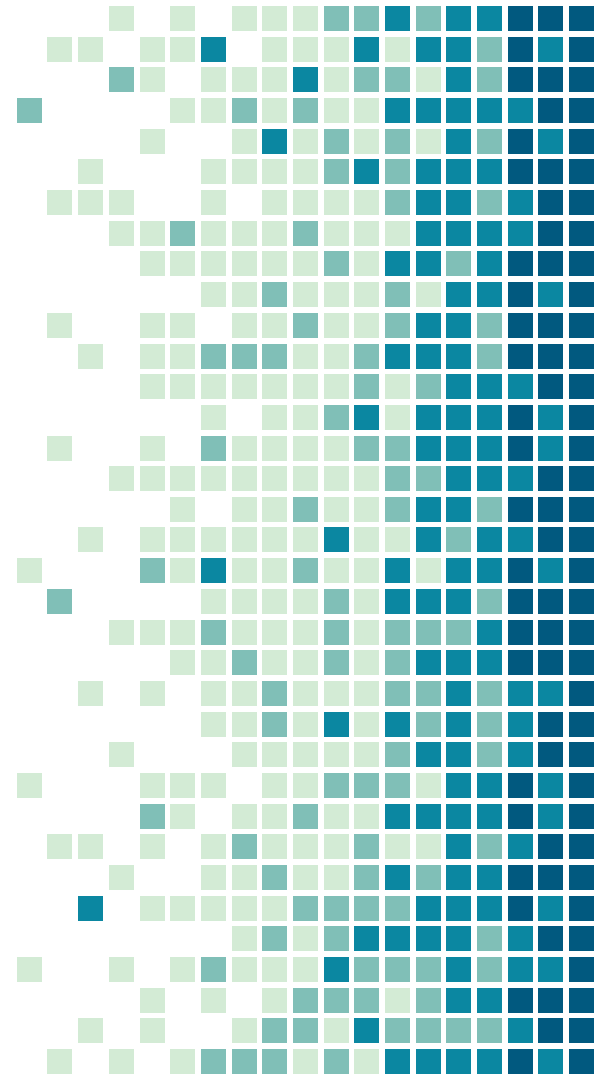


Banco de Dados I

Rebeca Barros



Segurança de Banco de Dados



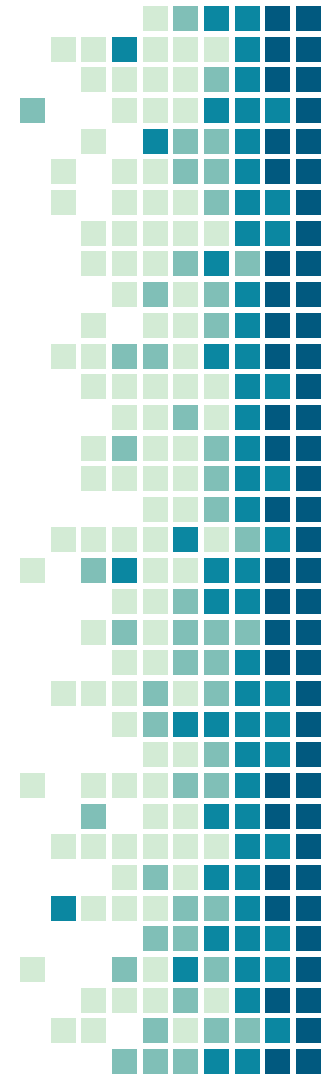
Tipos de Segurança

- A segurança é uma área ampla, que tenta resolver muitos problemas, entre eles:
 - Questões legais e éticas com relação ao direito de acessar certas informações;
 - Questões políticas em nível governamental, institucional ou corporativo sobre o que pode ou não ser público;



