DOCUMENTACIÓN: SERVICIO DE RESOLUCIÓN DE ROLES POR EMAIL

DESCRIPCIÓN GENERAL

Este módulo proporciona el sistema de autorización basado en roles para la aplicación, determinando los permisos de cada usuario según su dirección de correo electrónico. Su función principal es consultar la base de datos para resolver qué nivel de acceso tiene un usuario autenticado, implementando un modelo de tres roles jerárquicos.

FUNCIONALIDAD PRINCIPAL

El servicio actúa como el componente central de control de acceso, traduciendo la identidad del usuario (email) en permisos específicos dentro del sistema. Se ejecuta durante el proceso de autenticación para determinar qué recursos y operaciones estarán disponibles para cada usuario.

SISTEMA DE TRES ROLES JERÁRQUICOS

ADMINISTRADOR (ADMIN)

Rol con privilegios completos que permite acceso a todas las funcionalidades del sistema, incluyendo configuración avanzada, gestión de usuarios y operaciones administrativas. Se asigna cuando el campo admin es TRUE en la base de datos.

USUARIO DE ACCIÓN (ACTION)

Rol intermedio que permite realizar operaciones específicas además de las de lectura, pero sin acceso a funciones administrativas completas. Se asigna cuando el campo action es TRUE en la base de datos.

SOLO LECTURA (READONLY)

Rol básico por defecto que permite únicamente consultar información y visualizar datos, sin capacidad de modificar configuraciones o realizar operaciones que alteren el estado del sistema.

FLUJO DE RESOLUCIÓN DE ROLES

CONSULTA A BASE DE DATOS

Realiza una búsqueda en la tabla usuarios_google utilizando el email normalizado (minúsculas) como clave, verificando solo usuarios activos. Esta consulta determina los permisos específicos asignados al usuario.

CREACIÓN AUTOMÁTICA DE USUARIOS

Cuando un usuario se autentica por primera vez y no existe en la base de datos, el sistema crea automáticamente un registro con permisos de solo lectura. Esto permite una incorporación fluida de nuevos usuarios sin intervención administrativa inmediata.

FALLBACK SEGURO

En caso de cualquier error durante el proceso de resolución de roles, el sistema retorna automáticamente el rol de solo lectura, asegurando que nunca se concedan privilegios excesivos por error.

NORMALIZACIÓN DE IDENTIDAD

ESTANDARIZACIÓN DE EMAILS

Convierte todas las direcciones de correo electrónico a minúsculas antes de realizar búsquedas, previniendo problemas de coincidencia debido a diferencias de capitalización y asegurando consistencia en el almacenamiento.

GESTIÓN DE ERRORES ROBUSTA

MANEJO ELEGANTE DE FALLOS

Implementa múltiples capas de protección contra errores, incluyendo manejo de excepciones en consultas de base de datos y fallbacks seguros que previenen la denegación completa de servicio debido a problemas de resolución de roles.

LOGGING INFORMATIVO

Registra eventos importantes como la creación automática de nuevos usuarios y errores durante el proceso, facilitando el monitoreo y diagnóstico de problemas sin exponer información sensible.

INTEGRACIÓN CON AUTENTICACIÓN

Este servicio se ejecuta inmediatamente después de la verificación exitosa del token de Google, completando el proceso de autenticación con la determinación de autorizaciones específicas antes de emitir el token JWT propio de la aplicación.

ESCALABILIDAD Y MANTENIBILIDAD

FACIL EXPANSIÓN DE ROLES

La estructura modular permite fácil adición de nuevos roles o modificación de la lógica de resolución sin afectar otras partes del sistema de autenticación.

GESTIÓN CENTRALIZADA

Al centralizar la lógica de resolución de roles en un servicio dedicado, se facilita la implementación de cambios en la política de permisos y la auditoría del control de acceso.

SEGURIDAD POR DEFECTO

El diseño sigue el principio de privilegio mínimo, donde los usuarios nuevos reciben automáticamente el rol más restrictivo (solo lectura) hasta que un administrador explícitamente les conceda permisos adicionales.