**SISTEMA DE GESTIÓN DE INCIDENCIAS**

**Especificación de Requerimiento:**

ER002-Gestion de Roles

Versión 1.0

**Lima, abril del 2023**

**Control de Versiones**

**ÍNDICE**

[**1. Introducción 4**](#_1fob9te)

[**1.1 Propósito 4**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.83oiumq9bdi6)

[**1.2 Alcance 4**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.7zamywgv92lu)

[**1.3 Definiciones, siglas y abreviaciones 4**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.4zi9rf5bn5a6)

[**1.4 Referencias 4**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.3dy6vkm)

[**1.5 Resumen 5**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.loxb1dbw6com)

[**2. Descripción General 6**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.ca68ewe7hm48)

[**1.6 Diagrama de Casos de Usos 6**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.4d34og8)

[**1.7 Descripción 6**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.qjm1y8gdgaj2)

[**1.8 Actores 6**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.ic7dnko0oiy6)

[**1.9 Precondiciones 6**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.8hoddldjfdsb)

[**1.10 Pos Condiciones 7**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.9lkb78i6c63p)

[**1.11 Flujo Básico 7**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.5ragciye7xi8)

[**1.12 Excepciones 7**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.nvgan3pihxop)

[**1.13 Prototipos visuales 8**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.1ksv4uv)

[**1.14 Requerimientos no funcionales 8**](https://docs.google.com/document/d/1_TqQT0LrKVQ--LdTcyWWVABr4WAHY7RD/edit#heading=h.s6thmlx3zrtt)

# **Introducción**

El presente documento tiene como objetivo describir los requerimientos necesarios para la implementación de la funcionalidad de gestión de roles dentro del Sistema de Gestión de Incidencias.

## **Propósito**

El propósito de este requerimiento es establecer y administrar claramente los roles y responsabilidades de los diferentes usuarios del sistema, para garantizar una gestión efectiva y eficiente de las incidencias reportadas. Esto incluye la definición de los permisos y autorizaciones necesarios para cada rol, así como la asignación de tareas y responsabilidades específicas para cada usuario del sistema

## **Alcance**

Este requerimiento abarca desde la definición y establecimiento de los diferentes roles y responsabilidades de los usuarios, hasta la asignación de permisos y autorizaciones específicas para cada uno de ellos. Además, también incluye la gestión de usuarios, la comunicación y colaboración entre ellos, y el monitoreo y seguimiento del desempeño de cada rol.

## **Definiciones, siglas y abreviaciones**

* **Gestión de roles:** proceso de definir, asignar y administrar roles y responsabilidades de los usuarios en un sistema de gestión de incidencias.
* **Usuario:** Persona que utiliza el Sistema de Gestión de Incidencias para reportar o dar seguimiento a incidencias.
* **Rol:** Conjunto de responsabilidades y autorizaciones asignadas a un usuario en el sistema de gestión de incidencias.
* **Permiso:** Autorización otorgada a un usuario para acceder a ciertas funciones o áreas del sistema de gestión de incidencias.
* **Autorización:** Capacidad de un usuario para realizar ciertas acciones o funciones en el sistema de gestión de incidencias.
* **RBAC:** Role-Based Access Control (control de acceso basado en roles).
* **ACL:** Access Control List (lista de control de acceso).
* **SSO**: Single Sign-On (inicio de sesión único).
* **AD:** Active Directory (directorio activo).

## **Referencias**

Licitación de Requisitos.xls

Requisitos no funciones.xlsx

## **Resumen**

La funcionalidad de gestión de roles implica garantizar un acceso seguro y protegido al sistema, mientras se asegura que cada usuario tenga las herramientas y recursos necesarios para cumplir con sus responsabilidades en la resolución de incidencias en el Sistema de Gestión de Incidencias, con el fin de mejorar la eficiencia y efectividad de los procesos de gestión de incidencias, al mismo tiempo que se protege la privacidad y seguridad de los datos del usuario.

# **2. Descripción General**

## **2.1 Diagrama de Casos de Usos**

Diagrama

Descripción generada automáticamente

**Figura 1. Diagrama Caso de Uso: GR001- Gestión de roles**

## **2.2 Descripción**

La funcionalidad de gestión de roles permitirá asignar diferentes niveles de acceso y permisos a los usuarios del sistema, con el fin de garantizar la seguridad y la privacidad de la información. Asimismo, permite definir los permisos de cada rol, lo que significa que se pueden establecer permisos de lectura, escritura, edición y eliminación para cada función del sistema de gestión de incidencias.

