



 INFORME DE SEGUIMIENTO

FASE 5

Fortalecimiento de la gestión de identidades y diseño de topología segura

Entidad: Superintendencia de Transporte

Fecha: 18 de marzo de 2026

Naturaleza del documento: Informe de seguimiento y lineamientos técnicos

Enfoque: Gestión de identidades (IAM) y arquitectura segura de red

Entregables principales

1. Avance funcional del software IAM
2. Propuesta de topología segura para la intranet e infraestructura tecnológica institucional

RESUMEN EJECUTIVO

Resumen ejecutivo

El presente informe consolida el seguimiento de la quinta fase del proceso de fortalecimiento de ciberseguridad y gestión de accesos en la Superintendencia de Transporte.

Se documentan dos entregables principales:

Entregable I

El avance funcional del software IAM desarrollado para apoyar la administración de usuarios, roles y accesos.

Entregable II

Una propuesta de topología segura para la intranet e infraestructura tecnológica institucional, acompañada de lineamientos, recomendaciones normativas y plan de implementación.

1. Introducción

En el marco del fortalecimiento institucional en materia de seguridad digital, gestión de accesos y administración de infraestructura tecnológica, la quinta fase del proyecto se orientó a consolidar capacidades que permitan a la Superintendencia de Transporte mejorar el control sobre sus usuarios, roles, contratos y plataformas, así como definir una arquitectura de red segura que sirva de referencia para la operación de su intranet y servicios críticos.

Este informe presenta el seguimiento de los avances obtenidos en dicha fase, explicando:

Alcance funcional del software IAM

El alcance funcional del software IAM construido.

Limitaciones actuales de integración

Las limitaciones actuales de integración con el directorio institucional.

Propuesta de topología segura

La propuesta de topología segura recomendada para una gestión tecnológica alineada con buenas prácticas de ciberseguridad, segmentación, monitoreo, continuidad y control de accesos.

2. Objetivo

Documentar el seguimiento de la fase 5 del proceso de fortalecimiento tecnológico y de ciberseguridad de la Superintendencia de Transporte, dejando evidencia del avance en el desarrollo del software IAM para la gestión de usuarios y accesos, así como de la propuesta técnica de topología segura para la intranet e infraestructura institucional, con el fin de servir como insumo de apoyo documental y operativo para la mejora continua de la entidad.

Dejar trazabilidad sobre el estado actual del software de gestión de identidades y accesos.

Proponer una topología de red segura, segmentada y administrable, adecuada para la operación institucional.

Explicar los requerimientos pendientes por parte de la entidad para la integración completa con Microsoft Entra / Directorio Activo.

Establecer recomendaciones normativas, técnicas y operativas para la correcta implementación de controles de ciberseguridad.

3. Justificación

La presente fase se justifica por la necesidad de fortalecer los mecanismos institucionales de administración de usuarios, perfiles, contratos y accesos a sistemas, así como por la importancia de contar con lineamientos claros para una red interna segura.

