re_S19_A3_SL6_backend

Entrega AVA

Nome: _____ Turma: _____

Título da atividade: Protegendo dados – Segurança em banco de dados

1. Introdução

A segurança de bancos de dados é essencial para proteger informações sensíveis e garantir a conformidade com regulamentos.

2. Conceitos fundamentais

2.1 Controle de acesso

2.1.1 Políticas de permissões para diferentes níveis de usuários.

2.1.2 Princípio do menor privilégio: usuários recebem apenas as permissões necessárias.

2.2 Criptografia de dados

2.2.1 Em trânsito: protege dados enviados entre cliente e servidor.

2.2.2 Em repouso: garante que dados armazenados estejam criptografados.

3. Monitoramento e auditoria

3.1 Registro de atividades para identificar acessos suspeitos.

3.2 Alertas para tentativas de invasão.

4. Exemplo prático

Uma clínica médica deseja proteger informações de pacientes em seu banco de dados. Os objetivos são:

4.1 Configurar usuários com permissões específicas.

4.2 Implementar criptografia de dados sensíveis.

4.3 Monitorar acessos e gerar relatórios de auditoria.

5. Passo a passo

5.1 Definam permissões para médicos, administradores e recepcionistas.

5.2 Habilitem criptografia no banco de dados para proteger dados como CPF e histórico médico.

5.3 Configurem auditorias automáticas para registrar acessos e alterações.

Situação-problema

Vocês receberam uma mensagem no Teams:

“Precisamos garantir que apenas usuários autorizados possam acessar dados sensíveis no banco de dados. Além disso, precisamos de um plano para monitorar atividades suspeitas. Como vocês implementariam isso?”

Situação fictícia produzida pela SEDUC-SP.

Perguntas dissertativas

1. Por que o princípio do menor privilégio é importante?
2. Como a criptografia protege os dados em trânsito e em repouso?
3. Como implementar um sistema de auditoria eficiente?
4. Quais práticas podem prevenir acessos não autorizados ao banco?