigation icons. The main content area is divided into two sections. The top section, titled 'Solicitudes de Software', includes a description, three action buttons ('Descargar Plantilla', 'Carga Masiva', 'Solicitud Manual'), and a dropdown menu for selecting software. The bottom section, titled 'Historial de Solicitudes', shows a table with two records. A search bar is located above the table, and a pagination bar is at the bottom right.

Solicitudes de Software
Gestiona las solicitudes de acceso al software, carga masiva de Excel o crea solicitudes manualmente.

Selecccionar Software
prueba software 2

Descargar Plantilla Carga Masiva Solicitud Manual

Historial de Solicitudes
2 registro(s) encontrados

Buscar por nombre, cédula

ID	Usuario Solicitante	Cédula	Acción	Rol Solicitado	Estado	Solicitado por	ACCIONES
5	John Doe	12345678	CREATE	Recurso h	✓ Activo/Aprobado	Brandon llamas	👁️ ⌚
4	tes	123333	CREATE	Admin	✗ Rechazado/Inactivo	—	👁️ ⌚

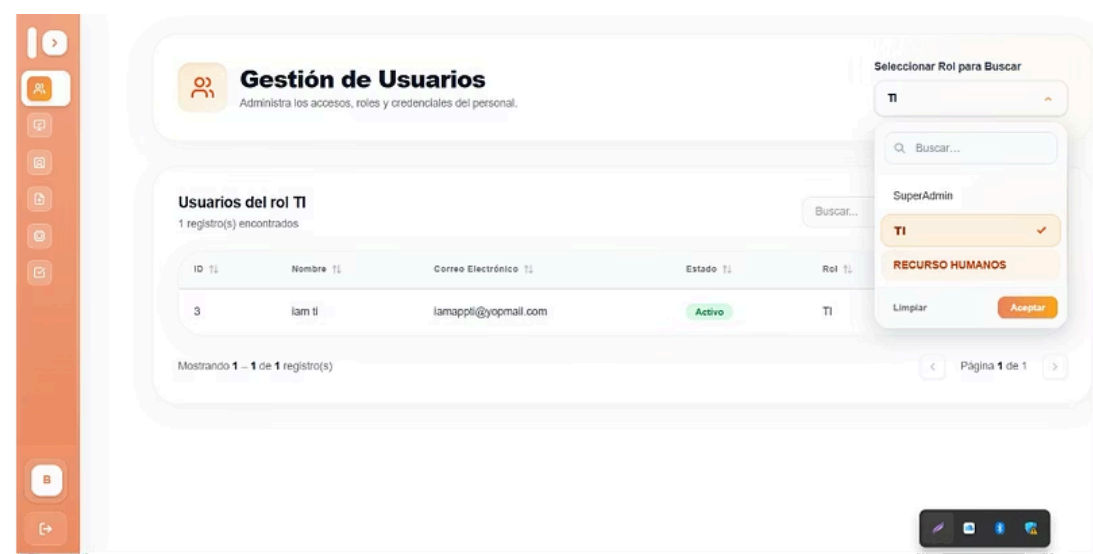
Mostrando 1 – 2 de 2 registro(s)

Página 1 de 1

7.5 Gestión de contratos y usuarios por Recursos Humanos

Hace posible que Recursos Humanos gestione contratos y relacione su vigencia con los usuarios de la institución, ayudando a mantener actualizada la información administrativa que impacta el control de accesos.