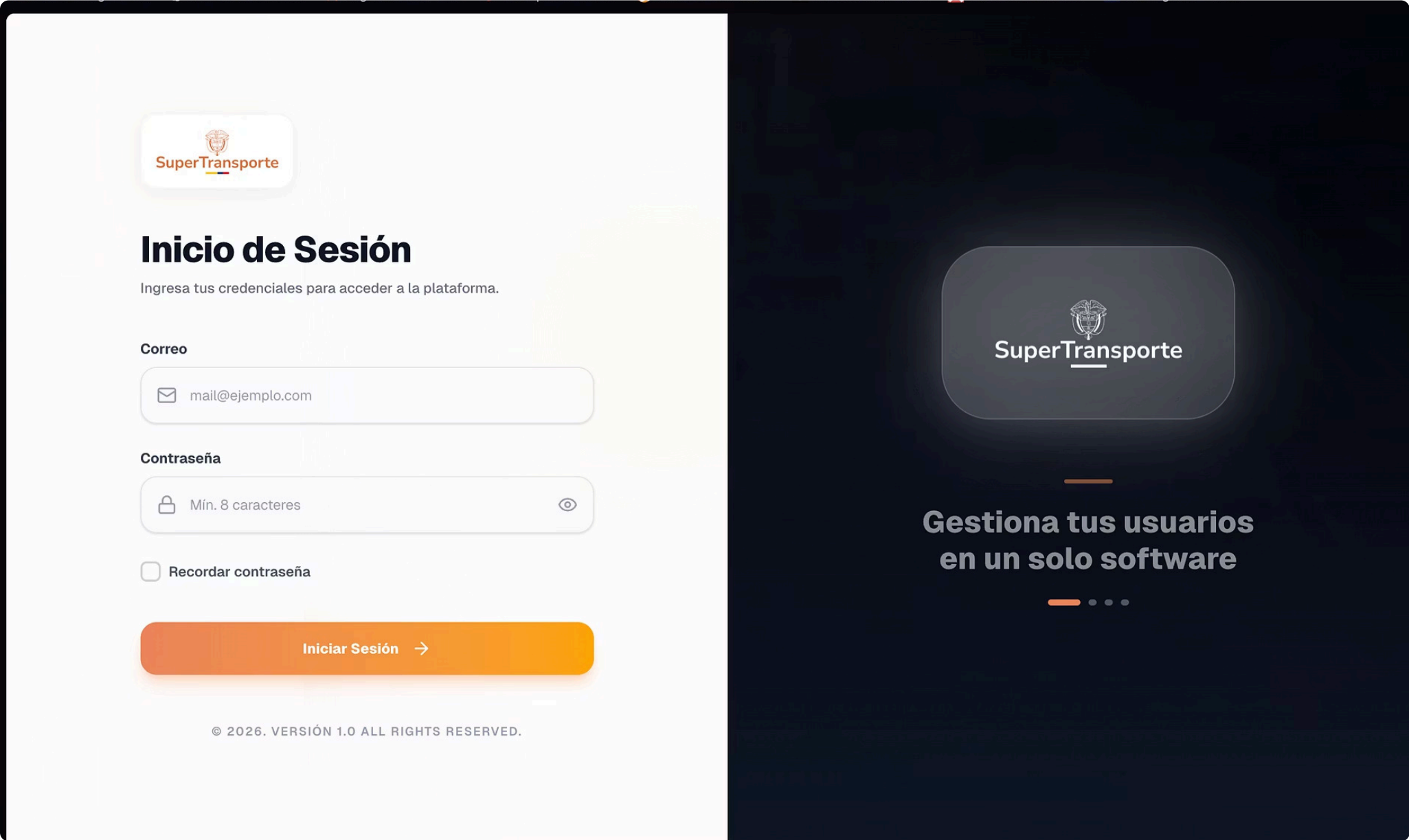
- La adecuada gestión de identidades, junto con una arquitectura tecnológica segmentada y monitoreada, reduce riesgos operativos, limita privilegios indebidos, mejora la trazabilidad de eventos y permite una respuesta más eficiente ante incidentes de seguridad.

3.1. Justificación del entregable 1: software IAM para gestión de identidades y accesos

Como parte del seguimiento de la quinta fase, se diseñó y desarrolló un software orientado a apoyar la administración de identidades y accesos dentro de la entidad. El propósito de esta solución es servir como punto central de control para procesos relacionados con usuarios, roles, contratos, solicitudes de acceso y, en fases posteriores, alertamiento e integración con componentes institucionales tales como Directorio Activo, Microsoft Entra, correo institucional y fuentes de log.

Estado general del software IAM

Estado actual	El software actualmente permite la gestión de solicitudes de usuario dentro de las plataformas definidas en el alcance funcional trabajado hasta esta fase.
Limitación principal	Para lograr un funcionamiento integral, la entidad debe habilitar una integración activa con su directorio institucional (Microsoft Entra / Active Directory / LDAP) y definir los permisos, aplicaciones registradas y flujos técnicos necesarios para el intercambio seguro de información.
Motivo de no integración	La integración directa con el directorio no se ejecutó en esta fase debido a que, al solicitar el acceso, se informó que no se contaba con los permisos necesarios, o no existía una aplicación registrada, API, clave o configuración dentro de Microsoft Entra que permitiera la gestión de usuarios mediante el software desarrollado.
Dependencias adicionales	Se requiere igualmente un buzón o correo de alertas, parámetros de envío institucional y definición de responsables de operación para alertas sobre contratos no vigentes y usuarios activos.



Gestión de software de la entidad

El sistema contempla el registro y administración de los softwares o plataformas institucionales, permitiendo identificar qué sistemas existen, qué responsables tienen y sobre cuáles se deben tramitar solicitudes o permisos.

