Controle de Acesso

Categorização de Privilégios e Níveis de Risco

Em Ciência de Dados, o acesso irrestrito é o maior risco de segurança.

Abertura: O Maior Risco de Segurança

Em Ciência de Dados, o acesso irrestrito é o maior risco de segurança. Um usuário com permissões excessivas pode, intencionalmente ou por erro, comprometer dados críticos, violar conformidade legal e prejudicar o negócio.

O que é Controle de Acesso? Conjunto de políticas e mecanismos que garantem que cada usuário e sistema tenha apenas as permissões estritamente necessárias para realizar seu trabalho. É a base da segurança em qualquer sistema de dados.

Privilégio (Permissão)

Ação específica que um usuário pode realizar em um banco de dados. Exemplos: SELECT (ler), INSERT (adicionar), UPDATE (modificar), DELETE (remover).

Papel (Role)

Grupo de usuários com responsabilidades similares. Ao invés de conceder privilégios a cada usuário, concedemos a um Papel. Exemplo: role_vendedor, role_medico, role_dba.

Princípio do Mínimo Privilégio (PoLP)

Regra de ouro da segurança: conceder a MENOR quantidade de privilégios possíveis para executar uma tarefa. Não conceder "tudo" por conveniência.

Por que isso importa para LGPD? A Lei Geral de Proteção de Dados (LGPD) exige que organizações protejam dados pessoais. Controle de acesso inadequado pode resultar em vazamento de dados, multas pesadas e danos à reputação. Implementar PoLP é conformidade legal obrigatória.

Conceitos Essenciais: Privilégio, Usuário, Papel e PoLP

O QUE É UM PRIVILÉGIO?

Um privilégio é uma ação específica que um usuário pode realizar em um banco de dados. Exemplos:

```
• SELECT: Ler dados (Baixo Risco)
• INSERT: Adicionar novos dados (Médio Risco)
• UPDATE: Modificar dados existentes (Alto Risco)
• DELETE: Remover dados (Crítico)
• CREATE/ALTER/DROP: Modificar estrutura (Crítico)
```

Usuário (Indivíduo)

Pessoa ou sistema específico. Exemplo: "João Silva", "api_integracao_001". Conceder privilégios a cada usuário individualmente é difícil de manter.

Papel (Role)

Grupo de usuários com responsabilidades similares. Exemplo: "role_vendedor", "role_medico". Conceder privilégios a papéis é mais fácil de manter e auditar.

PRINCÍPIO DO MÍNIMO PRIVILÉGIO (POLP)

Conceder a MENOR quantidade de privilégios possíveis para executar uma tarefa. Não conceder "tudo" por conveniência.

✓ CORRETO (POLP)

```
GRANT SELECT ON clientes
TO role_vendedor;
```

❌ INCORRETO (VIOLANDO POLP)

```
GRANT ALL ON *
TO role_vendedor;
```

Classificação de Privilégios SQL: DML

Data Manipulation Language - Manipulação de Dados

SELECT

Ler dados do banco. Apenas visualização, sem modificação.

NÍVEL DE RISCO

BAIXO

Impacto: Sem prejuízo financeiro. Erro não causa dano.

EXEMPLO

```
SELECT * FROM clientes;
```

INSERT

Adicionar novos dados ao banco. Pode poluir dados ou criar duplicatas.

NÍVEL DE RISCO

MÉDIO

Impacto: Dados inválidos, reversível com DELETE.

EXEMPLO

```
INSERT INTO vendas
VALUES (1, 100, '2025-01-15');
```

UPDATE

Modificar dados existentes. Pode alterar dados críticos ou financeiros.

NÍVEL DE RISCO

ALTO

Impacto: Dados críticos alterados, reversível com esforço.

EXEMPLO

```
UPDATE produtos
SET preco = 150
WHERE id = 5;
```

DELETE

Remover dados do banco. Perda irreversível se sem backup.

