CU-GE-24 — Gestionar usuarios y roles

Escenario origen: S-GE-15 | Administración del sistema

RF relacionados: RF13, RF7, RF8

Actor principal: Administrador
Actores secundarios: Sistema GRADE

Objetivo

Permitir que un Administrador cree, edite, desactive usuarios y asigne roles (Docente, Coordinador, Administrador), controlando accesos y responsabilidades en el sistema.

Precondiciones

- Usuario autenticado con rol de Administrador.
- El sistema se encuentra en operación normal.

Postcondiciones

- El usuario gestionado queda creado, editado o desactivado según acción.
- Los roles quedan asignados o modificados.
- La acción queda registrada en auditoría.

Flujo principal (éxito)

1. El Administrador accede al módulo Gestión de usuarios.
2. Selecciona acción: crear, editar o desactivar usuario.
3. El Sistema muestra formulario con datos básicos (nombre, correo, rol, estado).
4. El Administrador completa o modifica los datos.
5. El Sistema valida integridad (correo único, rol válido).
6. El Sistema guarda cambios y actualiza el registro.

7. El Sistema registra acción en auditoría.
8. El Sistema confirma la operación exitosa.

Flujos alternativos / Excepciones

- A1 — Correo duplicado: El Sistema rechaza creación/edición.
- A2 — Usuario no encontrado: El Sistema bloquea acción y alerta al Administrador.
- A3 — Error de permisos: El Sistema impide que roles inferiores gestionen usuarios.

Reglas de negocio

- RN-1: Cada usuario debe tener correo único como identificador.
- RN-2: Solo un Administrador puede asignar o cambiar roles.
- RN-3: Usuarios desactivados no pierden su historial ni auditoría.

Datos principales

- Usuarios(ID, nombre, correo, rol, estado, fecha creación, fecha última modificación).
- Auditoría(acción, usuario administrador, fecha/hora, cambios realizados).

Consideraciones de seguridad/permiso

- Acceso restringido al rol Administrador.
- Políticas de contraseñas seguras y gestión de accesos deben cumplirse.

No funcionales

- Disponibilidad: los cambios deben reflejarse en el acceso de inmediato.
- Seguridad: aplicar políticas institucionales de autenticación y roles.

Criterios de aceptación (QA)

- CA-1: El administrador puede crear, editar y desactivar usuarios correctamente.
- CA-2: Cada usuario tiene un rol único válido asignado.
- CA-3: Usuarios desactivados no pueden acceder al sistema pero mantienen historial.
- CA-4: Todas las operaciones quedan registradas en auditoría.