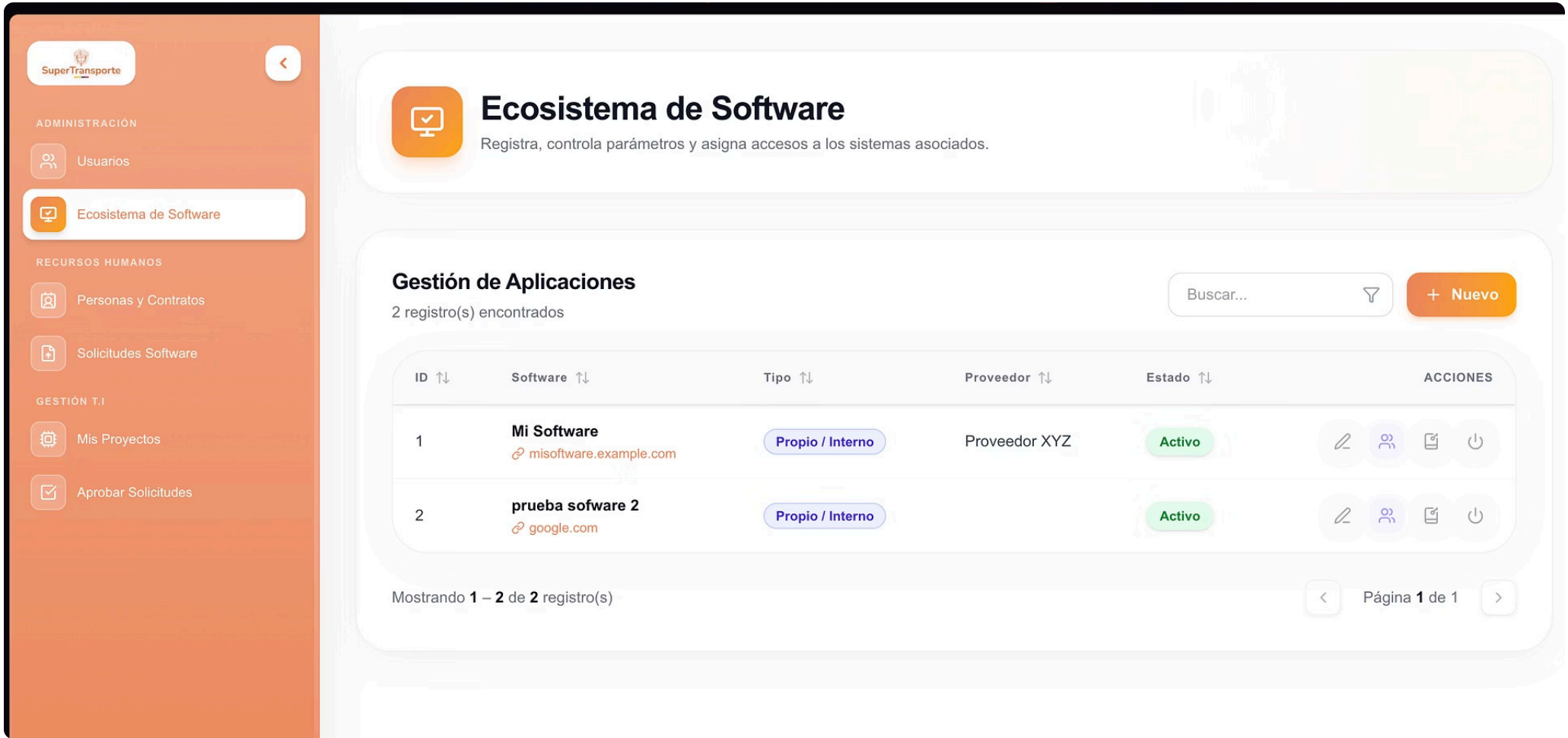
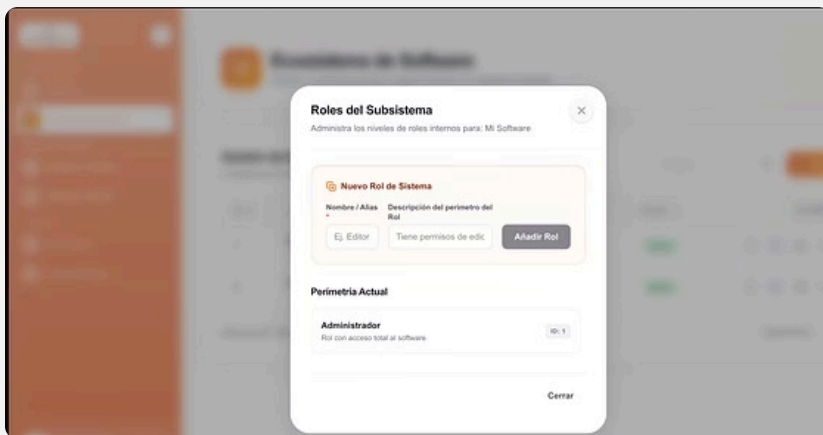