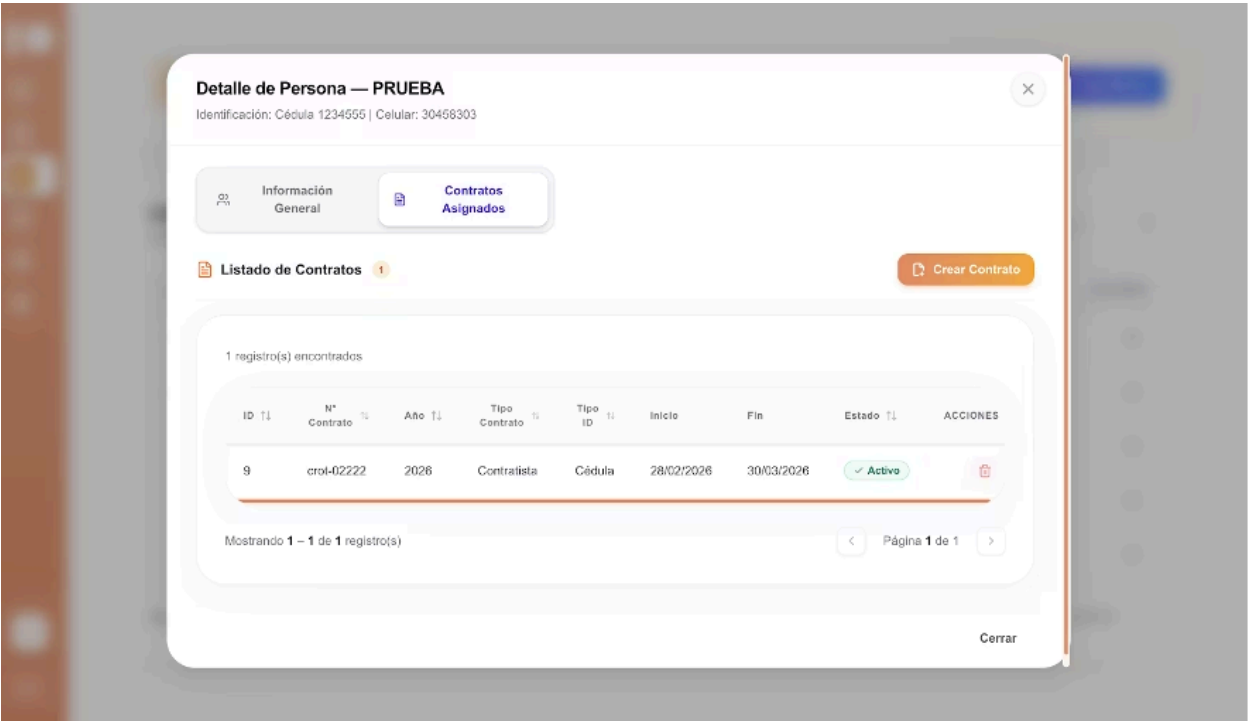
Evidencia sugerida: 7.5 Gestión de contratos y usuarios por Recursos Humanos



7.6 Consulta de usuarios activos con contratos

Permite visualizar los usuarios activos dentro de las plataformas que además poseen contratos asociados, facilitando revisiones de vigencia, control administrativo y validación operativa.

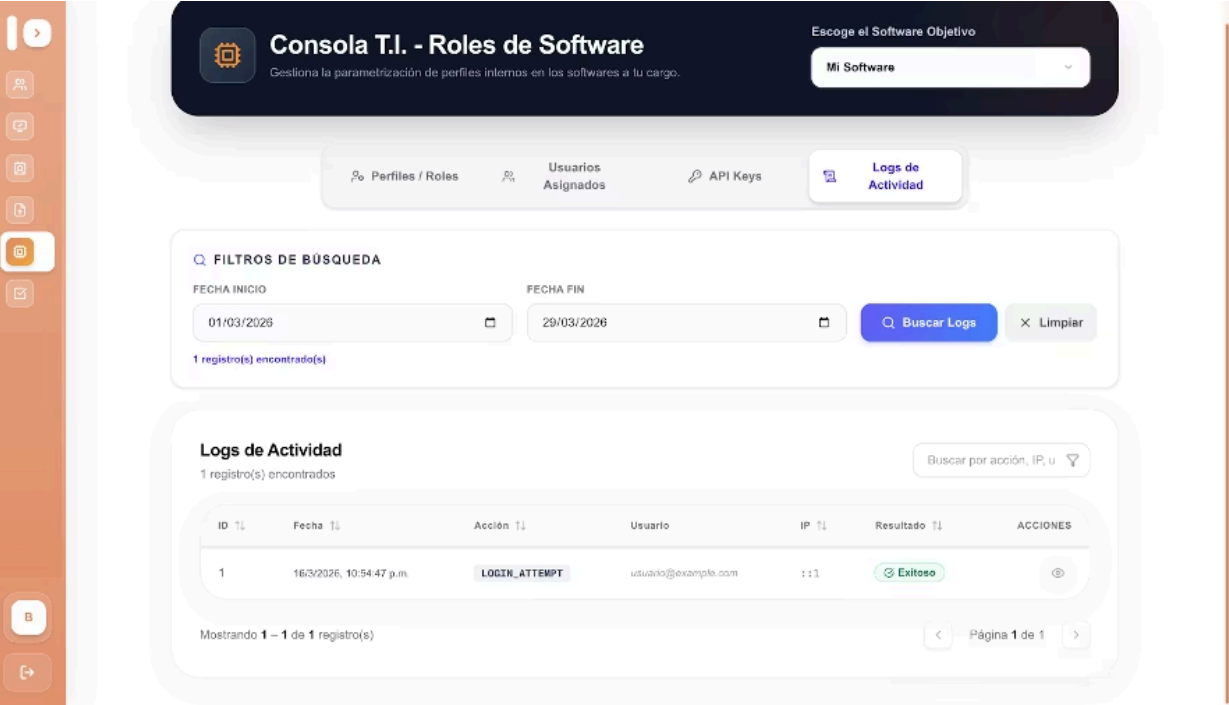
Evidencia sugerida: 7.6 Consulta de usuarios activos con contratos



