DOCUMENTACIÓN: CONTROLADOR DE AUTENTICACIÓN CON GOOGLE

DESCRIPCIÓN GENERAL

Este módulo implementa el flujo completo de autenticación mediante Google Identity Services. Su función principal es recibir tokens de identificación de Google, verificar su autenticidad, resolver permisos de usuario y emitir tokens JWT propios para el acceso a la aplicación.

FUNCIONALIDAD PRINCIPAL

El controlador gestiona el proceso de autenticación federada donde los usuarios pueden iniciar sesión usando sus cuentas de Google. Transforma un token de identificación de Google en una sesión válida dentro del sistema propio, asignando roles y permisos específicos según la configuración de la aplicación.

FLUJO DE AUTENTICACIÓN

RECEPCIÓN DE CREDENCIALES

Recibe el token de identificación de Google enviado desde el cliente frontend después de que el usuario completa el flujo de autenticación con Google. Valida la presencia del token antes de proceder con la verificación.

VERIFICACIÓN CRYPTOGRÁFICA

Utiliza el conjunto de claves públicas de Google para verificar la firma digital del token. Esta verificación asegura que el token fue emitido legítimamente por Google y no ha sido alterado. La verificación incluye validación del emisor, audiencia y integridad criptográfica.

EXTRACCIÓN DE IDENTIDAD

Una vez verificado el token, extrae la información de identidad del usuario incluyendo dirección de correo electrónico, nombre y estado de verificación. Requiere que el correo electrónico esté verificado por Google para prevenir suplantación de identidad.

RESOLUCIÓN DE ROLES

Consulta el sistema de usuarios para determinar los permisos y nivel de acceso correspondiente al correo electrónico autenticado. Esta resolución puede basarse en listas blancas configuradas o en registros existentes en la base de datos.

ACTUALIZACIÓN DE ACTIVIDAD

Registra el momento del último acceso exitoso en la base de datos para propósitos de auditoría y monitoreo de actividad de usuarios. Esta operación se realiza de manera no bloqueante para no afectar la experiencia de autenticación.

EMISIÓN DE TOKEN PROPIO

Genera un token JWT específico de la aplicación que contiene la identidad del usuario y sus roles asignados. Este token se utilizará para autorizar solicitudes posteriores a los recursos protegidos de la aplicación.

RESPUESTA AL CLIENTE

Devuelve al cliente la información del usuario autenticado, su rol asignado, el token de acceso y metadatos sobre la validez temporal del token.

CARACTERÍSTICAS DE SEGURIDAD

VERIFICACIÓN DE EMISOR

Confirma que el token fue emitido específicamente por los servidores legítimos de Google, previniendo el uso de tokens de proveedores no autorizados.

VALIDACIÓN DE AUDIENCIA

Asegura que el token fue creado específicamente para esta aplicación mediante la verificación del identificador de cliente de Google OAuth.

VERIFICACIÓN DE CORREO

Requiere que Google haya verificado la propiedad del correo electrónico, añadiendo una capa adicional de confianza en la identidad del usuario.

GESTIÓN DE ERRORES ROBUSTA

Proporciona respuestas de error específicas sin revelar información sensible interna, logueando detalles completos para diagnóstico mientras envía mensajes genéricos al cliente.

INTEGRACIÓN CON SISTEMAS EXTERNOS

GOOGLE JWKS

Utiliza el conjunto de claves públicas de Google obtenido dinámicamente para verificar tokens, asegurando compatibilidad con rotaciones de claves sin requerir actualizaciones de la aplicación.

BASE DE DATOS DE USUARIOS

Interactúa con el sistema de gestión de usuarios para resolver permisos y registrar actividad, manteniendo separación de responsabilidades mediante servicios especializados.

SERVICIO JWT PROPIO

Delega la generación de tokens a un servicio especializado que aplica las configuraciones específicas de seguridad y expiración de la aplicación.

BENEFICIOS DEL ENFOQUE

Este sistema permite aprovechar la infraestructura de autenticación de Google mientras mantiene control completo sobre la autorización y roles dentro de la aplicación. Los usuarios se benefician de un inicio de sesión simplificado sin comprometer la seguridad o el control de acceso granular.