Ilustración 1 — Listado de software

Gestión de usuarios y roles

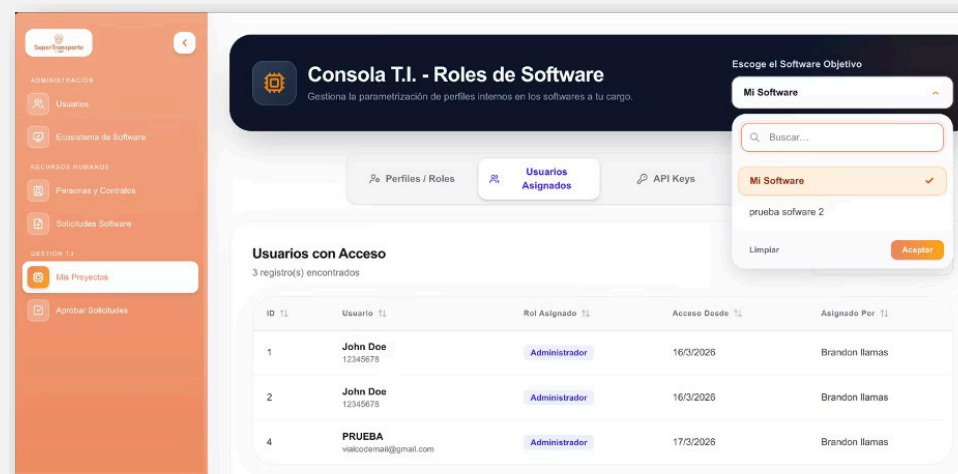
3.1.2. Gestión de usuarios

La solución incorpora la administración de usuarios asociados a las plataformas, permitiendo mantener una trazabilidad centralizada de los accesos y de los estados de los registros dentro del sistema.



3.1.3. Gestión de roles de usuario

Se habilita la gestión de roles o perfiles, con el fin de organizar los privilegios por funciones y evitar asignaciones desordenadas o excesivas dentro de las plataformas institucionales.



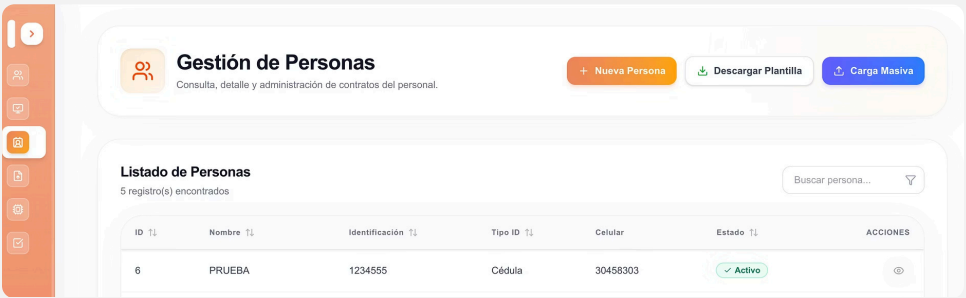
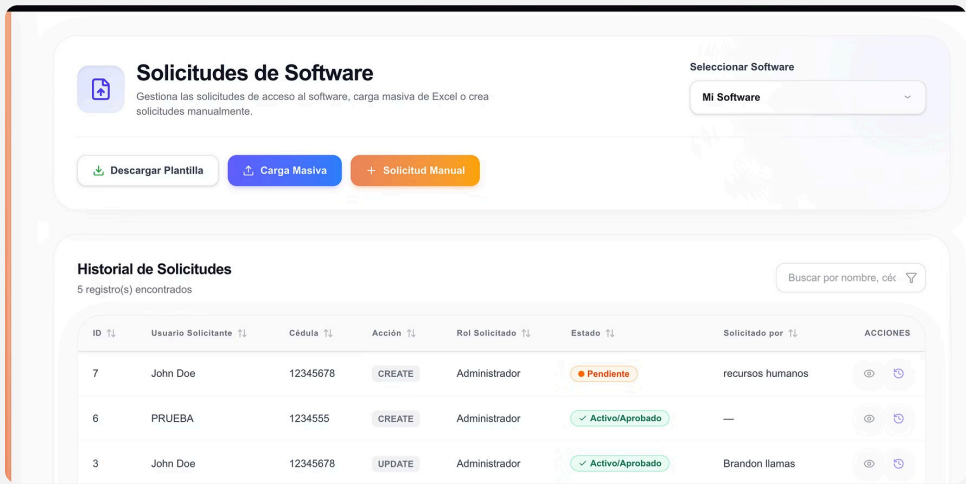
Participación de Recursos Humanos

3.1.4. Participación de recursos humanos para integrar o solicitar accesos

El software contempla que el área de recursos humanos pueda participar en el flujo de alta o solicitud de acceso de usuarios a los sistemas, fortaleciendo la articulación entre el ciclo contractual y la habilitación tecnológica.