7.7 Gestión de logs por parte de TI

El área de tecnología puede gestionar y revisar logs de aplicaciones, siempre que los sistemas actuales sean integrados con la plataforma. Esto fortalece la trazabilidad, el monitoreo y la capacidad de auditoría.

Evidencia sugerida: 7.7 Gestión de logs por parte de TI



The screenshot displays the 'Consola T.I. - Roles de Software' interface. The top navigation bar includes a dropdown menu for 'Escoge el Software Objetivo' set to 'Mi Software'. Below this, there are tabs for 'Perfiles / Roles', 'Usuarios Asignados', 'API Keys', and 'Logs de Actividad'. The 'Logs de Actividad' section features a search filter area with 'FECHA INICIO' (01/03/2026) and 'FECHA FIN' (29/03/2026) fields, a 'Buscar Logs' button, and a 'Limpiar' button. Below the search filters, it indicates '1 registro(s) encontrado(s)'. The 'Logs de Actividad' section shows a table with the following data:

ID TI	Fecha TI	Acción TI	Usuario	IP TI	Resultado TI	ACCIONES
1	16/3/2026, 10:54:47 p.m.	LOGIN_ATTEMPT	usuario@example.com	::1	Exitoso	

At the bottom of the table, it states 'Mostrando 1 - 1 de 1 registro(s)' and 'Página 1 de 1'.

7.8 Alertas sobre contratos no vigentes y usuarios activos

La solución puede enviar alertas sobre contratos vencidos asociados a usuarios que aún permanecen activos. Para esta funcionalidad se requiere un correo configurado para alertas y la integración con LDAP u otros directorios definidos por la institución.

Evidencia sugerida: 7.8 Alertas sobre contratos no vigentes y usuarios activos

Alerta - Usuarios con contrato vencido en software Mi Software

 Deliverability  Responder  Trasladar  Imprimir  Eliminar

 miércoles, 18 de marzo de 2026 16:00:05

Usuarios sin desactivar (Contrato Vencido)

Estimados administradores y equipo de TI / RRHH,

El siguiente es un listado de usuarios que **aún se encuentran activos** en el software **Mi Software**, pero su contrato registra como **Vencido**:

Nombre	Cédula/NIT	Email	Fecha Vencimiento Contrato
John Doe	12345678		12/31/2024
John Doe	12345678		12/31/2024