Tipos de Segurança

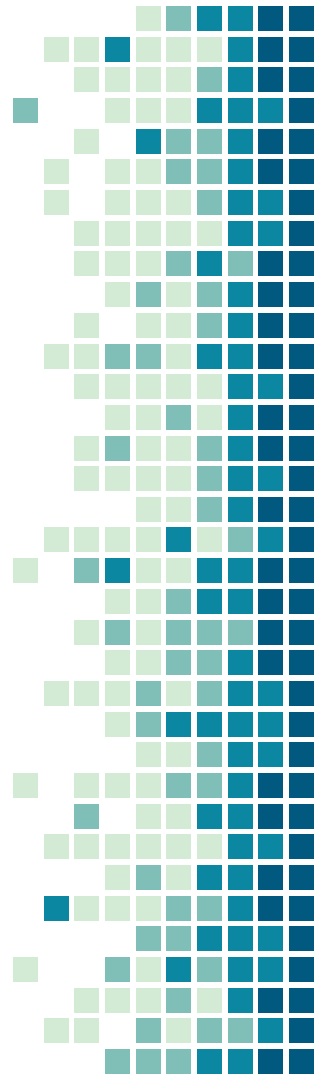
- Questões relacionadas ao sistema, como os níveis de sistema onde a segurança deve ser imposta. Físico, operacional, SGBD?
- Identificação de níveis de segurança e categorizar os dados/usuários de acordo com esses níveis.



Objetivos da Segurança

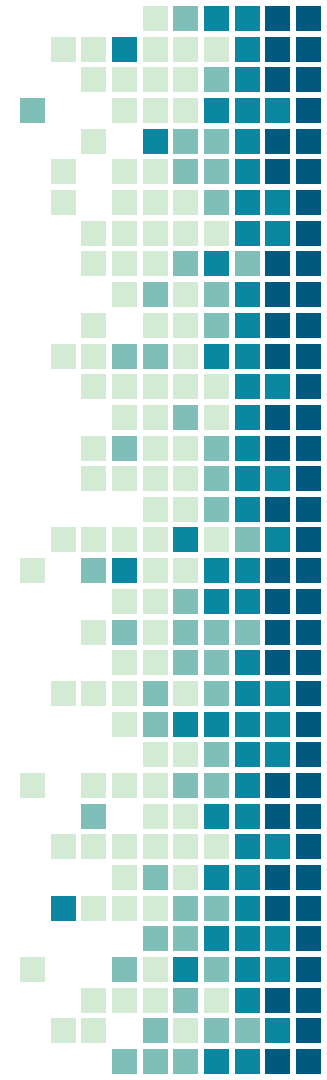
- **Integridade:** informação protegida contra modificações impróprias.
- **Disponibilidade:** informação disponível a um usuário que têm um direito legítimo sobre a mesma.
- **Confidencialidade:** proteção dos dados contra exposição não autorizada.

Ameaças aos banco de dados podem resultar na perda ou degradação de alguns ou todos os objetivos de segurança.



Medidas de Controle

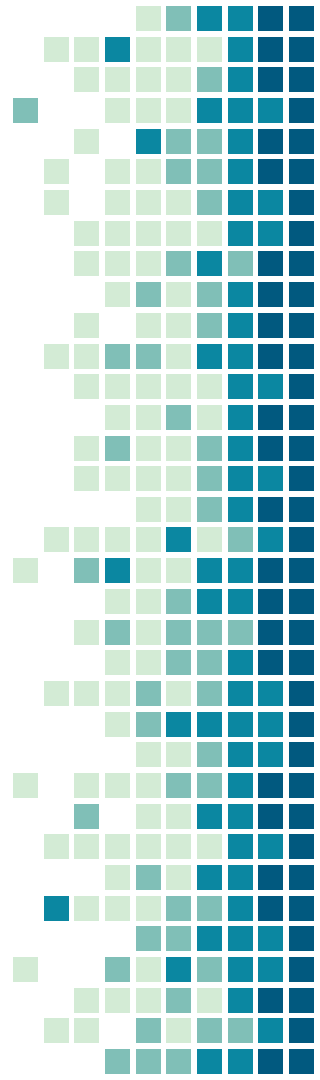
- Controle de Acesso;
- Controle de Inferência;
- Criptografia.



