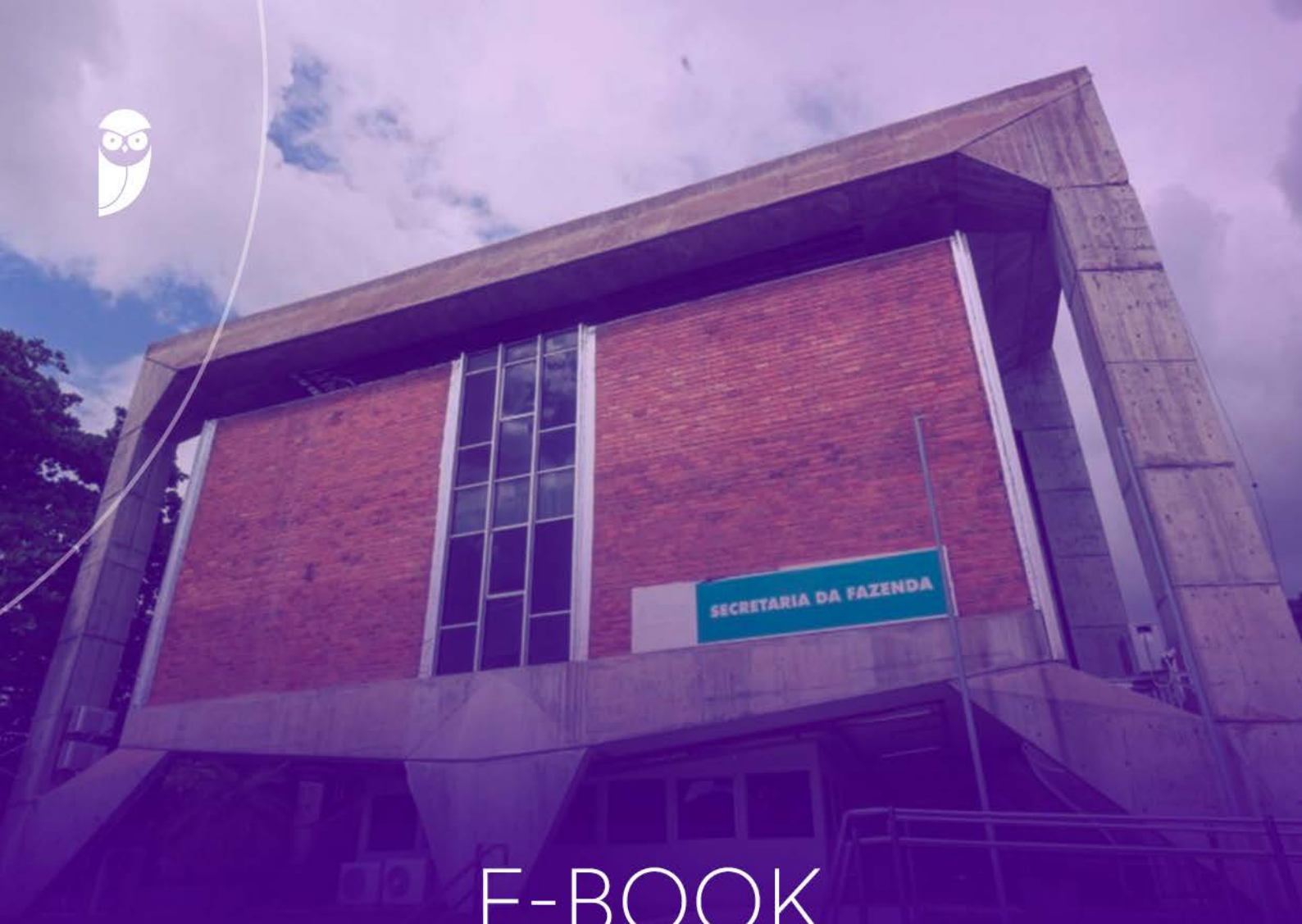


E-BOOK

SEFAZ PI

2025

TECNOLOGIA DA INFORMAÇÃO

50 QUESTÕES QUENTES DA FCC

APRESENTAÇÃO

Olá, futuro Auditor!

É com imensa satisfação que apresentamos o e-book de 50 questões quentes de Tecnologia da Informação para o concurso da SEFAZ-PI. Nossos melhores professores, cuidadosamente, selecionaram e comentaram as questões, explicando detalhadamente os assuntos mais difíceis!