3.1.5. Gestión de contratos y usuarios por parte de recursos humanos

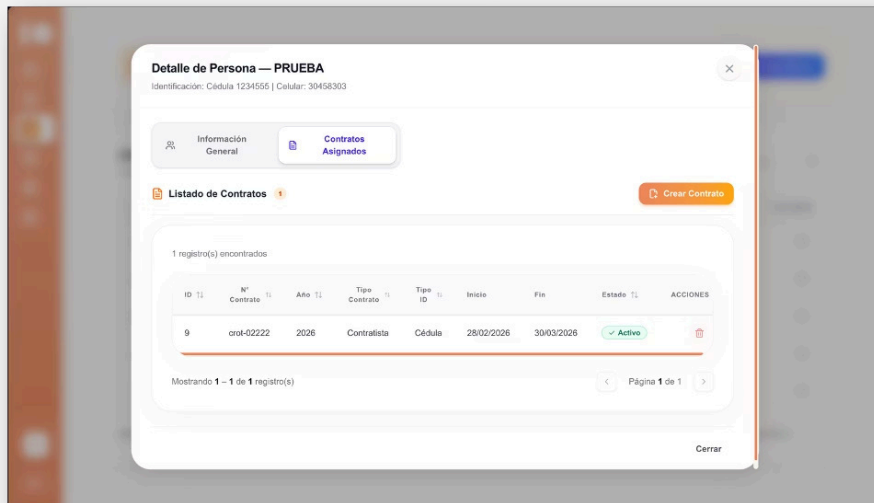
Se prevé que recursos humanos pueda gestionar contratos y usuarios, permitiendo una relación entre la vigencia contractual y el estado de acceso a plataformas institucionales.



Consulta de usuarios activos y gestión de logs

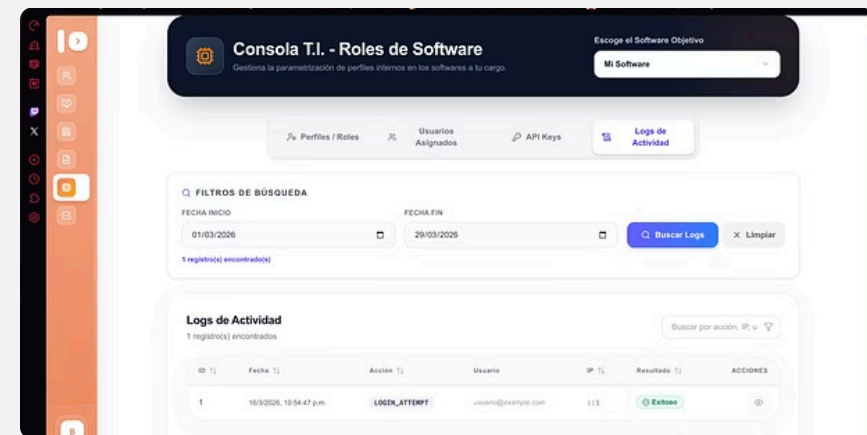
3.1.6. Consulta de usuarios activos con contratos

La herramienta fue pensada para permitir visibilidad sobre usuarios activos dentro de las plataformas y su relación con contratos vigentes, aportando control administrativo y reducción de riesgos por cuentas huérfanas.



3.1.7. Gestión de logs por parte del área de TI

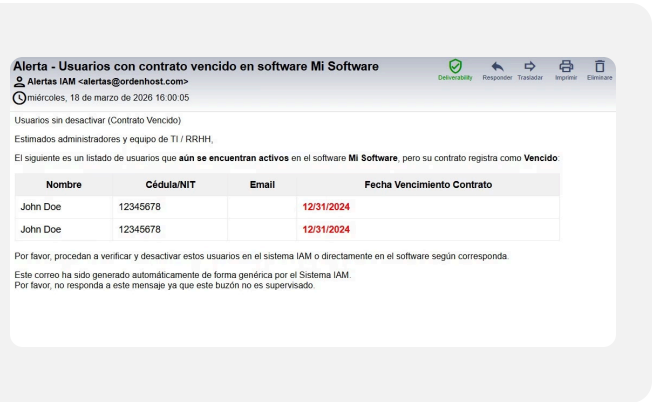
Se contempla permitir al área de TI gestionar los logs de las aplicaciones; no obstante, para ello será necesario integrar los sistemas actuales con la plataforma, de forma que los eventos relevantes puedan centralizarse y ser consultados.



Alertas, solicitudes y aprobaciones

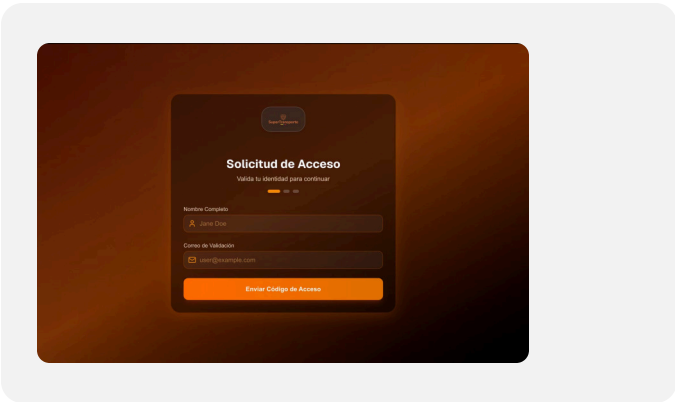
3.1.8. Alertas sobre contratos no vigentes y usuarios activos

La solución proyecta el envío de alertas relacionadas con usuarios activos cuyos contratos no se encuentren vigentes. Para esto se requiere un correo institucional de alertamiento y la integración con el directorio institucional para validar y correlacionar la información.