Controle de Acesso

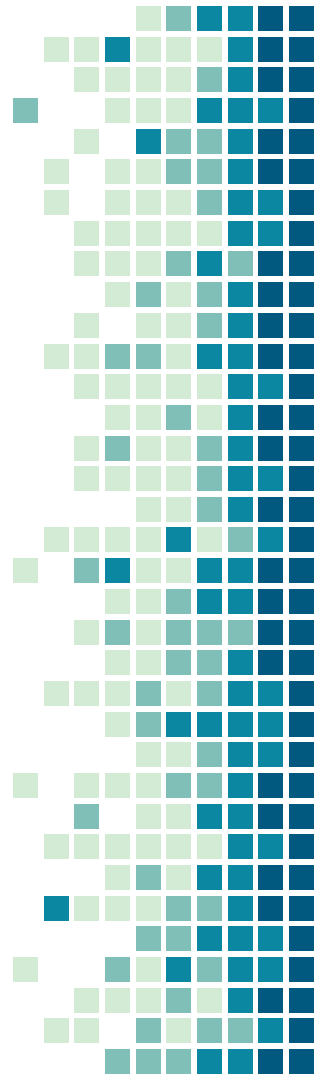
- É responsabilidade do administrador do BD e do administrador de segurança impor coletivamente as políticas de segurança de uma organização.
- Isso indica se o acesso deve ser permitido ou não a certo atributo do BD (coluna, tabela...) para usuários individuais ou para categoria de usuários.

■



Controle de Acesso

- 3 fatores importantes para decidir sobre revelar os dados são:
 - **Disponibilidade dos dados:** (normalmente tratado pelo controle de concorrência);
 - **Aceitabilidade de acesso:** Os dados só devem ser revelados a usuários autorizados.
 - **Garantia de autenticidade:** antes de conceder acesso, certas características externas sobre o usuário também podem ser consideradas.

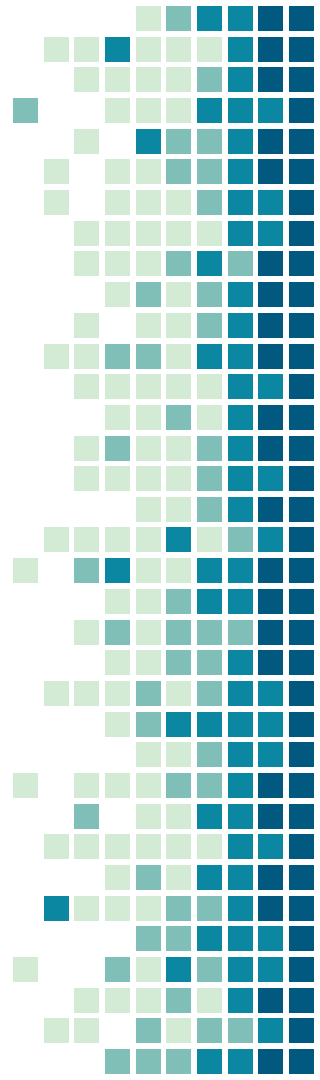


Controle de Acesso

- Dois níveis informais para definição de privilégios na utilização de um Banco de Dados:
 - **Nível de conta:** CREATE SCHEMA, CREATE TABLE, CREATE VIEW, ALTER, DROP, MODIFY, SELECT.
 - **Nível de tabela:** controlar o privilégio para acessar cada tabela ou visão individual do BD;

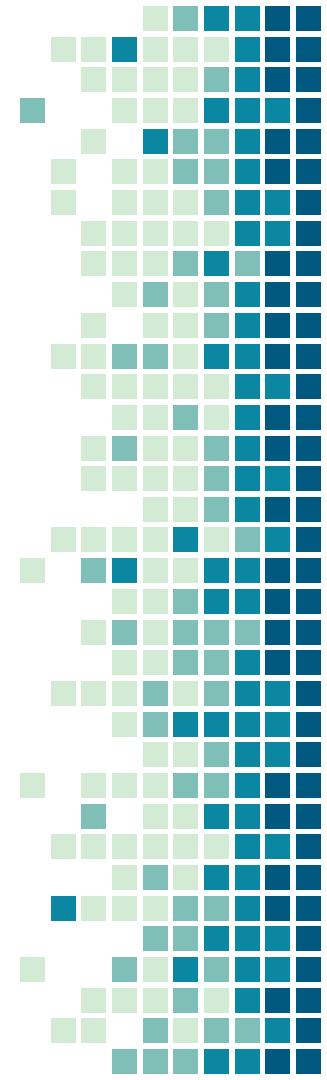
Controle de Acesso

- **Matriz de acesso;**
- Em SQL, os seguintes privilégios podem ser concedidos para cada tabela:
 - SELECT - para recuperação ou leitura;
 - Modificação (UPDATE, DELETE, INSERT);
 - Privilégio de referência - capacidade de referenciar uma tabela ao especificar restrições de integridade.