Todas as questões foram retiradas de provas da Fundação Carlos Chagas (FCC), banca tradicionalmente exigente na área contábil. A seleção priorizou os temas mais recorrentes e relevantes para concursos da área fiscal, especialmente aqueles que têm grande probabilidade de aparecer na sua prova da SEFAZ-PI.

Como, ao longo de sua preparação, é fundamental que você resolva diversas questões de concursos passados, sabemos que este material será de grande utilidade. Nosso objetivo é proporcionar mais uma valiosa ferramenta de estudo para deixá-lo mais perto de sua aprovação.

Aproveite muito este material! Bons estudos!

Faça parte do grupo de estudos do Estratégia Concursos no WhatsApp!

Use o QRCode abaixo e entre agora mesmo no grupo da Sefaz-PI.

1. (FCC - TRT 6 - 2025) Em um banco de dados Oracle aberto e em condições ideais, o comando utilizado para adicionar uma coluna custas do tipo NUMBER (10,2) à tabela processo, estabelecendo uma restrição que impede que valores de custas menores ou iguais a 10000 sejam inseridos, é

A) ADD COLUMN custas NUMBER (10,2) TO processo WITH CONSTRAINT processo_custas_ck CHECK (custas > 10000);

B) ALTER TABLE processo ADD custas NUMBER (10,2) ADD CONSTRAINT processo_custas_ck CHECK (custas >= 10000);

C) ALTER TABLE processo ADD custas NUMBER (10,2) CONSTRAINT processo_custas_ck WHERE (custas > 10000);

D) ADD COLUMN custas NUMBER (10,2) TO processo WHERE custas > 10000;

E) ALTER TABLE processo ADD custas NUMBER (10,2) CONSTRAINT processo_custas_ck CHECK (custas > 10000);

Comentários:

A) **ERRADO.** O item já inicia com uma sintaxe incorreta para adicionar uma coluna. As primeiras palavras-chave corretas seriam "ALTER TABLE". Ademais, "TO" não é uma palavra reservada no Oracle. Ainda, não é necessária a utilização da palavra reservada "WITH" para a definição de uma constraint, dado que tal palavra é utilizada no contexto de definições de variáveis.

B) **ERRADO.** O item apresenta 2 erros. O primeiro é que não é necessário utilizar a palavra "ADD" antes de "CONSTRAINT" para definir uma restrição. O segundo é que a condição "custas >= 10000" não impediria a inserção do valor 10000.

C) **ERRADO.** O único erro do item é utilizar "WHERE" onde deveria constar "CHECK".

D) **ERRADO.** O item traz uma sintaxe muito equivocada para a função desejada em comparação aos outros itens, os erros são muito semelhantes aos do item A, com a incoerência adicional da utilização da palavra reservada "WHERE" para tentar definir uma restrição.

E) **CORRETO.** O item traz uma sintaxe completamente correta para a função desejada.

Gabarito: E

2. (FCC - TRT 6 - 2025) Uma Analista de nome Maria Cecilia criptografa uma mensagem com sua chave privada e envia pela internet para João Miguel, que recebe a mensagem e a descriptografa com a chave pública de Maria Cecília para ler a mensagem. O uso da criptografia nesse caso está garantindo o princípio da

A) integridade.

B) confidencialidade.

C) confiabilidade.

D) autenticidade.

E) disponibilidade.

Comentários:

A criptografia assimétrica, também conhecida como criptografia de chave pública, é um método de criptografia que utiliza um par de chaves relacionadas para criptografar e descriptografar dados. Ao contrário da criptografia simétrica, que usa uma única chave para ambas as operações, a criptografia assimétrica emprega duas chaves distintas:

Chave pública: pode ser compartilhada livremente e é usada para criptografar dados.

Chave privada: mantida em segredo pelo proprietário e é usada para descriptografar dados que foram criptografados com a chave pública correspondente.

Em relação aos itens:

A) **ERRADO.** A integridade dos dados refere-se à característica de que os mesmos não sofrerão alterações indevidas. No caso do enunciado, não as medidas adotadas não garantem a integridade, uma vez que a mensagem pode ser corrompida no caminho até o destinatário.

B) **ERRADO.** A confidencialidade de informações é um princípio fundamental da segurança da informação, que garante que apenas pessoas autorizadas tenham acesso a dados sensíveis. Em tal caso, a confidencialidade não será garantida, uma vez que qualquer ator pode interceptar a mensagem e descriptografar com a chave pública de Maria.