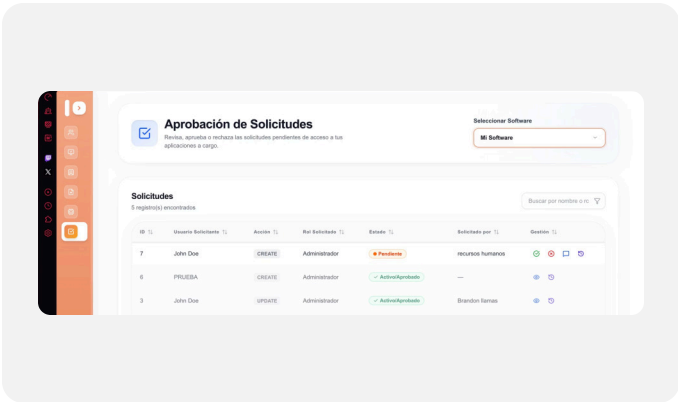
3.1.9. Solicitud de acceso por parte de trabajadores

El sistema permite estructurar el flujo para que los trabajadores puedan solicitar acceso a determinadas plataformas, dejando trazabilidad de la petición, su justificación y su estado.



3.1.10. Aprobación o desaprobación por TI

Se contempla que el área de TI pueda aprobar o desaprobar solicitudes de acceso a plataformas, integrando un control formal sobre la autorización de usuarios y la asignación de privilegios.



Recomendaciones para completar la madurez del software IAM



Registro en Microsoft Entra

Registrar una aplicación institucional en Microsoft Entra y definir el modelo de autenticación y autorización requerido.

Permisos administrativos

Otorgar permisos y consentimientos administrativos mínimos necesarios para lectura y/o gestión de usuarios, grupos o atributos del directorio, según el alcance aprobado por la entidad.

Integración segura con directorio

Definir una integración segura con LDAP/Active Directory o Microsoft Graph, según la arquitectura autorizada por la entidad.

Buzón de alertas institucional

Configurar un buzón de correo de alertas institucional y formalizar responsables de monitoreo y respuesta.

Integración de logs

Integrar las aplicaciones prioritarias al módulo de logs para centralizar trazabilidad, eventos y auditoría.

Catálogos oficiales

Definir catálogos oficiales de roles, responsables de aprobación y reglas de segregación de funciones.

ENTREGABLE 2

3.2. Justificación del entregable 2: propuesta de topología segura para la intranet e infraestructura

El segundo entregable de esta fase corresponde a una propuesta de topología segura para la Superintendencia de Transporte, orientada a servir como guía técnica para la organización de la intranet, la exposición controlada de servicios, la segregación de entornos y la protección de activos críticos.

- ❶ La finalidad de esta propuesta no es únicamente dibujar una red, sino establecer principios de distribución segura, gobierno técnico, monitoreo y respuesta que permitan operar de manera más robusta y trazable.

Una topología segura debe partir del entendimiento de que no todos los sistemas ni todos los usuarios deben convivir en el mismo segmento de red. La segmentación por zonas, el uso de controles perimetrales, la separación de redes de administración, la centralización de logs, el endurecimiento de estaciones y servidores, y la integración con un sistema de identidad fuerte son elementos esenciales para reducir la superficie de ataque y limitar el movimiento lateral ante incidentes.

4. Lineamientos técnicos para una topología segura

Segmentación por zonas

Separar, como mínimo, la zona externa, la DMZ, la red de usuarios internos, la red de aplicaciones, la red de bases de datos y la red de administración. Cada segmento debe contar con reglas explícitas de comunicación.

Control perimetral robusto

Ubicar firewall de nueva generación, IPS y WAF en el perímetro de exposición. Los servicios públicos no deben publicar directamente sistemas internos ni bases de datos.

Identidad como eje de control

Toda autenticación relevante debe apoyarse en un directorio institucional centralizado y, preferiblemente, en MFA para usuarios privilegiados, administradores, acceso remoto y aplicaciones sensibles.

Mínimo privilegio y segregación de funciones

Los accesos deben ser asignados únicamente según necesidad funcional. Las cuentas administrativas, operativas y de consulta deben mantenerse separadas.

Monitoreo y auditoría

Centralizar logs de firewall, servidores, sistemas, bases de datos y aplicaciones en un SIEM o plataforma equivalente, con alertas, casos de uso y conservación de evidencias.

Respaldo y continuidad

Mantener copias de seguridad cifradas, aisladas y probadas mediante ejercicios de restauración. La continuidad del negocio y la recuperación ante desastres deben estar documentadas.