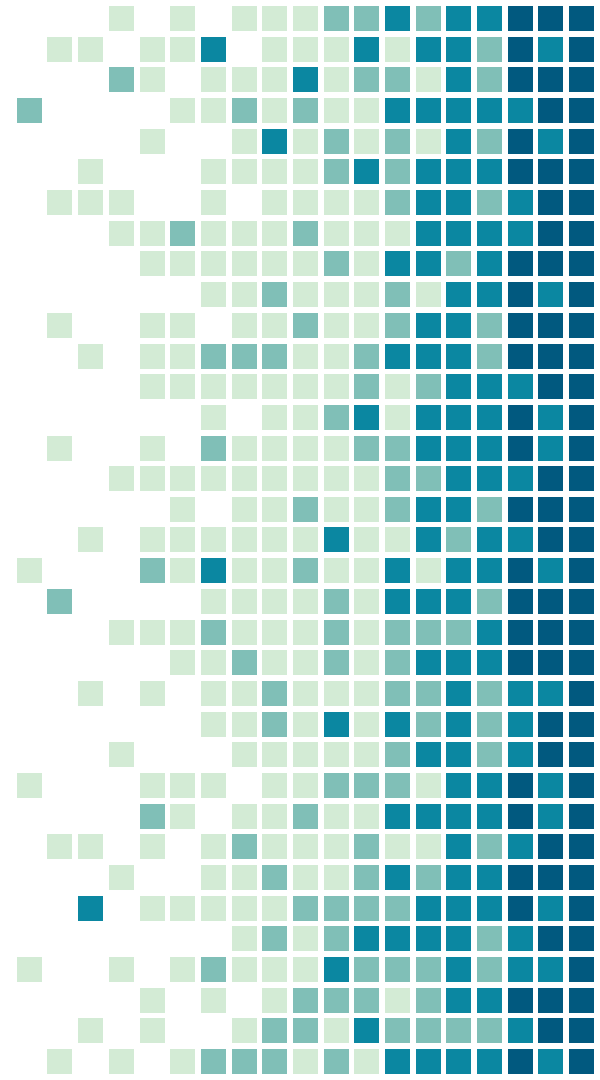
Controle de Acesso

- Revogar privilégios: **REVOKE;**
- Propagação de privilégios: **GRANT OPTION**



Segurança de Banco de Dados

Controle de Acesso no MYSQL



Tipos de Privilégios

Manipular os dados (DML)

- SELECT, INSERT, UPDATE, DELETE, EXECUTE

Modificar estrutura do BD (DDL)

- CREATE, ALTER, DROP (TABLE, VIEWS, INDEX, TRIGGER, EVENTS, PROCEDURE)

Administrativos

- CREATE USER, RELOAD, SHUTDOWN, SHOW DATABASES

Outros

- ALL, GRANT OPTION, USAGE

SHOW PRIVILEGES;

