SISTEMA DE GESTIÓN DE INCIDENCIAS

**Especificación de Requerimiento:**

ER003-Autenticación de Usuario

Versión 1.0

**Lima, abril del 2023**

**Control de Versiones**



**ÍNDICE**

[**1. Introducción 4**](#_heading=h.1fob9te)

[1.1 Propósito **4**](#_heading=h.83oiumq9bdi6)

[1.2 Alcance **4**](#_heading=h.7zamywgv92lu)

[1.3 Definiciones, siglas y abreviaciones **4**](#_heading=h.4zi9rf5bn5a6)

[1.4 Referencias **4**](#_heading=h.3dy6vkm)

[1.5 Resumen **5**](#_heading=h.loxb1dbw6com)

[**2. Descripción General 6**](#_heading=h.ca68ewe7hm48)

[1.6 Diagrama de Casos de Usos **6**](#_heading=h.4d34og8)

[1.7 Descripción **6**](#_heading=h.qjm1y8gdgaj2)

[1.8 Actores **6**](#_heading=h.ic7dnko0oiy6)

[1.9 Precondiciones **6**](#_heading=h.8hoddldjfdsb)

[1.10 Pos Condicione**s 7**](#_heading=h.9lkb78i6c63p)

[1.11 Flujo Básico **7**](#_heading=h.5ragciye7xi8)

[1.12 Excepciones **7**](#_heading=h.nvgan3pihxop)

[1.13 Prototipos visuales **8**](#_heading=h.1ksv4uv)

[1.14 Requerimientos no funcionales **8**](#_heading=h.s6thmlx3zrtt)

# Introducción

## Propósito

El propósito de la funcionalidad de autenticación de usuario en el sistema de gestión de incidencias es garantizar que solo los usuarios autorizados puedan acceder a la plataforma y realizar acciones dentro de ella. El sistema debe validar las credenciales del usuario y permitir el acceso solo si las credenciales son correctas y el usuario tiene los permisos necesarios.

## Alcance

El alcance de este requerimiento es garantizar que el sistema de gestión de incidencias tenga una funcionalidad de autenticación de usuario segura y confiable que permita a los usuarios autorizados acceder y utilizar las funcionalidades del sistema de manera segura.

El requerimiento incluye la implementación de un proceso de autenticación de usuario que permita validar las credenciales de los usuarios, establecer roles y permisos de acceso, y mantener la privacidad y la seguridad de la información del usuario y del sistema.

Se incluye la implementación de medidas de seguridad apropiadas para evitar el acceso no autorizado y garantizar la confidencialidad y la integridad de los datos del sistema.

## Definiciones, siglas y abreviaciones

* **Autenticación**: Proceso de confirmar la identidad de un usuario.
* **Credenciales**: Información de identificación y autenticación de un usuario, como nombre de usuario y contraseña.
* **Rol**: Conjunto de permisos y responsabilidades asignados a un usuario dentro del sistema.
* **Permiso**: Acción o funcionalidad que se otorga a un usuario dentro del sistema.
* **Acceso no autorizado**: Intento de acceder al sistema o a sus recursos sin tener los permisos adecuados.
* **Seguridad**: Medidas de protección de la información y los recursos del sistema para prevenir el acceso no autorizado, la divulgación, la modificación o la destrucción de datos.