Administración segura

Las labores administrativas deben realizarse desde una red o segmento de administración dedicado, utilizando bastiones, MFA y registro de sesiones cuando aplique.

Gestión de endpoints

Los equipos de usuario y servidores deben contar con hardening, antivirus/EDR, control de parches, cifrado de disco cuando aplique y políticas de uso definidas.

Gestión de vulnerabilidades

Realizar escaneos periódicos, priorización por criticidad, seguimiento de hallazgos y validación del cierre técnico de vulnerabilidades.

Integración controlada

Las integraciones entre aplicaciones, directorio, correo, RR.HH. y módulos de logs deben hacerse mediante canales autenticados, cifrados y con revisión previa de permisos.

5. Qué hacer y qué no hacer

Buenas prácticas recomendadas

✓ Qué hacer

- Separar redes por función y criticidad.
- Exigir autenticación fuerte.
- Documentar reglas de acceso.
- Revisar privilegios periódicamente.
- Centralizar logs.
- Usar cuentas nominativas.
- Validar respaldos.
- Realizar gestión de cambios.
- Proteger accesos remotos con VPN y MFA.

❌ Qué no hacer

- No mantener todos los sistemas en una misma red plana.
- No publicar bases de datos a Internet.
- No usar cuentas compartidas sin trazabilidad.
- No dejar usuarios activos sin validación contractual.
- No exponer escritorios remotos sin control.
- No depender únicamente del antivirus.
- No dejar reglas temporales sin depuración.

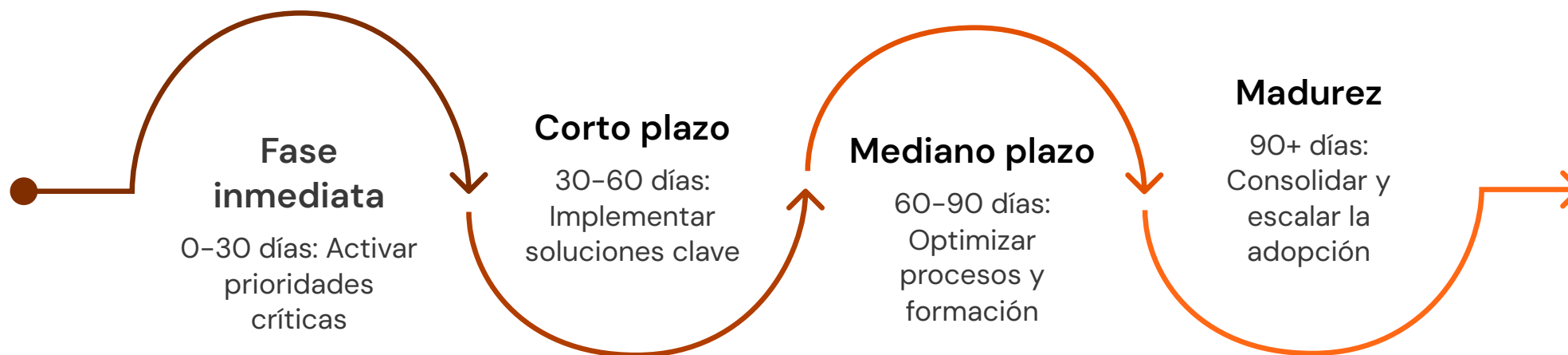
6. Marco normativo y de referencia aplicable

La propuesta técnica y organizacional aquí descrita puede alinearse con los siguientes referentes normativos, reglamentarios y de buenas prácticas aplicables al contexto colombiano de entidades públicas y a la gestión moderna de seguridad de la información:

- 1 Ley 1581 de 2012**
Marco general para la protección de datos personales y el tratamiento adecuado de información personal.
- 2 Ley 1273 de 2009**
Fortalece la protección penal de la información y de los datos, incorporando delitos informáticos al ordenamiento colombiano.
- 3 Decreto 1078 de 2015**
Decreto Único Reglamentario del sector TIC, como referente transversal de gobierno digital y lineamientos del sector.
- 4 Resolución 500 de 2021 y Resolución 02277 de 2025**
Del Ministerio TIC, mediante las cuales se establecen lineamientos y estándares para la estrategia de seguridad digital y el Modelo de Seguridad y Privacidad de la Información (MSPI).
- 5 MSPI actualizado**
Marco de referencia para la planeación, operación, evaluación del desempeño y mejoramiento continuo de la seguridad y privacidad de la información en entidades públicas.
- 6 ISO/IEC 27001:2022**
Buenas prácticas internacionales alineadas con controles asociados para la gestión del riesgo, el gobierno del acceso, la documentación y la mejora continua.