**2.3 Actores**

* Administrador del sistema: Encargado de administrar y configurar el sistema. Este actor tiene acceso al panel de control del sistema y tiene la capacidad de asignar roles a otros usuarios.
* Técnicos: Son los usuarios con habilidades y conocimientos especializados para manejar y resolver incidencias. Este actor tiene acceso a las incidencias asignadas a ellos según su rol asignado.
* Usuarios: Son los usuarios finales que utilizan el sistema para reportar incidencias. Este actor puede agregar incidencias al sistema, ver el estado de las incidencias reportadas y agregar comentarios adicionales. de registro y las cuentas de usuario.
* Sistema: Encargado de recopilar la información y validarla para permitir la creación de una cuenta de usuario en el Sistema de Gestión de Incidencias.

## **2.4 Precondiciones**

1. El sistema de gestión de incidencias está en funcionamiento.
2. El administrador del sistema tiene acceso al panel de control del sistema.
3. Los técnicos y usuarios ya están registrados en el sistema y han iniciado sesión.

## **2.5 Postcondiciones**

1. El técnico tiene acceso y permisos adecuados para manejar y resolver incidencias en el sistema de gestión de incidencias según su rol asignado.
2. Los usuarios pueden reportar incidencias y ver el estado de sus incidencias reportadas en el sistema.
3. El sistema mantiene un registro de la asignación de roles.