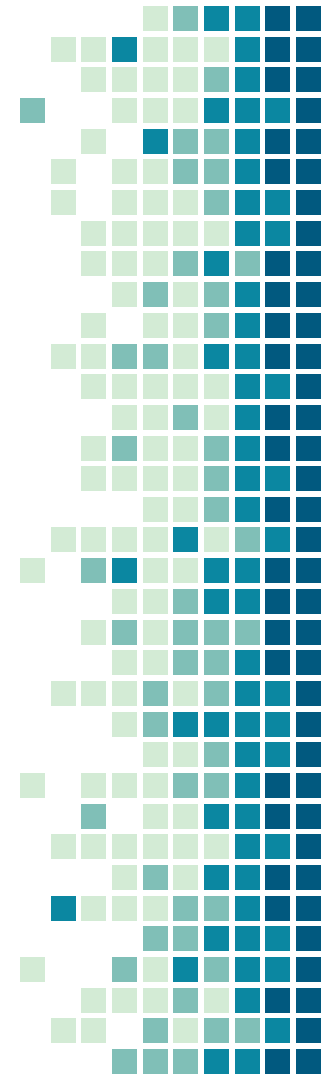
Níveis de Privilégios

Global

Database

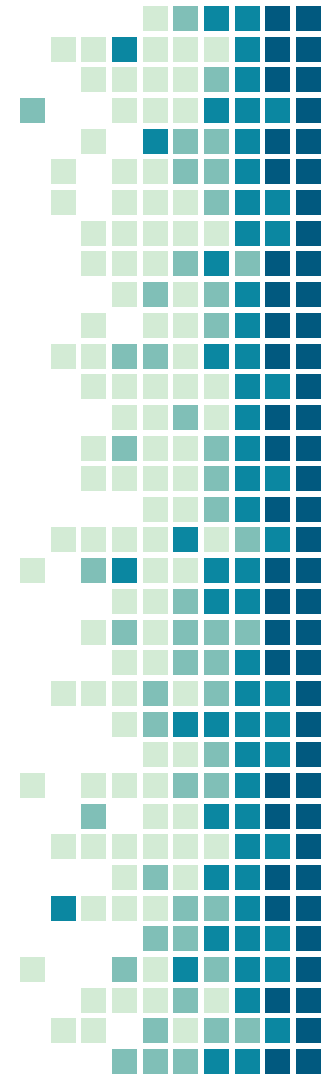
Table

Column



Níveis de Privilégios

- `use mysql;`
- Tabelas de Privilégios: `user`, `db`, `tables_priv`, `columns_priv`;



Criando Usuários

- `CREATE USER username IDENTIFIED BY password`
 - `CREATE USER usuario1 IDENTIFIED BY 'senha1'`
 - `CREATE USER admin IDENTIFIED BY 'admin1'`

Concedendo Privilégios

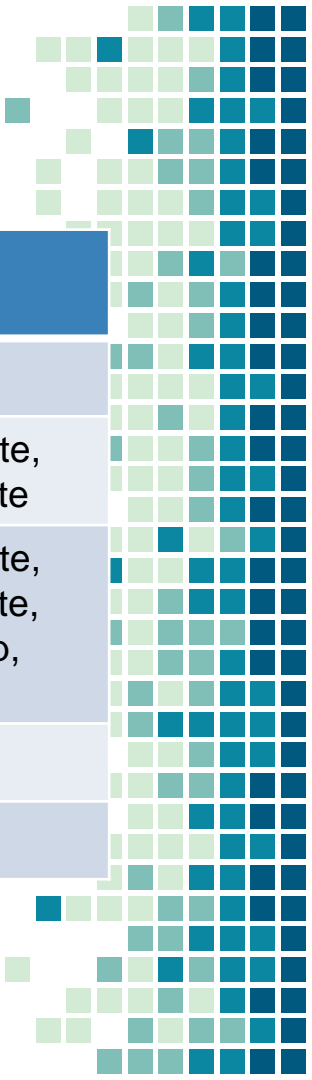
- `GRANT lista_privilégios ON [banco.]tabela TO username IDENTIFIED BY password [WITH GRANT OPTION]`
 - `GRANT ALL ON *.* TO admin IDENTIFIED BY 'admin1';`
 - `GRANT SELECT, INSERT, UPDATE, DELETE ON ap.* TO usuario1@localhost IDENTIFIED BY 'senha1' WITH GRANT OPTION;`

Concedendo Privilégios

- `GRANT SELECT, INSERT, UPDATE ON ap.vendedores TO usuario1@localhost IDENTIFIED BY 'senha1' ;`
- `GRANT SELECT (vendedor_nome, vendedor_estado, vendedor_cep), UPDATE (vendedor_endereco1) ON ap.vendedores TO usuario1@localhost IDENTIFIED BY 'senha1' ;`

Revogando Privilégios

- **REVOKE** *lista_privilégios* **ON** *[banco.]tabela* **FROM** *username*
 - **REVOKE ALL, GRANT OPTION FROM**
usuariol
 - **REVOKE UPDATE, DELETE ON**
ap.faturas FROM
usuariol@localhost



Usuário	Banco de Dados	Tabela	Coluna	Privilégios
admin	*	*	*	*
usuario1	bdAcademia	*	*	Insert, Update, Select, Delete
usuario2	bdAcademia	*	*	Insert, Update, Select, Delete, Create, Drop, Alter, Grant
Usuario3	bdAcademia	Pagamento	*	Select
Usuario4	bdAcademia	Pagamento	valor	Select