7. Plan sugerido a seguir

Ruta sugerida de implementación



La ruta de implementación está diseñada para avanzar de manera progresiva, asegurando que cada fase consolide las bases necesarias para la siguiente, garantizando una adopción ordenada y sostenible de los controles de ciberseguridad.

FASE INMEDIATA

Plan sugerido — Fase inmediata (0–30 días)

Gobierno del proyecto

Definir gobierno del proyecto e identificar sistemas prioritarios.

Inventario

Inventariar usuarios y roles, formalizar responsables.

Microsoft Entra

Registrar aplicación en Microsoft Entra y definir alcance de integración autorizado.

CORTO Y MEDIANO PLAZO

Plan sugerido — Corto y mediano plazo (30–90 días)

Corto plazo (30–60 días)

- Habilitar integración de directorio en modo controlado.
- Configurar MFA para accesos privilegiados.
- Establecer buzón de alertas.
- Definir catálogos de roles.
- Segmentar redes críticas y administrativas.

Mediano plazo (60–90 días)

- Integrar fuentes de log priorizadas.
- Activar correlación básica de eventos.
- Conectar información contractual y de RR.HH.
- Formalizar procedimientos de altas, modificaciones y bajas de usuarios.

MADUREZ

Plan sugerido – Madurez (90 días en adelante)

- Ampliar integración de sistemas.
- Ejecutar revisiones periódicas de privilegios.
- Fortalecer SIEM/SOC.
- Hacer pruebas de restauración.
- Medir indicadores y documentar acciones de mejora continua bajo el ciclo PHVA.

8. Conclusión

Los entregables documentados en esta fase aportan de manera directa al fortalecimiento institucional de la Superintendencia de Transporte, en especial en lo relacionado con la gestión y administración de usuarios, roles y accesos a plataformas.

Software IAM

El software IAM desarrollado constituye una base funcional importante para formalizar procesos de solicitud, revisión y control de accesos, y su potencial puede ampliarse significativamente una vez la entidad habilite la integración técnica con su directorio institucional, el correo de alertas y las fuentes de información necesarias para automatizar validaciones y correlaciones.

Topología segura

La topología segura propuesta ofrece una referencia clara para la correcta implementación de la red y de los servicios tecnológicos institucionales, promoviendo segmentación, trazabilidad, monitoreo, control de privilegios y continuidad operativa.

En conjunto, estos insumos fortalecen a la entidad tanto documentalmente como tecnológicamente, brindando apoyo concreto a sus procesos de ciberseguridad y estableciendo una base ordenada para futuras etapas de mejora continua.

9. Referencias de apoyo

Ministerio TIC — MSPI

Ministerio TIC. Modelo de Seguridad y Privacidad de la Información (MSPI) y lineamientos de Gobierno Digital.

Resolución 02277 de 2025

Ministerio TIC. Resolución 02277 de 2025, actualización del MSPI.

Ley 1581 de 2012

Función Pública / Gestor Normativo. Ley 1581 de 2012.

Ley 1273 de 2009

SUIN–Juriscol. Ley 1273 de 2009.

Decreto 1078 de 2015

SUIN–Juriscol. Decreto 1078 de 2015.

Microsoft Learn

Microsoft Learn. Guías de registro de aplicaciones en Microsoft Entra y permisos para integración con Microsoft Graph.

RESUMEN DE ENTREGABLES

Resumen de entregables de la Fase 5

Entregable	Descripción	Estado / Observación
Software IAM	Gestión de usuarios, roles, contratos, solicitudes de acceso y alertas.	Funcional en alcance definido. Pendiente integración con Microsoft Entra / Active Directory / LDAP y buzón de alertas.
Topología segura	Propuesta de arquitectura de red segmentada para la intranet e infraestructura institucional.	Propuesta entregada con lineamientos, recomendaciones normativas y plan de implementación.
Recomendaciones normativas	Alineación con Leyes 1581/2012, 1273/2009, Decreto 1078/2015, Resoluciones MSPI e ISO/IEC 27001:2022.	Documentadas en el presente informe.
Plan de implementación	Ruta sugerida en cuatro fases: inmediata, corto, mediano plazo y madurez.	Definido con actividades y responsables sugeridos por fase.

Información del documento

Datos del informe

Documento: Informe de Seguimiento — Fase 5

Entidad: Superintendencia de Transporte

Fecha: 18 de marzo de 2026

Naturaleza: Informe de seguimiento y lineamientos técnicos

Enfoque: Gestión de identidades (IAM) y arquitectura segura de red

Alcance del documento

El presente informe consolida los avances de la Fase 5 del proceso de fortalecimiento de ciberseguridad y gestión de accesos, documentando el estado del software IAM y la propuesta de topología segura para la Superintendencia de Transporte.

Este documento tiene carácter técnico-institucional y sirve como insumo de apoyo documental y operativo para la mejora continua de la entidad.