UNIVERSIDAD NACIONAL DE COLOMBIA

Universidad Nacional de Colombia - sede Bogotá
Facultad de Ingeniería
Departamento de Sistemas e Industrial
Curso: Ingeniería de Software 1 (2016701)

ASIGNACIÓN Y GESTIÓN DE ROLES	
ACTORES Administrador	**REQUERIMIENTO** SEC-R16.2: El Sistema debe gestionar la asignación de roles (Administrador, Entrenador, Recepción) a los Usuarios Internos y aplicar el control de permisos asociados a cada rol, restringiendo el acceso a módulos no autorizados.

DESCRIPCIÓN

Este caso de uso permite al Administrador asignar, modificar y revocar roles a los usuarios internos del sistema. Cada rol tiene permisos específicos que determinan a qué módulos y funcionalidades puede acceder el usuario. El sistema debe aplicar estas restricciones en tiempo real.

PRECONDICIONES

- El usuario que realiza la acción debe tener rol de Administrador.
- El usuario interno al que se le asignará el rol debe existir en el sistema.

FLUJO NORMAL

1. El Administrador accede al módulo de "Gestión de Usuarios Internos". [Ver Mockup 3.1].
2. El sistema muestra la lista de usuarios internos registrados.
3. El Administrador selecciona un usuario específico.
4. El sistema muestra el detalle del usuario incluyendo su rol actual.
5. El Administrador selecciona la opción "Asignar/Modificar Rol".
6. El sistema muestra las opciones de roles disponibles: Administrador, Entrenador, Recepción. [Ver Mockup 3.2].
7. El Administrador selecciona el rol deseado.
8. El sistema muestra un resumen de los permisos asociados al rol seleccionado.
9. El Administrador confirma la asignación.
10. El sistema actualiza el rol del usuario en la base de datos.
11. El sistema aplica inmediatamente las restricciones de acceso según el nuevo rol.
12. El sistema registra el cambio en el log de auditoría.
13. El sistema muestra un mensaje de confirmación.

FLUJOS ALTERNATIVOS

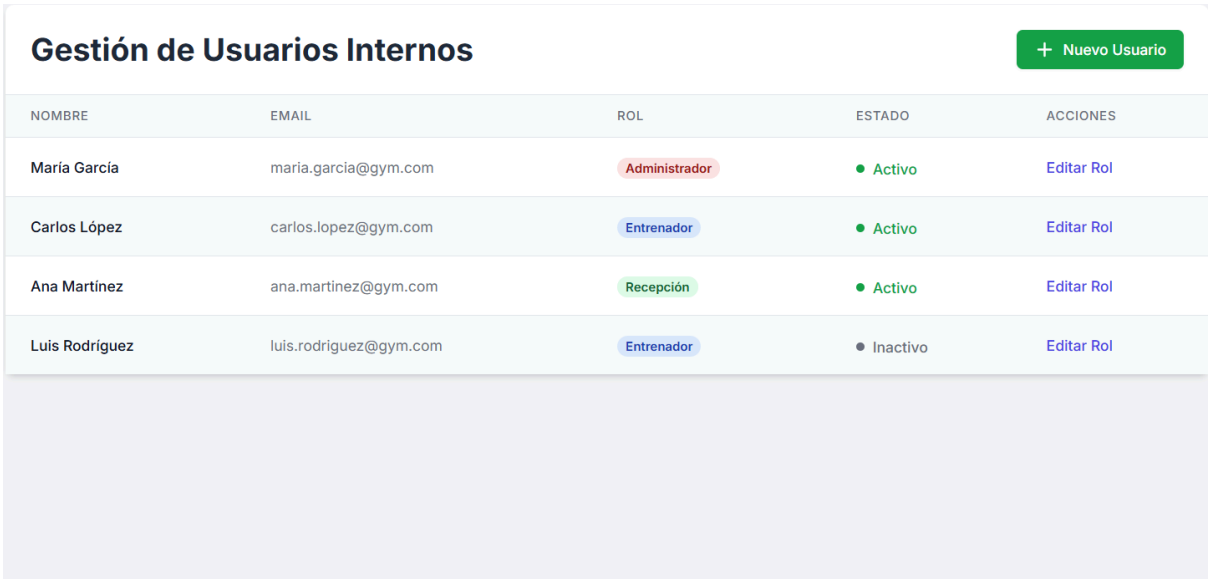
A1. Intento de acceso a módulo restringido

1. Un usuario intenta acceder a un módulo para el cual su rol no tiene permisos.

2. El sistema detecta la falta de autorización. 3. El sistema muestra un mensaje de "Acceso denegado". 4. El sistema registra el intento en el log de seguridad. 5. El sistema redirige al usuario al módulo principal permitido para su rol.
POSTCONDICIONES El usuario tiene asignado el nuevo rol. Los permisos del usuario se han actualizado según el rol asignado. Se ha registrado el cambio en el log de auditoría. Las restricciones de acceso se aplican de forma inmediata.
NOTAS • El sistema debe implementar RBAC (Role-Based Access Control). • Los permisos por rol deben estar definidos en una matriz de permisos configurable. • Un Administrador no debe poder quitarse a sí mismo el rol de Administrador si es el único en el sistema.