C) **ERRADO.** A confiabilidade de dados é um aspecto crucial na gestão de informações, assegurando que os dados sejam precisos, consistentes e confiáveis para uso em diversas aplicações. No caso da questão, a confiabilidade não poderia ser garantida pelas medidas adotadas, uma vez que um esquema de criptografia assimétrica não tem como garantir a qualidade da informação em si. Ademais, a mensagem pode ser corrompida no caminho até o destinatário.

D) **CERTO.** A autenticidade refere-se à característica de que a informação realmente advém de determinada origem. No caso da questão, há garantia de autenticidade, considerando uma infraestrutura de chaves públicas, dado o fato de que apenas a chave pública de Maria seria capaz de descriptografar os dados. Se há garantia de que o par de chaves realmente pertence a Maria, há garantia de autenticidade de dados.

E) **ERRADO**. A disponibilidade de dados é um dos pilares da segurança da informação, garantindo que os dados e sistemas estejam acessíveis e utilizáveis por usuários autorizados quando necessário. No caso da questão, não há como garantir a disponibilidade da mensagem com os meios utilizados dado o fato de que, por exemplo, o próprio canal de comunicação poderia ser interrompido, de modo que a mensagem sequer chegaria a João.

Gabarito: D

3. (FCC - TRT 7- 2024) Entende-se por criptografia assimétrica o mecanismo de segurança que torna dados indecifráveis para pessoas que não possuem a chave correta para decodificá-los,

A) sendo necessárias uma chave privada e outra pública, que deverão ser utilizadas simultaneamente para descriptografar os dados.

B) não sendo necessária a utilização de chave específica para descriptografar a informação, quando esta for acessada pelo destinatário autorizado.

C) sendo necessária apenas uma chave, que é utilizada tanto para criptografar quanto para descriptografar os dados.

D) não sendo obrigatório o cadastro da pessoa física no Sistema Nacional de Certificação Digital, Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), para obtenção de assinatura eletrónica qualificada.

E) sendo necessárias duas chaves distintas, uma para criptografar e outra para descriptografar os dados.

Comentários:

A criptografia assimétrica, também conhecida como criptografia de chave pública, é um método de criptografia que utiliza um par de chaves relacionadas para criptografar e descriptografar dados. Ao contrário da criptografia simétrica, que usa uma única chave para ambas as operações, a criptografia assimétrica emprega duas chaves distintas:

Chave pública: pode ser compartilhada livremente e é usada para criptografar dados.

Chave privada: mantida em segredo pelo proprietário e é usada para descriptografar dados que foram criptografados com a chave pública correspondente.

A **criptografia simétrica**, também conhecida como criptografia de chave secreta, é um método de criptografia que utiliza **uma única chave** para tanto criptografar (codificar) quanto descriptografar (decodificar) os dados. Isso significa que o remetente e o destinatário da mensagem devem possuir e compartilhar a mesma chave secreta.

Em relação aos itens:

A) **ERRADO.** Na verdade, a utilização típica de tal mecanismo de segurança é criptografar com uma chave e descriptografar com a outra.

B) **ERRADO.** A chave a ser utilizada para descriptografar os dados é a específica ao par de chaves a que pertence a chave que foi utilizada para criptografar os dados.

C) **ERRADO.** O item descreve, na verdade, o modo de funcionamento da criptografia simétrica.

D) **ERRADO.** Na verdade, ao contrário do que o item afirma, é necessário o cadastro mencionado para que a combinação de chaves tenha fidedignidade em relação aos dados relacionados no certificado digital.

E) **CERTO.** O item traz corretamente uma das características da criptografia assimétrica.

Gabarito: E

4. (FCC - TRT 7 - 2024) A combinação de mecanismos de proteção que deve ser utilizada por uma organização que deseja implementar um sistema de comunicação segura entre seus servidores, garantindo que os dados não possam ser lidos ou modificados por terceiros, é:

A) criptografia assimétrica (ECC) para confidencialidade e hash criptográfico (MD5) para integridade.

B) criptografia simétrica (ECC) para confidencialidade e hash criptográfico (SHA-256) para integridade.

C) criptografia assimétrica (RSA) para confidencialidade e assinaturas digitais para autenticidade.

D) certificados digitais para confidencialidade e hash criptográfico (SHA-1) para integridade.

