

GUÍA DE REVISIÓN DE ROLES Y PERMISOS - SISTEMA EMPRESARIAL

Overskull

Guía de revisión de roles y permisos - sistema empresarial

22/12/2025

Versión 1.0

Queda prohibido cualquier tipo de explotación y, en particular, la reproducción, distribución, comunicación pública y/o transformación, total o parcial, por cualquier medio, de este documento sin el previo consentimiento expreso y por escrito a overskull.

ÍNDICE

1. **INTRODUCCIÓN** 1.1 Objetivo
2. **GESTIÓN DE ROLES EN EL SISTEMA**
 - 2.1 Acceso a Mantenimiento Usuario
 - 2.2 Edición y Asignación de Roles
3. **COORDINACIÓN CON EL GESTOR** 3.1 Consultas sobre Roles Adicionales
4. **PROTOCOLOS DE SEGURIDAD (TENER EN CUENTA SIEMPRE)**
 - 4.1 Alerta de Inactivación de Usuario
 - 4.2 Uso de Usuarios Alternativos

1. INTRODUCCIÓN

1.1 Objetivo

Establecer el procedimiento estándar para la modificación y validación de roles dentro del sistema **EMPRESARIAL**, asegurando que el equipo de QA pueda realizar sus pruebas sin comprometer la disponibilidad de sus accesos.

2. GESTIÓN DE ROLES EN EL SISTEMA

2.1 Acceso a Mantenimiento Usuario

Para gestionar los permisos de un perfil, se debe seguir la siguiente ruta:

1. Ingresar al módulo de **Mantenimiento Usuario**.
2. Utilizar los filtros de búsqueda para localizar al usuario mediante su **DNI** o **CE** (Carné de Extranjería).
3. Una vez ubicado, presionar el icono de la **hamburguesa** (menú de opciones) situado en la fila del registro.

2.2 Edición y Asignación de Roles

1. Seleccionar la opción **Editar** del menú desplegable.
2. Se presentará un **modal de Roles** donde se deben marcar o desmarcar los permisos.
3. La configuración debe realizarse estrictamente **en base a lo solicitado en la tarea** asignada.

3. COORDINACIÓN CON EL GESTOR

3.1 Consultas sobre Roles Adicionales

Si durante la ejecución de la tarea se detecta que los roles asignados no son suficientes para completar el flujo funcional, es obligatorio:

- Consultar directamente con el **gestor** sobre la necesidad de un rol adicional.
- Validar si dicho rol es compatible con el perfil de usuario que se está probando.

4. PROTOCOLOS DE SEGURIDAD (TENER EN CUENTA SIEMPRE)

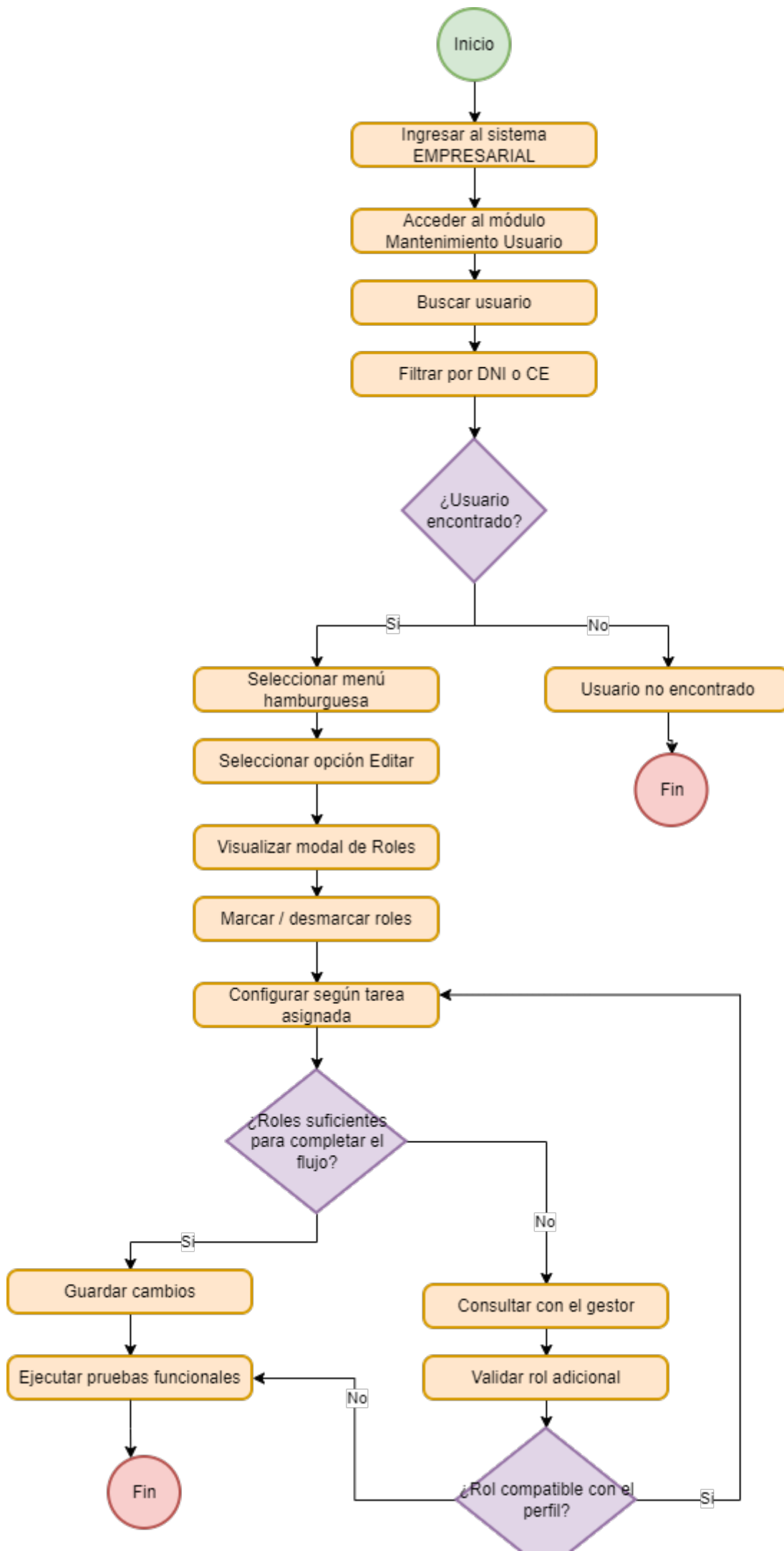
4.1 Alerta de Inactivación de Usuario

El sistema cuenta con un mecanismo de seguridad que monitorea los cambios frecuentes de privilegios. Se debe tener en cuenta que **si cambias tu rol repetidamente, el sistema inactivará automáticamente tu usuario**, bloqueando tu acceso.

4.2 Uso de Usuarios Alternativos

Para mitigar el riesgo de bloqueo de cuentas personales:

- **Es obligatorio trabajar con un usuario alternativo** (perfil de prueba) para realizar las validaciones de roles.
- Bajo ninguna circunstancia se deben realizar cambios constantes sobre el usuario principal de QA.



Revisión #7

Creado 2025-12-22 17:39:23 -05 por percy

Actualizado 2025-12-31 13:18:17 -05 por Leo