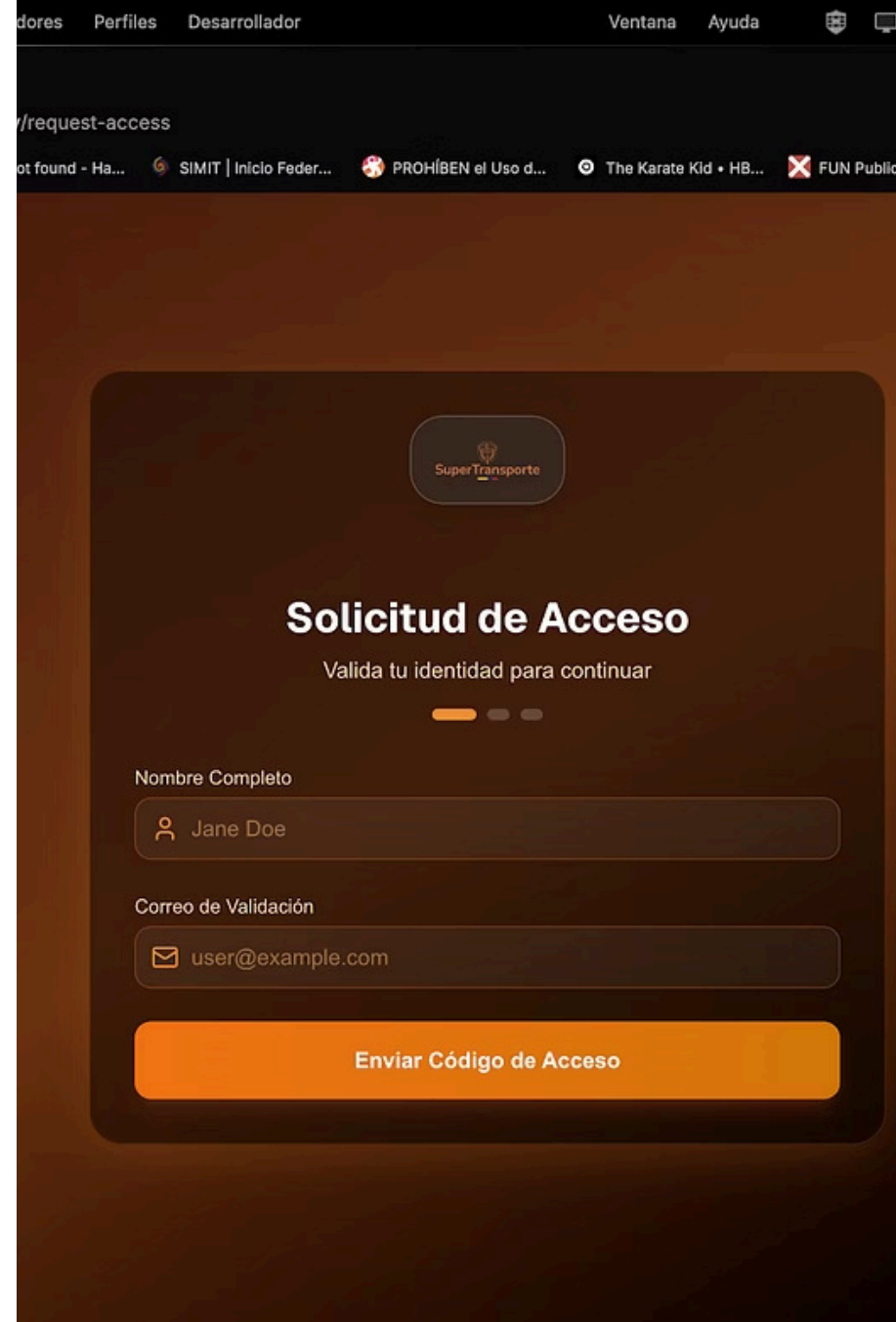
Por favor, procedan a verificar y desactivar estos usuarios en el sistema IAM o directamente en el software según corresponda.

Este correo ha sido generado automáticamente de forma genérica por el Sistema IAM.
Por favor, no responda a este mensaje ya que este buzón no es supervisado.

7.9 Solicitudes de acceso por parte de trabajadores

Los trabajadores pueden solicitar acceso a plataformas desde un flujo controlado, lo que reduce procesos informales y mejora la gestión centralizada de aprobaciones.

Evidencia sugerida: 7.9 Solicitudes de acceso por parte de trabajadores



The screenshot shows a web browser window with the URL `/request-access`. The browser's address bar and tabs are visible at the top. The main content area displays a dark-themed form titled "Solicitud de Acceso" (Access Request) with the subtitle "Valida tu identidad para continuar" (Validate your identity to continue). The form includes a "SuperTransporte" logo at the top. Below the title, there are two input fields: "Nombre Completo" (Full Name) with the value "Jane Doe" and "Correo de Validación" (Validation Email) with the value "user@example.com". At the bottom of the form is a large orange button labeled "Enviar Código de Acceso" (Send Access Code).

dores Perfiles Desarrollador Ventana Ayuda

/request-access

ot found - Ha... SIMIT | Inicio Feder... PROHÍBEN el Uso d... The Karate Kid • HB... FUN Publico

SuperTransporte

Solicitud de Acceso

Valida tu identidad para continuar

Nombre Completo

Jane Doe

Correo de Validación

user@example.com

Enviar Código de Acceso

7.10 Aprobación o desaprobación por parte de TI

El equipo de TI puede aprobar o desaprobar solicitudes de acceso dentro de la plataforma, dejando trazabilidad sobre la decisión y fortaleciendo el control sobre el ciclo de vida de los accesos.

Evidencia sugerida: 7.10 Aprobación o desaprobación por parte de TI

Aprobación de Solicitudes
Revisa, aprueba o rechaza las solicitudes pendientes de acceso a tus aplicaciones a cargo.

Seleccionar Software
Mi Software

Solicitudes
5 registro(s) encontrados

Buscar por nombre o rol...