E) criptografia simétrica (3DES) para confidencialidade e certificados digitais para integridade.

Comentários:

Trata-se de questão um pouco mais avançada que exige conhecimento de algumas técnicas criptográficas e suas classificações em simétricas, assimétricas ou de hash. De maneira resumida:

Técnicas assimétricas:

- ECC
- RSA

Técnicas simétricas:

- 3DES

Técnicas de hash:

- MD5
- SHA-256
- SHA-1

Em relação aos itens:

A) **ERRADO.** O item foi dado como errado, mas, em uma interpretação mais abrangente, o MD5 poderia ser utilizado em um esquema de verificação de integridade.

B) **ERRADO.** O ECC é, na verdade, uma técnica de criptografia assimétrica.

C) **CERTO.** O item traz corretamente uma combinação para garantir confidencialidade e autenticidade.

D) **ERRADO.** Certificados digitais são um conjunto de informações atrelado a um par de chaves em um esquema de chave pública, tendo um escopo superior ao de uma mera confidencialidade.

E) **ERRADO.** Certificados digitais são um conjunto de informações atrelado a um par de chaves em um esquema de chave pública, tendo um escopo superior ao de uma mera integridade.

Gabarito: C

5. (FCC - TRT 7 - 2024) Uma organização que está aprimorando seu sistema de controle de acesso tem como meta garantir que os usuários se autentiquem de maneira segura, que as permissões sejam gerenciadas eficientemente e que todas as atividades sejam auditadas para posterior análise. A prática correta que essa organização deve adotar para alcançar uma segurança robusta no controle de acesso é

A) utilizar autenticação de dois fatores com senha e e-mail, permissões de acesso configuradas individualmente e auditorias detalhadas registrando os logs de acesso.

B) utilizar senhas fortes combinadas com perguntas de segurança, permissões configuradas diretamente para cada usuário e auditorias constantes que registrem somente os acessos bem-sucedidos.

C) implementar MFA utilizando perguntas de segurança, permissões de acesso definidas por grupos amplos e auditorias que registrem todos os eventos de acesso.

D) utilizar autenticação de dois fatores com senha e SMS, permissões configuradas individualmente e auditorias que registrem somente os acessos não autorizados.

E) implementar autenticação multifatorial (MFA) com biometria e um aplicativo de autenticação, RBAC com permissões baseadas em papéis e auditorias detalhadas que registrem todas as tentativas de acesso.

Comentários:

Em primeiro lugar, espera-se que o candidato identifique três requisitos de segurança no enunciado, tratando da forma de autenticação, do gerenciamento de permissões e da auditoria; e que perceba que cada alternativa da questão propõe, igualmente, três práticas, uma por requisito. Visitemos em detalhe cada alternativa:

A) O enunciado deixou claro que as permissões devem ser gerenciadas **eficientemente**, o que não é o caso da configuração individual. **ITEM INCORRETO.**

B) O primeiro erro está em sugerir a configuração das permissões diretamente para cada usuário, como no item A. Outro erro está em sugerir o registro somente dos acessos bem-sucedidos. Com efeito, tentativas de acesso malsucedidas podem prover informação valiosa para auditorias, como revelar ataques de força bruta. **ITEM INCORRETO.**

C) Há uma leve impropriedade em "que registrem os eventos de acesso" (subentende-se, "que registrem os eventos de acesso sucedido") pois, como discutido nos comentários do item B, é de igual importância registrar as tentativas de acesso, isto é, os acessos malsucedidos. Além disso, apesar de a definição das permissões de acesso por grupos amplos ser tão "eficiente" quanto menos grupos houver (isto é, quanto mais amplos forem eles), é possível que a banca considere essa afirmação incorreta na medida em que grupos de acesso muito amplos dificilmente satisfarão as necessidades de controle de acesso de uma organização complexa e com perfis diversos de usuário, mas isso é uma hipótese. De qualquer forma, por uma razão ou pela outra, **ITEM INCORRETO.**

D) O primeiro erro está em sugerir, novamente, a configuração individual das permissões, o que, como dito acima, não atende ao requisito de eficiência explícito no enunciado. Ademais, há erro em "auditorias que registrem somente os acessos não autorizados", pois os acessos autorizados são importantes para auditar as ações que foram feitas durante um acesso legítimo a um sistema. Em outras palavras, o objetivo da auditoria não é apenas identificar acessos indevidos, mas também ações ilegítimas feitas por uma pessoa que, apesar de ter acesso a um sistema, pode ter feito seu uso incorreto. **ITEM INCORRETO.**

