Historia de Usuario: Gestión de Roles y Permisos (RBAC)

Información General

ID: US-AUTH-001 **Módulo:** Administración / Configuración **Prioridad:** Crítica **Sprint:** Sprint 1

Historia de Usuario

Como Administrador del sistema (Backoffice) **Quiero** crear roles (ej. "Director", "Gestor de áreas", "Analista") y asignar permisos granulares por módulo (ej. "Ver Activos", "Crear Riesgos") **Para** asegurar que cada usuario solo pueda ejecutar las acciones autorizadas para su función (RBAC).

Criterios de Aceptación

Feature: Creación y Asignación de Roles

Scenario: Creación de un rol estándar (RBAC)

```
Given el "Administrador backoffice" está en el módulo de "Administración > Roles"
And no existe un rol llamado "Analista de Activos"
When el administrador crea un nuevo rol con el nombre "Analista de Activos"
And le añade una descripción "Rol para crear y gestionar activos"
And hace clic en "Guardar"
Then el sistema crea el nuevo rol "Analista de Activos"
```

```
And el rol aparece en el listado de roles disponibles
```

Scenario: Asignación de rol a un usuario

```
Given existe el rol "Analista de Activos"
And existe el usuario "analista.juan@email.com"
When el "Administrador" edita el perfil del usuario
"analista.juan@email.com"
And le asigna el rol "Analista de Activos"
And guarda los cambios
Then el usuario "analista.juan@email.com" hereda todos los permisos
definidos en ese rol
```

Feature: Asignación de rol inicial

Scenario: Creación de usuario con rol asignado

```
Given el "Administrador backoffice" está en el módulo de gestión de
usuarios
And no existe el usuario
When el administrador selecciona creación y llena los datos del usuario
And selecciona un rol para el usuario
And hace clic en "Guardar"
Then el sistema crea el nuevo usuario con el rol definido
And el usuario aparece en el listado de usuarios disponibles
```

Feature: Asignación de Permisos (RBAC)

Scenario: Asignar permisos a rol "Analista de Activos"

```
Given existe el rol "Analista de Activos" sin permisos
When el "Administrador" edita el rol
And navega a la sección "Permisos del Módulo: Gestión de Activos"
And selecciona (C)REATE, (R)EAD, (U)PDATE
And des-selecciona (D)ELETE
And navega a "Permisos del Módulo: Gestión de Riesgos"
And selecciona "Read (Incidentes)" y "Create (Incidentes)"
And guarda los cambios
Then el rol "Analista de Activos" ahora tiene permisos CRUD (sin Delete)
en Activos y permisos de Crear/Ver en Incidentes
```

```
And cualquier usuario con ese rol solo puede realizar esas acciones
```

Scenario: Asignar permisos a rol "Director - Lectura"

```
Given existe el rol "Director"
When el "Administrador" edita el rol "Director"
And asigna permisos de solo (R)EAD a los módulos: "Activos", "Riesgos",
"Controles", "Auditoría" y "Reportes"
And no asigna permisos (C)REATE, (U)PDATE, (D)ELETE
Then los usuarios con rol "Director" pueden navegar y ver toda la
información de esos módulos
And no ven los botones de "Crear Nuevo", "Editar" o "Eliminar" en la UI
```

Feature: Consulta y Auditoría

Scenario: El Administrador no puede eliminar su propio rol

```
Given el usuario "admin@backoffice.com" tiene el rol "Administrador
backoffice" (Super-Admin)
When el "Administrador" intenta eliminar su propio rol o el rol
"Administrador backoffice"
Then el sistema muestra un error de protección
And la acción de eliminar (botón) está deshabilitada para ese rol
```

Flujo de Usuario (RBAC)

Flujo de Gestión de Roles y Permisos (RBAC)

150%

📌 **Tips:** Use mouse wheel to zoom, click and drag to pan, or use the controls above

🔧 Documentación Técnica Relacionada

API Endpoints (RBAC)

```
GET /roles
POST /roles
GET /roles/{id}
PUT /roles/{id}
DELETE /roles/{id} (Protegido para Super-Admin)

GET /permissions (Listar todos los permisos disponibles por módulo)
POST /roles/{id}/permissions (Asignar permisos a rol)

GET /users/{id}/roles
POST /users/{id}/roles (Asignar rol a usuario)
```

Reglas de Negocio (RBAC)

- **RBAC (Role-Based Access Control):** Define qué puede hacer un usuario (Permisos).
- La UI debe ocultar dinámicamente los botones (Crear, Editar, Eliminar) si el usuario no tiene el permiso correspondiente para la vista actual.
- Los permisos deben ser granulares y definidos en el backend (ej. ASSET_CREATE, ASSET_READ, ASSET_DELETE, RISK_CREATE, RISK_READ_ALL, RISK_READ_OWN).

Roles Iniciales del Sistema

Rol	Código	Descripción	Contexto	Nivel de acceso
Administrador Backoffice	BO_ADMIN	Acceso total al sistema incluyendo configuración de backend. No necesita	Backoffice	Acceso completo sin restricciones

		acciones específicas.		
Gestor de Clientes	CLIENT_MANAGER	Colaborador de empresa que puede alterar configuraciones de clientes asignados	Backoffice	Acceso completo a clientes asignados
Administrador	ADMIN	Acceso completo a todas las funcionalidades del sistema tenant	Tenant	Acceso completo
Gestor de áreas	AREA_MANAGER	Acceso limitado a módulos operativos y completo en reportes. Requiere acciones específicas.	Tenant	Acceso limitado según acciones
Director	DIRECTOR	Enfoque en dashboards y reportes ejecutivos	Tenant	Solo consulta
Gerente	MANAGER	Acceso a información gerencial y reportes	Tenant	Solo consulta
Coordinador	COORDINATOR	Acceso a herramientas	Tenant	Solo consulta

		de coordinación y reportes		
Analista	ANALYST	Acceso de solo lectura para análisis de datos	Tenant	Solo consulta

Modelo de Datos (RBAC)

- **roles:** id, role_name, description
- **permissions:** id, permission_key, description, module
- **role_permissions:** role_id, permission_id
- **users:** id, name, email
- **user_roles:** user_id, role_id

🏷 Etiquetas

`auth` `roles` `permissions` `rbac` `admin` `sprint-1` `security`

Última actualización: 03/11/2025