NÍVEL DE RISCO

CRÍTICO

Impacto: Perda permanente, viola auditoria fiscal.

EXEMPLO

```
DELETE FROM vendas
WHERE cliente_id = 10;
```

Classificação de Privilégios SQL: DDL

DDL (Data Definition Language): Comandos que modificam a estrutura do banco de dados (tabelas, índices, schemas). Diferente de DML, que modifica dados. DDL é CRÍTICO porque pode destruir estruturas inteiras.

CREATE

DESCRIÇÃO

Criar novas tabelas, índices, schemas, views. Estrutura permanente.

RISCO

CRÍTICO

RESTRIÇÃO

Apenas DBAs e sistemas de migração automatizada. Nunca conceder a desenvolvedores.

EXEMPLO

```
CREATE TABLE clientes ( id INT PRIMARY KEY, nome VARCHAR(100) );
```

ALTER

DESCRIÇÃO

Modificar estrutura existente: adicionar/remover colunas, alterar tipos, renomear.

RISCO

CRÍTICO

RESTRIÇÃO

Apenas DBAs. ALTER em produção pode causar downtime. Requer planejamento.

EXEMPLO

```
ALTER TABLE clientes ADD COLUMN email VARCHAR(100);
```

DROP

DESCRIÇÃO

Deletar tabelas, índices, schemas, views. Perda IRREVERSÍVEL de estrutura.

RISCO

CRÍTICO

RESTRIÇÃO

Apenas DBAs. DROP em produção é desastre. Exigir backup e aprovação.

EXEMPLO

```
DROP TABLE clientes; -- ⚠️ CUIDADO: Perda irreversível!
```

⚠️ **NUNCA conceder CREATE, ALTER ou DROP a usuários normais. Apenas DBAs e sistemas de migração automatizada com auditoria ativa. Violação desta regra = risco crítico de segurança e integridade.**

Níveis de Risco: Escala de Impacto

1 Baixo Risco

DEFINIÇÃO
Ação de leitura em dados não sensíveis. O erro não causa prejuízo financeiro ou legal.

EXEMPLOS
SELECT em catálogo de produtos, SELECT em logs públicos, SELECT em dados de referência.

IMPACTO
Sem prejuízo. Pode ser concedido amplamente a muitos usuários.

2 Médio Risco

DEFINIÇÃO
Ação de escrita que adiciona dados ou altera dados não financeiros. O erro é reversível.

EXEMPLOS
INSERT em vendas, UPDATE em telefone de cliente, INSERT em vacinações, UPDATE em logs.

IMPACTO
Reversível com esforço. Requer auditoria. Conceder apenas a papéis específicos.

3 Alto Risco

DEFINIÇÃO
Ação que envolve alteração de dados críticos (financeiros, pessoais) ou exclusão reversível.

EXEMPLOS
UPDATE em salário, UPDATE em preço de produto, UPDATE em CPF, DELETE com soft-delete.

IMPACTO
Impacto financeiro direto. Requer auditoria ativa. Conceder apenas a gerentes.

4 Risco Crítico

DEFINIÇÃO
Ação que causa perda irreversível de dados, afeta segurança do sistema ou viola leis.

EXEMPLOS
DELETE de clientes, DROP TABLE, ALTER TABLE, UPDATE em dados de auditoria, DELETE em vendas.

IMPACTO
Perda permanente. Violação legal (LGPD). Restrito a DBAs e sistemas automatizados.

