# Relatório de Segurança – Tópico 5.3

## Objetivo

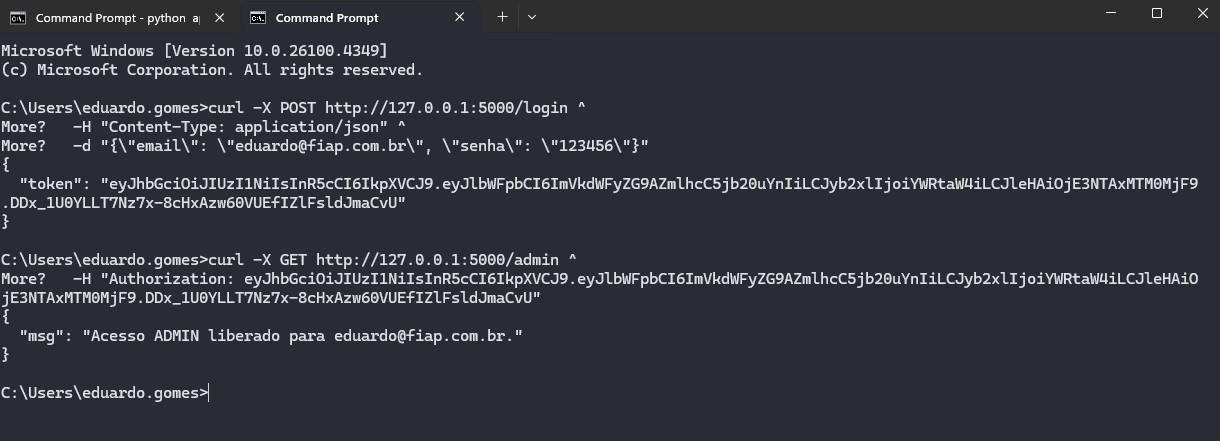
Implementar princípios de Zero Trust Architecture (ZTA), que pressupõem verificação contínua de identidade e controle de acesso, garantindo que cada requisição a um recurso protegido seja autenticada, autorizada e monitorada, mesmo dentro da rede.

## Ações Realizadas

- Criado endpoint de autenticação que gera token JWT com nível de acesso (role).  
- Implementado endpoint `/admin` acessível apenas a usuários com perfil `admin`.  
- Acesso condicionado à validação de token, assinatura e permissões.  
- Toda requisição a endpoint protegido é verificada: identidade, validade e privilégio mínimo.  
- Criado log (`access.log`) para auditoria dos acessos.

## Evidência

Terminal demonstrando acesso autorizado à rota `/admin` com perfil `admin` e token JWT válido.



## Conclusão

A arquitetura Zero Trust oferece uma abordagem robusta de segurança ao assumir que nenhum ponto da rede é confiável por padrão.   
Ao aplicar validações rigorosas em todas as requisições, o sistema se torna mais resiliente contra acessos indevidos e eleva o nível de proteção de dados e serviços.