Propósito

Maneja la autenticación de usuarios mediante Google Identity Services (GIS) y emisión de tokens JWT propios.

Endpoints Principales

googleAuth(req, res)

Método: POST
Ruta: /auth/google
Descripción: Autenticación con Google OAuth2

Flujo de Autenticación

Recepción de Credencial

Recibe el credential (ID token de Google) desde el frontend

Valida la presencia del credential

Verificación del Token Google

Utiliza JWKS de Google para verificar la firma

Valida issuer y audience (GOOGLE_CLIENT_ID)

Extrae payload con información del usuario

Validación de Email

Verifica que el email esté verificado por Google

Extrae nombre y email del payload

Resolución de Rol

Utiliza resolveRoleByEmail() para determinar el rol del usuario

Basado en las listas blancas de ADMIN_WHITELIST y ACTION_WHITELIST

Emisión de JWT Propio

Crea token de acceso con información del usuario

Incluye: sub, email, name, role

Configura expiración según ENV.JWT_EXPIRES_IN

Respuesta Exitosa

```
{
  "user": { "email": "usuario@email.com", "name": "Nombre Usuario"
```

```
},
  "role": "admin|user|guest",
  "accessToken": "jwt_token",
  "tokenType": "Bearer",
  "expiresIn": "15m"
}
```

Manejo de Errores

400: Credential requerido

401: Token inválido o expirado

403: Email no verificado