ID	Usuario Solicitante	Acción	Rol Solicitado	Estado	Solicitado por	Gestión
7	John Doe	CREATE	Administrador	Pendiente	recursos humanos	👁️ 🗑️ 💬 ⌚
6	PRUEBA	CREATE	Administrador	Activo/Aprobado	—	👁️ ⌚
3	John Doe	UPDATE	Administrador	Activo/Aprobado	Brandon Iliamas	👁️ ⌚
2	km	CREATE	Administrador	Rechazado/inactivo	—	👁️ ⌚
1	John Doe	CREATE	Administrador	Activo/Aprobado	Brandon Iliamas	👁️ ⌚

Mostrando 1 – 5 de 5 registro(s)

7.11 Flujo básico de uso recomendado



Registrar softwares

Registrar o verificar los softwares institucionales que serán administrados.



Crear usuarios

Crear o sincronizar usuarios de acuerdo con la estructura organizacional.



Definir roles

Definir roles y permisos según el perfil de cada dependencia.



Registrar contratos

Registrar contratos o su vigencia cuando el proceso requiera control contractual.



Recibir solicitudes

Recibir solicitudes de acceso de Recursos Humanos o de trabajadores.



Validar y aprobar

Validar y aprobar o rechazar solicitudes desde TI.



Monitorear

Monitorear usuarios activos, contratos vigentes y alertas generadas por la plataforma.



Revisar logs

Revisar logs y trazabilidad para auditoría y seguimiento.

8. Colección Postman entregable

Como parte del entregable técnico, se incluye en el archivo comprimido (ZIP) una colección de Postman con los endpoints de la aplicación. Esta colección facilita las pruebas de conectividad, validación funcional de la API, revisión de parámetros y apoyo a procesos de integración o soporte técnico.

- ✓ Se recomienda utilizar dicha colección para verificar autenticación, administración de usuarios, roles, contratos, solicitudes y demás recursos expuestos por el backend. También puede servir como apoyo para documentación operativa y para pruebas posteriores de mantenimiento.

9. Recomendaciones de operación y seguridad

Cambio de credenciales

Cambiar las credenciales creadas por defecto después de la primera instalación.

Protección del archivo .env

Restringir el acceso al archivo .env y evitar publicarlo o compartirlo por medios inseguros.

Credenciales diferenciadas

Usar credenciales diferenciadas por ambiente y rotarlas periódicamente.

Seguridad en base de datos

Asegurar la base de datos MySQL con accesos limitados y respaldos periódicos.

Implementar HTTPS

Implementar HTTPS en ambientes publicados para proteger credenciales y sesiones.

Monitoreo de logs

Monitorear logs y alertas para identificar accesos indebidos, errores o inconsistencias.

Proceso formal de usuarios

Definir un proceso formal para altas, bajas y modificaciones de usuarios.

Validar integraciones

Validar las integraciones con correo y LDAP antes de habilitar automatismos en producción.

⚠ Aplicar estas recomendaciones ayudará a mantener una administración más segura de los usuarios del software y a reforzar la gobernanza sobre los accesos institucionales.

10. Conclusión

El Software de Gestión de Usuarios constituye una herramienta de apoyo para mejorar la administración, la trazabilidad y la seguridad asociada a la gestión de identidades, contratos y accesos dentro de la entidad. Su diseño modular, junto con el uso de buenas prácticas como bcrypt, variables de entorno, control por roles y un backend estructurado con NestJS, permite una base sólida para su operación y crecimiento.

Con la correcta instalación del backend, la configuración del frontend y el uso disciplinado de los módulos funcionales, la plataforma puede contribuir significativamente a optimizar procesos de Recursos Humanos y Tecnología, reducir riesgos derivados de accesos no controlados y fortalecer el gobierno de usuarios en los sistemas institucionales.

Administración

Mejora la administración de identidades, contratos y accesos dentro de la entidad.

Trazabilidad

Diseño modular con bcrypt, variables de entorno y control por roles para una base sólida.

Gobernanza

Fortalece el gobierno de usuarios en los sistemas institucionales.



Superintendencia de Transporte

Software de Gestión de Usuarios — Manual de Instalación y Uso

Versión	Fecha	Clasificación
1.0	18 de marzo de 2026	Documento técnico oficial

Documento técnico y funcional para despliegue, administración y operación del sistema. Este manual puede complementarse con capturas del sistema, diagramas de flujo y evidencias de operación según el entorno de despliegue.