DOCUMENTACIÓN: SERVICIO DE JWT (JSON WEB TOKENS)

DESCRIPCIÓN GENERAL

Este módulo proporciona servicios criptográficos para la generación y verificación de tokens JWT utilizados en el sistema de autenticación. Su función principal es crear tokens seguros para sesiones de usuario y validar su integridad en solicitudes posteriores, implementando el estándar JWT con algoritmos criptográficos robustos.

FUNCIONALIDAD PRINCIPAL

El servicio maneja todo el ciclo de vida de los tokens JWT, desde la creación inicial durante el proceso de autenticación hasta la verificación en cada solicitud protegida. Implementa las mejores prácticas de seguridad para tokens web JSON.

GENERACIÓN DE TOKENS

FIRMA CRIPTOGRÁFICA

Utiliza el algoritmo HS256 (HMAC con SHA-256) para firmar digitalmente los tokens, asegurando su integridad y autenticidad. Este algoritmo proporciona un balance óptimo entre seguridad y rendimiento para aplicaciones web.

ESTRUCTURA DEL PAYLOAD

Crea tokens que contienen información esencial del usuario necesaria para la autorización, incluyendo identificador único, correo electrónico, nombre completo y rol dentro del sistema. Esta información se incluye en el payload del token para evitar consultas recurrentes a la base de datos.

GESTIÓN DE EXPIRACIÓN

Configura tiempos de expiración específicos para los tokens basados en las variables de entorno, permitiendo ajustar la seguridad según los requisitos de la aplicación. Los tokens expirados son automáticamente rechazados durante la verificación.

VERIFICACIÓN DE TOKENS

VALIDACIÓN CRIPTOGRÁFICA

Verifica la firma digital de los tokens recibidos para asegurar que no han sido alterados después de su emisión. Esta validación previene ataques de modificación de tokens.

EXTRACCIÓN DE INFORMACIÓN

Decodifica el payload del token y extrae la información del usuario, haciendo disponible los datos de identidad para los middlewares y controladores subsiguientes sin necesidad de acceder a la base de datos.

SEGURIDAD IMPLEMENTADA

CLAVE SECRETA ROBUSTA

Utiliza una clave secreta derivada de las variables de entorno, codificada apropiadamente para uso criptográfico. La fortaleza de esta clave es fundamental para la seguridad del sistema de tokens.

BUENAS PRÁCTICAS JWT

Implementa configuraciones seguras incluyendo timestamps de emisión, expiración controlada y headers de protección adecuados, siguiendo las recomendaciones del estándar JWT.

INTEGRACIÓN CON EL SISTEMA DE AUTENTICACIÓN

Este servicio se integra directamente con el middleware de autenticación, proporcionando las funciones necesarias para verificar tokens en cada solicitud protegida. También es utilizado por el controlador de autenticación de Google para emitir tokens propios después de la validación exitosa con el proveedor externo.

GENERACIÓN DE CLAVES SEGURAS

Incluye documentación para la generación segura de claves JWT utilizando herramientas criptográficas nativas de Node.js, asegurando que las claves utilizadas en producción tengan la entropía suficiente para resistir ataques de fuerza bruta.

BENEFICIOS DE LA IMPLEMENTACIÓN

ESTADO SIN SESIÓN

Permite una arquitectura sin estado donde el servidor no necesita mantener información de sesión, escalando horizontalmente sin problemas de consistencia.

EFICIENCIA EN RENDIMIENTO

Reduce la carga en la base de datos al evitar consultas recurrentes para validar la autenticación del usuario en cada solicitud.

SEGURIDAD CONFIABLE

Implementa estándares industry-recognized para autenticación basada en tokens, proporcionando un nivel de seguridad apropiado para aplicaciones web modernas.

INTEROPERABILIDAD

Los tokens generados son compatibles con el estándar JWT, permitiendo su uso potencial con otros sistemas y herramientas que soporten este formato ampliamente adoptado.