Cenários Práticos: Clínica, Loja Virtual, RH

Clínica de Saúde

PAPÉIS

- Médico
- Enfermeiro
- Recepcionista
- DBA

TABELAS

- pacientes
- consultas
- vacinacoes

EXEMPLO

```
GRANT SELECT ON
pacientes TO
role_medico;
```

RISCO TÍPICO

ALTO RISCO

Loja Virtual

PAPÉIS

- Vendedor
- Analista BI
- Gerente Catálogo
- Atendente Suporte
- DBA

TABELAS

- clientes
- produtos
- vendas

EXEMPLO

```
GRANT SELECT,
INSERT ON vendas
TO role_vendedor;
```

RISCO TÍPICO

CRÍTICO

RH da Empresa

PAPÉIS

- Gerente RH
- Analista RH
- Recepcionista RH
- Funcionário
- DBA

TABELAS

- funcionarios
- faltas
- ferias

EXEMPLO

```
GRANT UPDATE
(salario) ON
funcionarios TO
role_gerente_rh;
```

RISCO TÍPICO

CRÍTICO

Atividade em Grupo: Classificação de Cenários

Contexto: Divida a turma em grupos de 3-4 alunos. Cada grupo receberá 3 cenários de negócio de contextos diferentes (Clínica, Loja Virtual, RH). A tarefa é preencher a tabela, definindo o Privilégio Necessário (SQL) e o Nível de Risco (Baixo, Médio, Alto, Crítico). Tempo: 20-25 minutos.

Passos da Atividade

1. **Entender o Contexto**
   Leia o cenário de negócio atribuído ao seu grupo (Clínica, Loja Virtual ou RH). Identifique os usuários, papéis e dados envolvidos.

2. **Analisar a Tarefa Específica**
   Para cada tarefa (ex: "Registrar uma nova venda"), determine qual privilégio SQL é necessário (SELECT, INSERT, UPDATE, DELETE, CREATE, ALTER, DROP).

3. **Classificar o Nível de Risco**
   Avalie o impacto: Baixo (leitura, sem prejuízo), Médio (escrita reversível), Alto (dados críticos), Crítico (perda irreversível, LGPD).

4. **Justificar a Classificação**
   Prepare uma justificativa breve (1-2 frases) explicando por que escolheu esse nível de risco. Exemplo: "DELETE é Crítico porque causa perda irreversível de dados de auditoria fiscal."

9 CENÁRIOS PARA CLASSIFICAÇÃO (3 POR CONTEXTO)

🏥 CLÍNICA

1. Consultar histórico de exames de um paciente
2. Inserir novo registro de vacinação
3. Alterar telefone de contato do paciente

🛒 LOJA VIRTUAL

4. Adicionar novo produto ao catálogo
5. Visualizar dados de endereço e CPF dos clientes
6. Excluir todos os pedidos de um cliente (LGPD)

👔 RH

7. Alterar o valor do salário de um funcionário
8. Cadastrar um novo funcionário
9. Consultar a lista de faltas do mês

FORMATO ESPERADO DA RESPOSTA

Cenário	Tarefa Específica	Privilégio	Nível de Risco
Clínica	Consultar histórico de exames	SELECT	Baixo
Loja Virtual	Excluir pedidos (LGPD)	DELETE	Crítico

Matriz de Decisão: Quando Conceder Privilégios?

Use este fluxograma para tomar decisões sobre concessão de privilégios. Responda as 3 perguntas sequencialmente. Se em qualquer ponto a resposta for NÃO, não conceda o privilégio.

PERGUNTA 1

O papel realmente precisa MODIFICAR dados?

✓ SIM	✗ NÃO
Ir para Pergunta 2	Não conceder. Apenas SELECT.

↓

PERGUNTA 2

Qual é o impacto se o privilégio for mal utilizado?

✓ BAIXO/MÉDIO	✗ ALTO/CRÍTICO
Ir para Pergunta 3	Ir para Pergunta 3

↓

PERGUNTA 3

Há alternativa menos arriscada?

✓ SIM	✗ NÃO
Usar alternativa (ex: UPDATE com restrição)	Conceder com auditoria ativa

EXEMPLOS PRÁTICOS

Caso 1: Vendedor registra vendas

```
P1: Precisa modificar? SIM
P2: Impacto? MÉDIO
P3: Alternativa? NÃO
```

✓ CONCEDER: INSERT em vendas

Caso 2: Atendente corrige CPF

```
P1: Precisa modificar? SIM
P2: Impacto? CRÍTICO
P3: Alternativa? SIM
```

✗ NÃO CONCEDER UPDATE em CPF

Caso 3: Analista BI gera relatórios

```
P1: Precisa modificar? NÃO
```

✓ CONCEDER: SELECT apenas

Debate: Alto vs Crítico - Qual a Diferença?

