**Atividade 1**

**Contexto**

Um dos clientes – uma loja de eletrônicos do sistema para vendas oferecido pela empresa de desenvolvimento de *software* na qual você trabalha – relatou problemas graves com o banco de dados. Os problemas foram os seguintes:

* Um acesso indevido aconteceu no banco de dados. As hipóteses são de SQL *injection* ou de uso indevido de *login* e senha de funcionário.
* O acesso indevido apagou dados das tabelas de venda e pagamento.
* Um dos funcionários da loja emite periodicamente alguns relatórios com consultas diretas ao banco de dados. Essa pessoa, ao tentar ajudar, acabou removendo ainda duas tabelas. Nota-se que ela usava usuário **root**.
* O último *backup* anterior ao desastre aconteceu duas semanas antes. Houve perda de dados, embora, felizmente, a partir das notas fiscais físicas, a loja tenha conseguido recadastrar boa parte das vendas desse período.

Diante dessa situação, a equipe de desenvolvimento precisa agir baseada em procedimentos que diminuam os riscos de um desastre semelhante acontecer no futuro.

**Atividade**

Crie, em sua máquina, o banco de dados definido pelo *script* disponível em **Conteúdo > Material complementar** e analise e execute as seguintes ações de segurança:

1. Crie um usuário chamado user\_relatorio. Crie *role* para ele, com acesso ao comando **SELECT** de todas tabelas da base de dados **uc4atividades**. Não pode ser definido para este usuário nenhum outro comando DDL ou DML além do **SELECT**.
2. Crie usuário chamado user\_funcionario. Crie *role* para esse usuário. Ele poderá manipular as tabelas de venda, cliente e produto da base de dados **uc4atividades**, ou seja, poderá fazer apenas os comandos de **SELECT**, **INSERT**, **UPDATE** e **DELETE**.
3. Elabore um plano de *backups* regular da base de dados **uc4atividades** para rodar periodicamente (especifique o período) ou um agendamento usando uma ferramenta automatizada. Pode-se utilizar como ponto de partida qualquer exemplo de plano de *backup* explicado no conteúdo desta UC.

Para os itens 1 e 2, grave em *scripts* **.sql** os comandos utilizados. Para o item 3, envie um relatório (.docx, .odt ou .pdf) com evidências do plano de *backup*, incluindo *prints*, comandos utilizados e a periodicidade recomendada.

**Entrega**

Envie um arquivo compactado (ZIP, RAR ou 7z), contendo os *scripts* criados e o relatório de *backup*, no local destinado à entrega da atividade até a data indicada no cronograma de estudos.

**Dica de leitura**

Para esta atividade, leia os seguintes materiais:

* Recuperação de dados
* Segurança do banco de dados

**Avaliação**

Nesta atividade, você será avaliado nos indicadores:

* *Mantém rotina de* backup *e restauração de acordo com parâmetros de segurança definidos para o sistema.*
* *Monitora segurança do banco de dados de acordo com parâmetros definidos para o sistema.*