## Referencias

Plan de Elicitación de Requerimientos - SGI-PER.docx

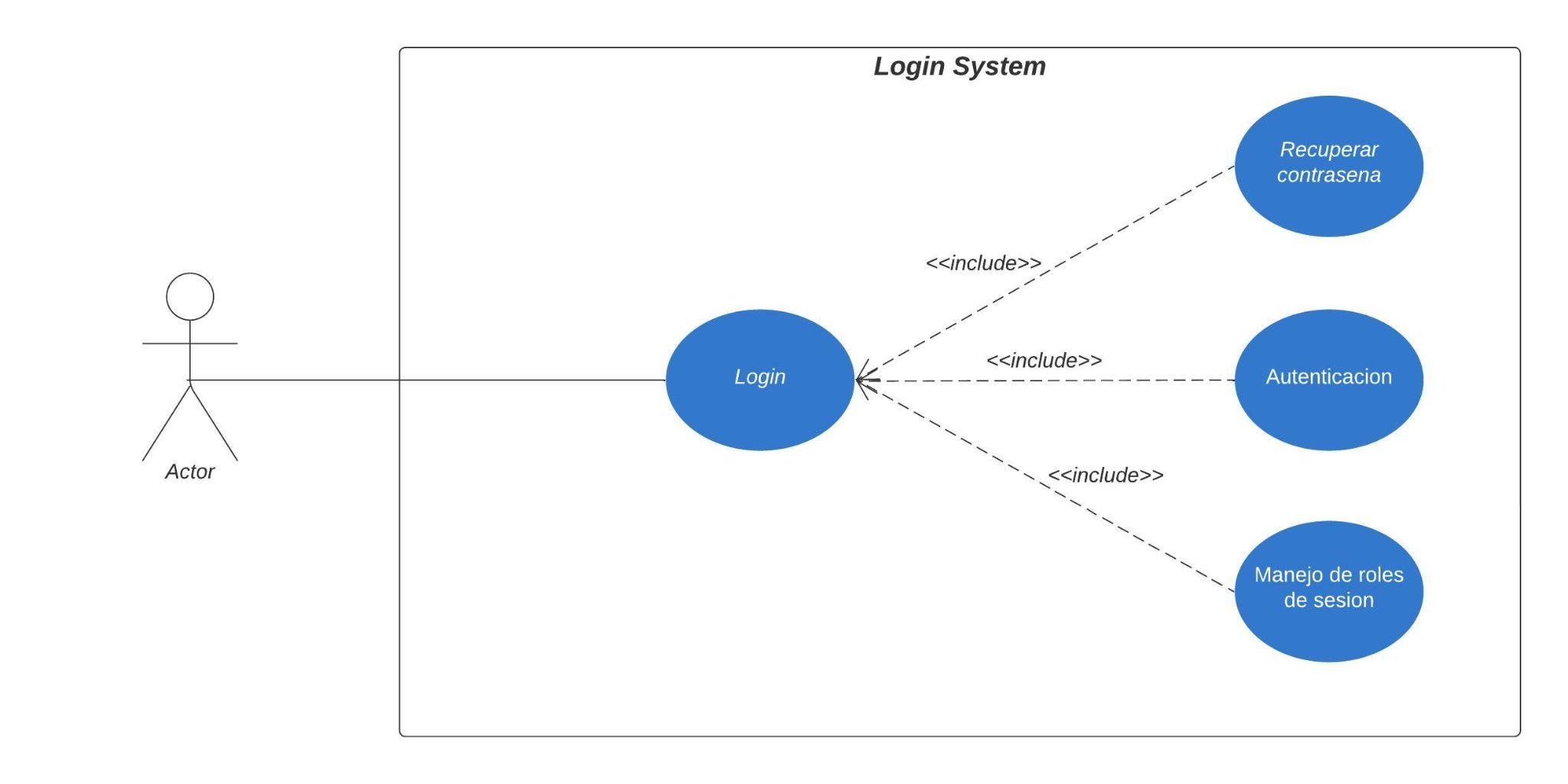
Plan de Gestión de la Configuración de Software - SGI-PGCS.docx

## Resumen

La funcionalidad de autenticación de usuario en el sistema de gestión de incidencias es esencial para garantizar que solo los usuarios autorizados puedan acceder y utilizar el sistema de manera segura y protegida. Este requerimiento establece la implementación de un proceso de autenticación que permita validar las credenciales del usuario, establecer roles y permisos de acceso, y mantener la privacidad y la seguridad de la información del usuario y del sistema.

# 2. Descripción General

## Diagrama de Casos de Usos



**Figura 1. Diagrama Caso de Uso: CU003- Autenticación de Usuario**

## Descripción

Esta funcionalidad permitirá que el usuario acceda al sistema dependiendo del rol que tenga dentro del sistema, también se encontrará el apartado de recuperación de contraseña el cual abrirá un ticket para el área encargada el cual le generará las credenciales para que pueda recuperar su contraseña.

## Actores

* Usuario
* Administrador
* Personal técnico

## Precondiciones

* El usuario debe tener una cuenta registrada en el sistema de gestión de incidencias.
* El administrador del sistema debe tener una cuenta registrada y tener acceso a las funciones de administración del sistema.
* El personal técnico debe tener una cuenta registrada y tener acceso a las funciones de resolución de incidencias del sistema.
* El sistema de gestión de incidencias debe estar disponible y en línea para que los usuarios puedan iniciar sesión y utilizar las funciones de autenticación.
* La información de inicio de sesión, incluyendo el nombre de usuario y la contraseña, deben ser ingresados correctamente por el usuario para poder acceder a las funciones del sistema de gestión de incidencias.