O que diferencia um Risco Alto de um Risco Crítico? Ambos envolvem UPDATE, mas com impactos muito diferentes. Vamos explorar.

Alto Risco

Exemplo 1: UPDATE em Nome do Produto

SQL: UPDATE produtos SET nome = 'Novo Nome' WHERE id = 5;

Exemplo 2: UPDATE em Telefone do Cliente

SQL: UPDATE clientes SET telefone = '11999999999' WHERE id = 10;

Por que é Alto Risco?

- Afeta dados importantes, mas reversível com backup
- Impacto operacional, sem violação legal imediata
- Pode ser corrigido com UPDATE novamente
- Requer auditoria, mas não é desastre

Risco Crítico

Exemplo 1: UPDATE em Preço do Produto

SQL: UPDATE produtos SET preco = 10 WHERE id = 5;

Exemplo 2: UPDATE em CPF do Cliente

SQL: UPDATE clientes SET cpf = '12345678901' WHERE id = 10;

Por que é Crítico?

- Afeta dados financeiros ou de identidade
- Impacto financeiro direto ou violação LGPD
- Pode comprometer auditoria fiscal e legal
- Requer aprovação de múltiplos níveis

QUESTÕES PARA DEBATE EM SALA

? **Pergunta 1:** Se UPDATE em nome do produto é Alto Risco, por que UPDATE em preço é Crítico? Qual é a diferença fundamental?

? **Pergunta 2:** UPDATE em CPF é Crítico porque viola LGPD. Mas e UPDATE em data de nascimento? Seria Alto ou Crítico? Por quê?

? **Pergunta 3:** Em um banco de dados de saúde, UPDATE em diagnóstico seria Alto ou Crítico? Justifique sua resposta considerando impacto legal e financeiro.

? **Pergunta 4:** Como você definiria a "linha" entre Alto Risco e Crítico? Qual é o critério decisivo?

Conclusão: Do Risco para GRANT/REVOKE

O CAMINHO PERCORRIDO NESTA AULA

1. **Conceitos Essenciais**
2. **Classificação DML/DDL**
3. **Níveis de Risco**
4. **Aplicação Prática**

PRÓXIMO PASSO: TRADUZIR RISCO EM COMANDOS SQL

A categorização de privilégios e níveis de risco que aprendemos hoje é o PRIMEIRO PASSO. O próximo passo será traduzir essas decisões em comandos SQL GRANT (conceder) e REVOKE (revogar). Exemplo:

```
GRANT SELECT ON pacientes TO role_medico;
GRANT SELECT, INSERT ON vendas TO role_vendedor;
REVOKE DELETE ON vendas FROM role_vendedor;
```

CHECKLIST DE APRENDIZADOS

- ✓ Entendi o Princípio do Mínimo Privilégio (PoLP)
- ✓ Entendo por que DDL (CREATE, ALTER, DROP) é crítico
- ✓ Consigo aplicar esses conceitos em cenários reais (Clínica, Loja, RH)
- ✓ Consigo classificar privilégios DML (SELECT, INSERT, UPDATE, DELETE)
- ✓ Consigo avaliar o nível de risco de uma ação (Baixo, Médio, Alto, Crítico)
- ✓ Entendo a importância do controle de acesso para LGPD e conformidade

"Segurança em Ciência de Dados não é apenas tecnologia, é responsabilidade." *Como Engenheiros de Dados, somos guardiões de dados críticos. Cada decisão sobre quem pode acessar o quê impacta a privacidade, segurança e conformidade legal da organização. Use o poder do controle de acesso com sabedoria.*