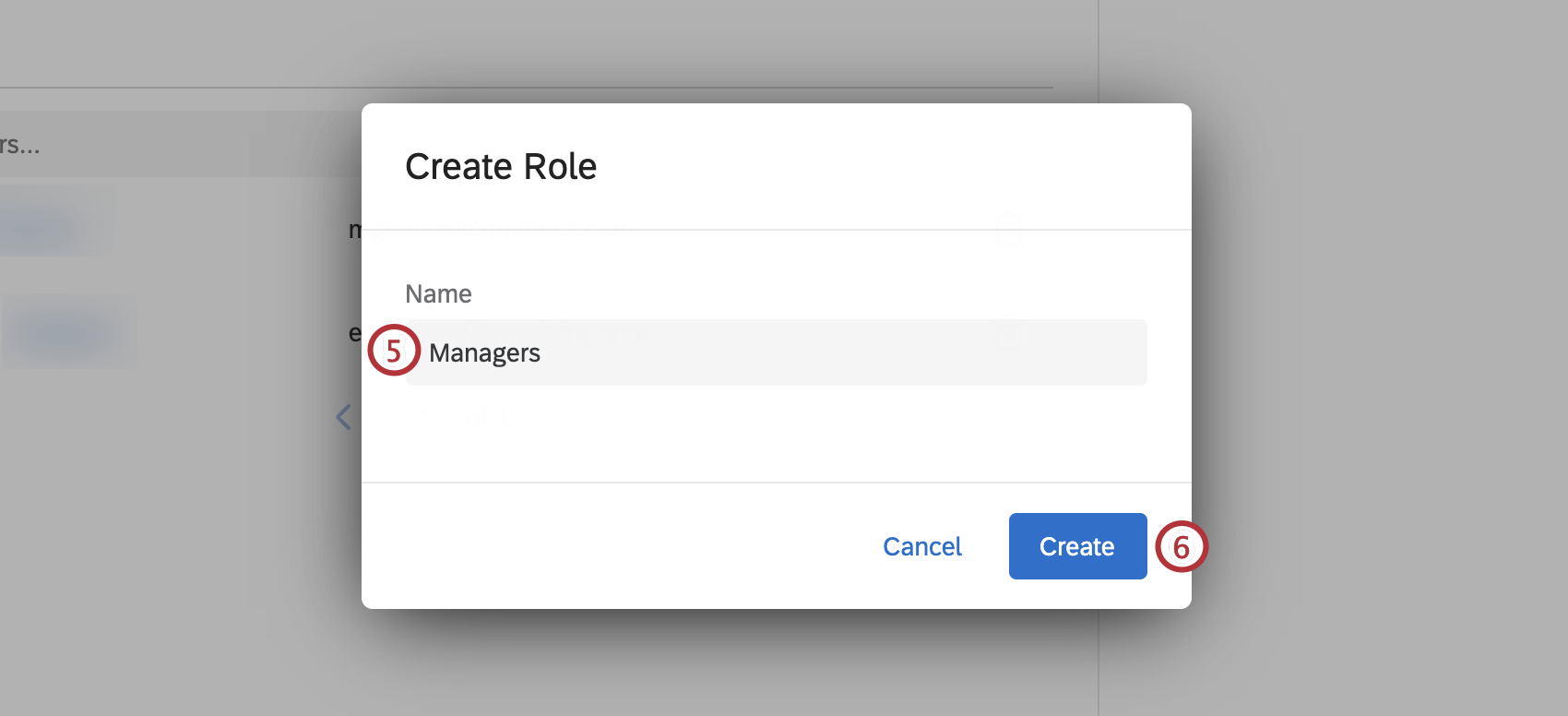
## **2.6 Flujo de Eventos**

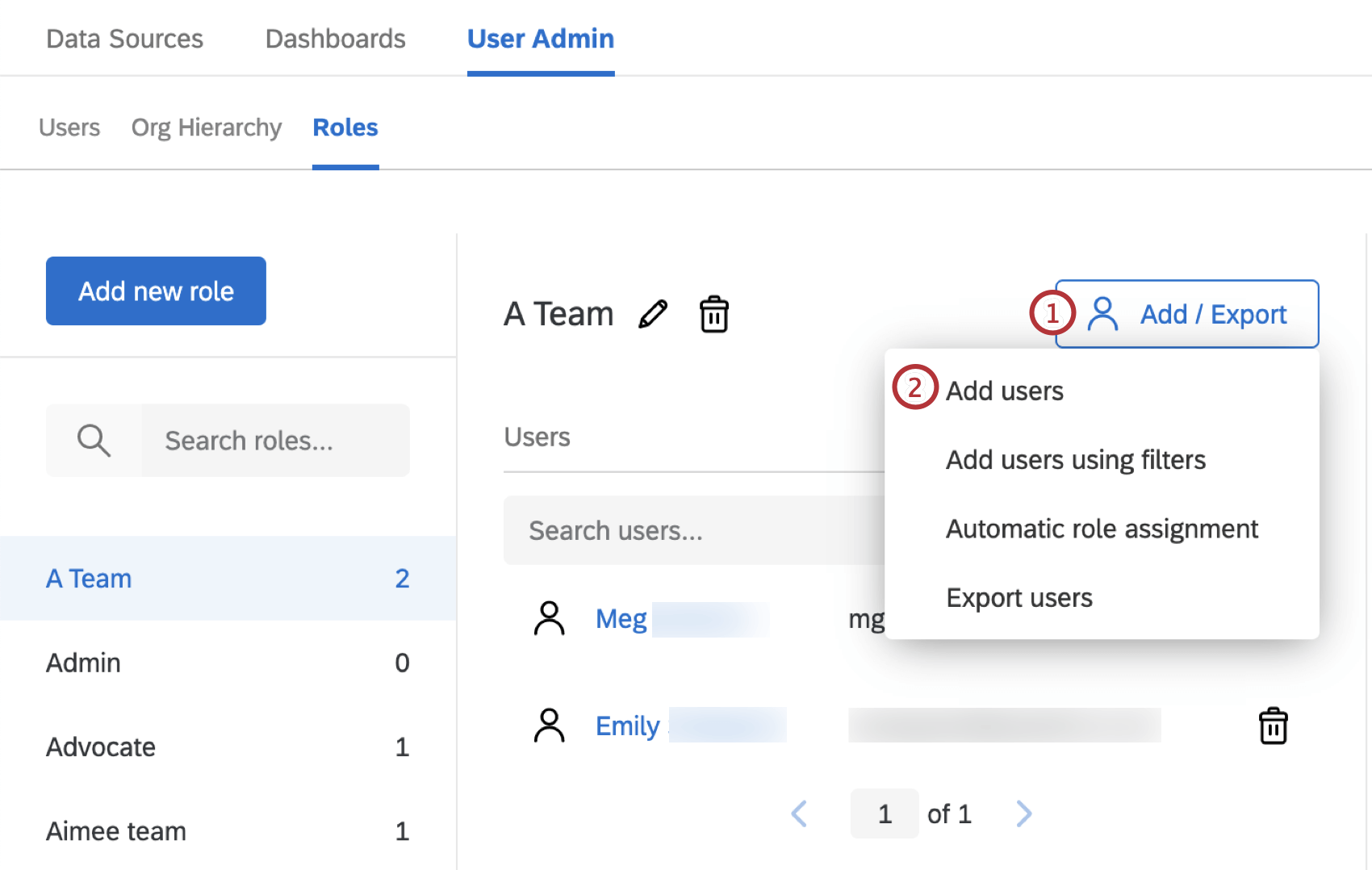
1. El administrador del sistema accede al panel de control del sistema y selecciona la opción de "Gestión de Roles".
2. El sistema muestra una lista de roles disponibles, junto con una descripción de cada uno de ellos.
3. El administrador del sistema selecciona un técnico para asignarle un rol.
4. El sistema muestra una lista de roles disponibles para asignar al técnico.
5. El administrador del sistema selecciona el rol adecuado para el técnico, que le permita manejar y resolver incidencias.
6. El sistema guarda la asignación de rol y muestra un mensaje de confirmación.
7. El técnico puede acceder al sistema y ver las incidencias asignadas a él, actualizar su estado y resolverlas según sea necesario.
8. Si un usuario reporta una incidencia, el sistema asigna automáticamente la incidencia al técnico correspondiente según su rol asignado.
9. El usuario puede ver el estado de sus incidencias reportadas y agregar comentarios adicionales.

