

Implementação de Hash para Integridade de Documentos

Arquivos Criados

1. **src/integrity/integrity.service.ts**
 - Serviço responsável pela geração e verificação de hashes SHA-256
 - Implementa métodos para gerar, armazenar e verificar hashes de documentos
2. **src/integrity/integrity.module.ts**
 - Módulo que registra o IntegrityService
 - Gerencia as dependências do serviço de integridade
3. **src/migrations/1683456789000-IntegrityHashColumns.ts**
 - Migração para adicionar as colunas de hash à tabela de documentos
 - Adiciona hashOriginal e hashSigned à tabela documents
4. **src/config/typeorm.config.ts**
 - Configuração do TypeORM para execução de migrações
 - Define a conexão com o banco de dados e as entidades/migrações

Arquivos Modificados

1. **src/document/document.entity.ts**
 - Adicionados campos hashOriginal e hashSigned para armazenar os hashes
2. **src/document/document.module.ts**
 - Adicionado IntegrityModule aos imports
 - Configurado forwardRef para resolver dependências circulares
3. **src/document/document.service.ts**
 - Injetado IntegrityService no construtor
 - Modificado método create para gerar e armazenar hash do documento original
 - Adicionado método generateFinalDocument para gerar e armazenar hash do documento final
4. **src/document/document.controller.ts**
 - Adicionado IntegrityService ao construtor
 - Implementados endpoints para verificar integridade do documento:
 - GET /api/documents/:id/integrity
 - POST /api/documents/:id/integrity/verify
5. **src/app.module.ts**
 - Adicionado IntegrityModule aos imports do módulo principal
6. **package.json**
 - Adicionados scripts para gerenciar migrações do TypeORM

Funcionalidades Implementadas

1. Geração de Hash SHA-256

- Hash gerado automaticamente no upload do documento original
 - Hash gerado para o documento final após todas as assinaturas
2. **Armazenamento de Hash**
 - Hash original armazenado no campo hashOriginal
 - Hash do documento assinado armazenado no campo hashSigned
 3. **Verificação de Integridade**
 - Endpoint para verificar se o documento possui hash
 - Endpoint para recalculer o hash e comparar com o armazenado

Como Executar a Migração

Para adicionar as colunas de hash ao banco de dados, execute:

```
npm run migration:run
```

Como Testar

1. **Upload de Documento**
 - Faça upload de um documento para gerar o hash original
2. **Verificar Hash Original**
 - Use o endpoint GET /api/documents/:id/integrity
3. **Verificar Integridade**
 - Use o endpoint POST /api/documents/:id/integrity/verify

Considerações de Segurança

- Os hashes SHA-256 são considerados seguros para verificação de integridade
- A verificação de integridade ajuda a detectar alterações não autorizadas nos documentos
- Recomenda-se implementar medidas adicionais de segurança, como assinaturas digitais com certificados