## Pos Condiciones

1. El sistema autentica al usuario si la información de inicio de sesión ingresada es correcta.
2. Si la autenticación es exitosa, el sistema permite al usuario acceder a las funciones permitidas según su rol o permisos asignados en el sistema.
3. Si la autenticación es incorrecta, el sistema muestra un mensaje de error y solicita al usuario que vuelva a ingresar la información de inicio de sesión.
4. Después de la autenticación, el sistema mantiene un registro de la sesión del usuario en el sistema de gestión de incidencias, incluyendo la hora de inicio y finalización de la sesión y las acciones realizadas por el usuario en el sistema.
5. Si el usuario cierra la sesión en el sistema, el sistema finaliza la sesión y cierra todas las funciones permitidas del usuario en el sistema.
6. Si el usuario cierra la sesión en el sistema, el sistema redirige al usuario a la página de inicio de sesión del sistema.

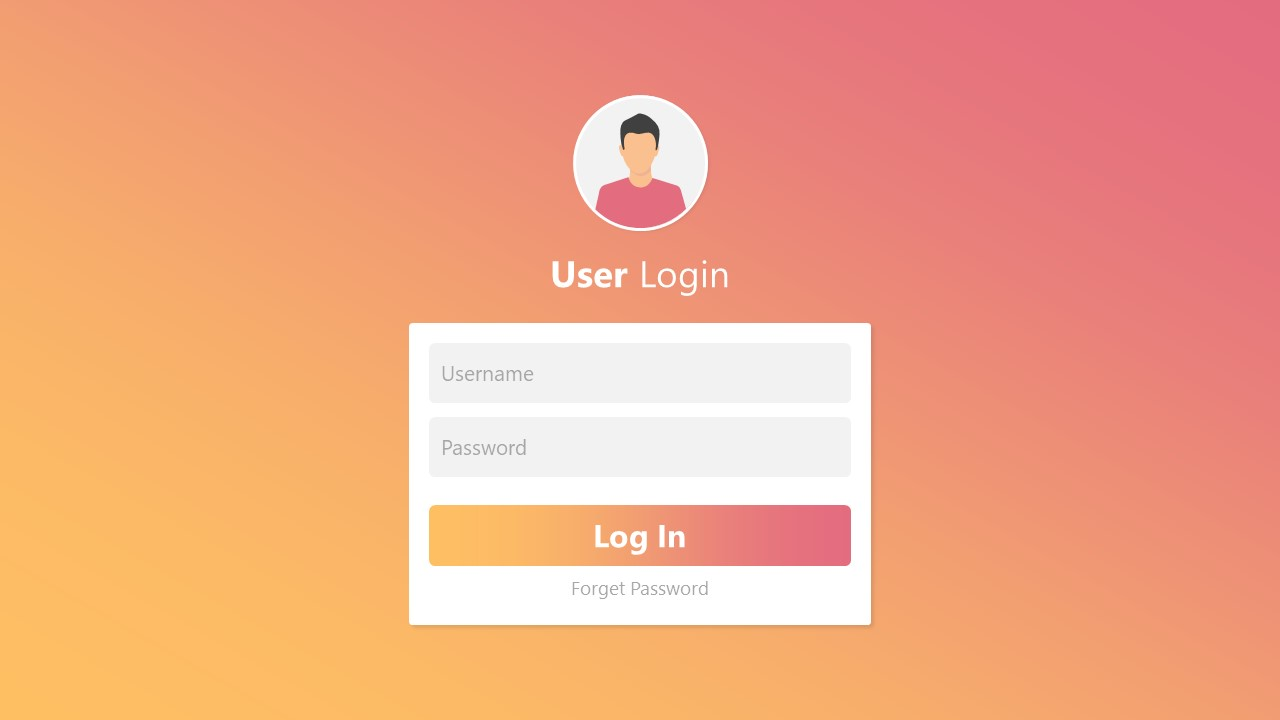
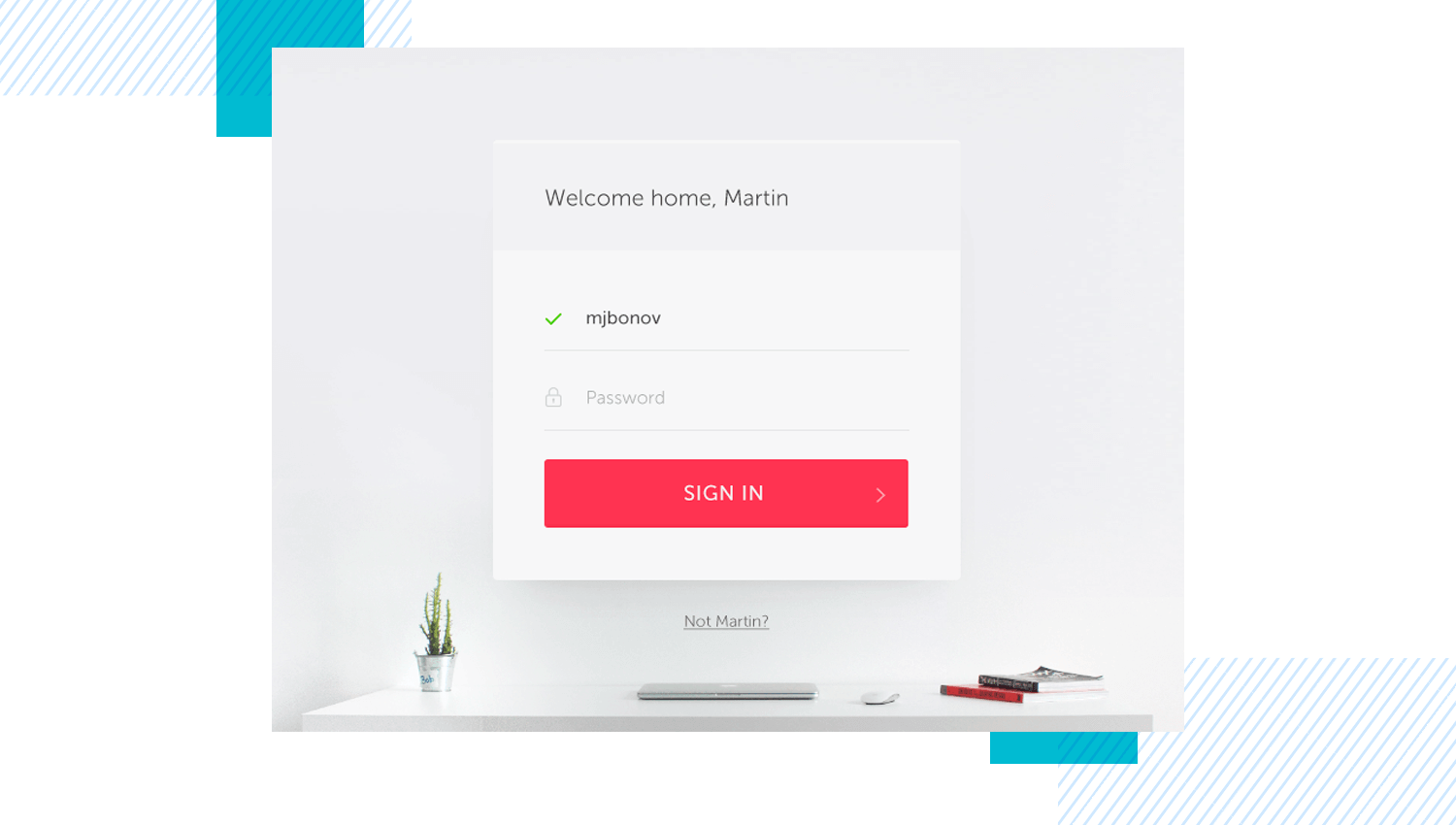
## 1.11 Flujo Básico

