Middlewares\Auth.js

```
// Importamos el módulo jsonwebtoken
const jwt = require('jsonwebtoken');

// Importamos la llave secreta desde la configuración del entorno
const llave = require('dotenv').config().parsed.SECRET_KEY;

//Importamos el logger
const logger = require('../Config/logger');

// Exportamos un middleware que verifica el token JWT
module.exports = (req,res,next) =>{
    // Obtenemos el token de autorización de los encabezados de la solicitud
    const headerAuth = req.headers.authorization;

    // Si no se proporcionó el token, enviamos un mensaje de error
    if(!headerAuth){
        logger.error('No se proporcionó token.');
        res.status(401).send({
            message: "No se proporcionó token"
        });
        return;
    }

    // Extraemos el token del encabezado de autorización
    const token = headerAuth.split(' ')[1]; // Bearer token

    // Verificamos el token
    jwt.verify(token, llave, (err,decoded) =>{
        // Si hay un error (por ejemplo, el token es inválido), enviamos un mensaje de error
        if(err){
            logger.error('Token inválido. ', err);
            res.status(401).send({
                message: "Token inválido"
            });
            return;
        }else{
            // Si el token es válido, lo decodificamos y lo adjuntamos a la solicitud
            req.decoded = decoded;
        }

        // Pasamos al siguiente middleware
        next();
    });
}
```