## **2.7 Excepciones**

* Permiso insuficiente: si el administrador del sistema no tiene los permisos necesarios para asignar roles a otros usuarios, el sistema mostrará un mensaje de error indicando que el usuario no tiene permisos suficientes para realizar la tarea.
* Usuario no registrado: si el usuario que se desea asignar un rol no está registrado en el sistema, el administrador del sistema debe registrar al usuario antes de asignarle un rol. De lo contrario, el sistema no podrá asignar un rol al usuario.
* Rol inapropiado: si el administrador del sistema asigna un rol inapropiado a un usuario, es posible que el usuario no tenga acceso a las funciones necesarias para realizar sus tareas. Por ejemplo, si un técnico no tiene acceso a las funciones necesarias para manejar y resolver incidencias, no podrá realizar sus tareas adecuadamente.
* Incidencia asignada a un técnico inapropiado: si el sistema asigna automáticamente una incidencia a un técnico inapropiado, la incidencia puede no resolverse adecuadamente o puede haber una demora en la resolución de la incidencia.

## **2.8 Prototipos visuales**





**Figura 2. Prototipos Visuales: GR001- Asignación de roles**

## **2.9 Requerimientos no funcionales**

* RNF-01 Fiabilidad: El sistema debe tener la capacidad de manejar una gran cantidad de usuarios registrados simultáneamente sin disminuir su rendimiento o su capacidad de respuesta.
* RNF-04 Seguridad: El sistema debe garantizar la seguridad de la información del usuario al momento de crear la cuenta, por lo que debe implementar medidas de seguridad adecuadas para proteger la información personal y sensible del usuario, como la contraseña y el correo electrónico.
* RNF-06 Usabilidad: El proceso de registro debe ser fácil de seguir y comprender para el usuario. La interfaz de usuario debe ser intuitiva y fácil de navegar, con instrucciones claras para el usuario en cada paso.
* RNF-07 Disponibilidad: El sistema debe estar disponible las 24 horas del día, los 7 días de la semana, para permitir que los usuarios creen cuentas en cualquier momento que lo necesiten.
* RNF-08 Cumplimiento normativo: El sistema debe cumplir con las leyes y regulaciones aplicables, como las leyes de privacidad de datos, y garantizar que la información personal del usuario se maneje de manera adecuada y legal.
* RNF-09 Mantenimiento: El sistema debe ser fácil de mantener y actualizar, y debe ser capaz de manejar actualizaciones y parches de seguridad sin afectar la disponibilidad del servicio. Además, el sistema debe estar respaldado regularmente para evitar la pérdida de datos.