1. El usuario accede a la página de inicio de sesión del sistema.
2. El sistema presenta al usuario un formulario de inicio de sesión que solicita el nombre de usuario y la contraseña del usuario.
3. El usuario ingresa su nombre de usuario y contraseña en los campos correspondientes del formulario de inicio de sesión.
4. El sistema verifica la información de inicio de sesión ingresada por el usuario.
5. Si la información de inicio de sesión es correcta, el sistema autentica al usuario y redirige al usuario a la página de inicio del sistema de gestión de incidencias.
6. Si la información de inicio de sesión es incorrecta, el sistema muestra un mensaje de error y solicita al usuario que vuelva a ingresar la información de inicio de sesión.

## 1.12 Excepciones

* Si el usuario ingresa información de inicio de sesión incorrecta varias veces, el sistema puede bloquear temporalmente la cuenta del usuario para prevenir intentos de inicio de sesión fraudulentos.
* Si el sistema no puede autenticar al usuario debido a problemas de conectividad, el sistema muestra un mensaje de error y solicita al usuario que intente nuevamente más tarde.
* Si el sistema no puede autenticar al usuario debido a problemas de hardware o software, el sistema muestra un mensaje de error y solicita al usuario que se comunique con el administrador del sistema para solucionar el problema.
* Si el sistema no puede acceder a la base de datos de usuarios debido a un problema técnico, el sistema muestra un mensaje de error y no permite que el usuario inicie sesión hasta que se solucione el problema.
* Si el usuario olvida su contraseña, el sistema permite que el usuario restablezca su contraseña siguiendo un procedimiento de recuperación de contraseña seguro.

## 1.13 Prototipos visuales



## 1.14 Requerimientos no funcionales

* RNF-01 Fiabilidad
* RNF-04 Seguridad
* RNF-06 Usabilidad