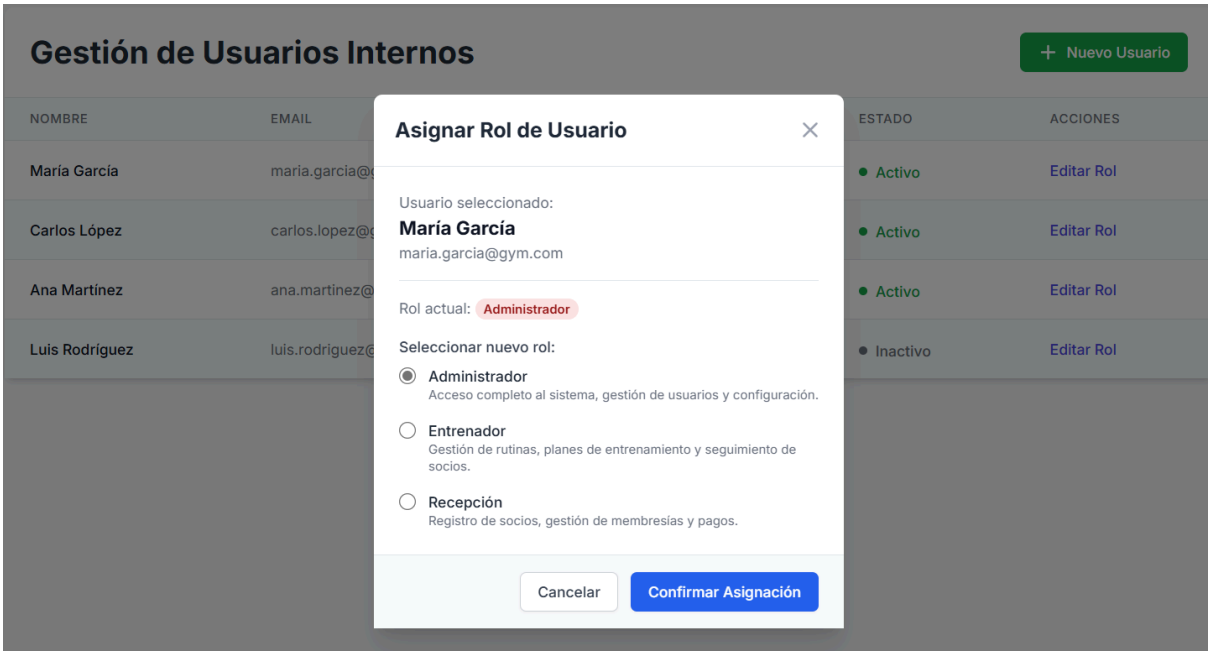
MOCKUPS

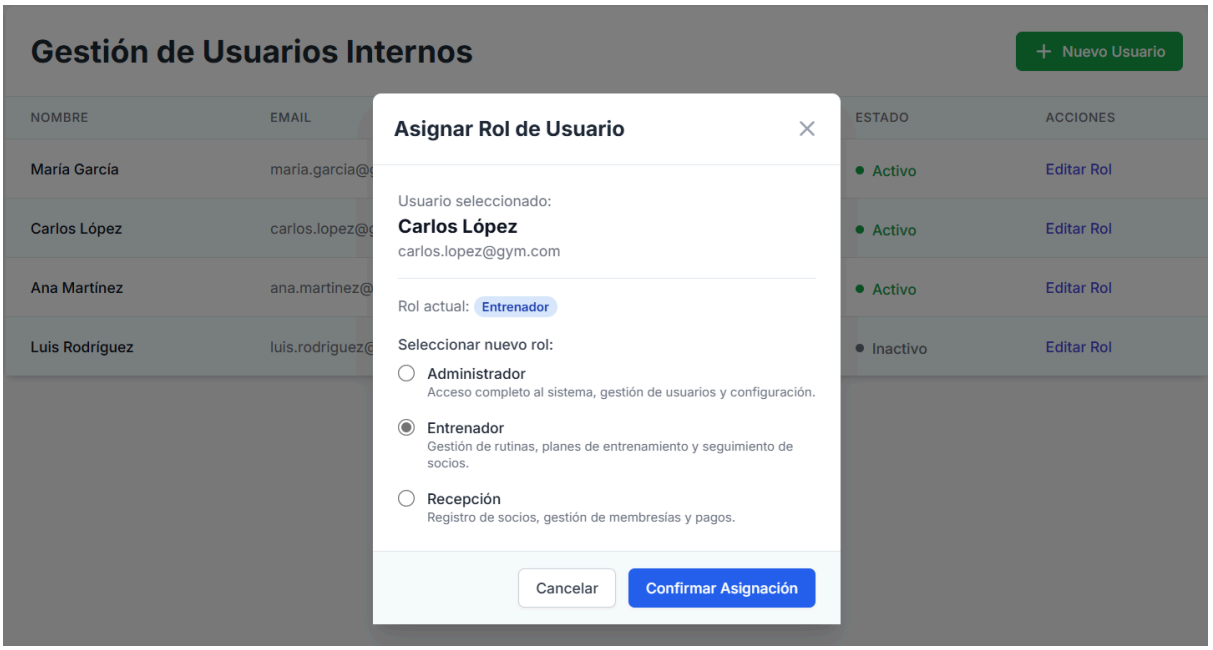
Mockup 3.1: Gestión de Usuarios Internos



Descripción: *Lista de usuarios internos con sus roles actuales, estado y opción para editar rol.*

Mockup 3.2: Modal de Asignación de Rol





Descripción: *Ventana emergente que permite seleccionar el nuevo rol mediante radio buttons, mostrando la descripción de permisos de cada rol.*