E) Vale lembrar que RBAC (*Role-Based Access Control*) significa justamente que as permissões serão baseadas em papéis e é muito mais eficiente que gerenciar as permissões de forma individual. Os outros dois requisitos também são atendidos pelas sugestões do item, com destaque ao fato de que, ao dizer "auditorias detalhadas que registrem todas as tentativas de acesso", o enunciado não está, de forma alguma, afirmando que **somente** os acessos não autorizados seriam registrados (esse foi um erro do item D). **ITEM CORRETO.**

Gabarito: E

6. (FCC - TRT 7 - 2024) Um Analista utilizou um comando SQL para eliminar uma tabela supérflua de seu banco de dados. O comando que ele utilizou é calegorizado no contexto de linguagem de

A) controle de dados.

B) descrição de dados.

C) manipulação de dados.

D) consulta de dados.

E) definição de dados.

Comentários:

O Analista usou um comando DROP TABLE, que faz parte do subconjunto do SQL a que chamamos Linguagem de Definição de Dados (ou DDL, da sigla em inglês).

Gabarito: E

7. (FCC - TRT 7 - 2024) Após executar o comando Oracle TRUNCATE TABLE, um Analista decidiu desfazer a ação por meio de rollback. A ação foi

A) ineficaz, pois ele já havia dado commit na tabela objeto.

B) eficaz, após a execução de um drop realizado na tabela objeto.

C) ineficaz, pois esse comando não permite o rollback.

D) ineficaz, pois ele já havia atualizado a tabela objeto.

E) eficaz, após a execução de um alter realizado na tabela objeto.

Comentários:

Vale lembrar que o comando TRUNCATE TABLE remove todas as linhas de uma tabela, sem suprimi-la. Possui o mesmo efeito de uma operação DELETE FROM (sem a cláusula WHERE, já que sempre remove TODAS as linhas), porém, costuma ser mais rápido.

Uma característica do TRUNCATE TABLE que varia com SGBD usado (Oracle, MS SQL Server etc.) é se ele admite rollback ou não. No caso do Oracle, como pode ser confirmado na documentação, NÃO se admite rollback. Portanto, o item C está correto.

As alternativas B e E estão incorretas por afirmar que o rollback é possível, e A e D estão incorretas por assumirem que o TRUNCATE TABLE foi operado sobre uma tabela-objeto, o que não pode ser inferido do enunciado. Sem entrar em detalhes, Oracle possui tabelas-objeto e tabelas relacionais, conceitos que não se confundem.

Vale dizer que, não fosse o uso injustificado do termo “tabela-objeto” no item A, poderíamos defendê-lo como correto, pois o banco de dados Oracle faz um COMMIT implícito antes e depois do comando TRUNCATE TABLE (assim como para todos os comandos de tipo DDL, em que a documentação do Oracle inclui o TRUNCATE), o que, por si só, já significa que o rollback seria ineficaz.

Fontes: https://docs.oracle.com/en/database/oracle/oracle-database/23/sqlrf/TRUNCATE-TABLE.html
https://docs.oracle.com/en/database/oracle/oracle-database/23/sqlrf/Types-of-SQL-Statements.html

Gabarito: C

8. (FCC - Pref J Guararapes - 2024) Uma prefeitura está criando um banco de dados para gerenciar suas transações e contas de cidadãos. Para assegurar a precisão dos dados, implementaram várias regras para restringir os valores inseridos nas tabelas, como valores não nulos para certas colunas e correspondência entre chaves estrangeiras e primárias. Considerando o modelo de dados relacional, no contexto descrito, uma restrição de integridade

A) assegura a conformidade dos dados com regras específicas, como a unicidade e a validade dos valores.

B) assegura que as transações sejam revertidas em caso de falha, sendo as informações de erros armazenadas em logs de auditoria.

C) impede a criação de índices na tabela e chaves primárias compostas na tabela ou multivaloradas.

D) mpede a atualização de qualquer registro no banco de dados sem uso de assinatura digital,

E) garante que todos os usuários tenham os mesmos privilégios de acesso provendo unicidade de acesso e transparência.

Comentários:

Vejamos todos os itens:

A) Descreve corretamente para que serve uma restrição de integridade. Chaves primárias garantem que cada dado possui um conjunto de colunas na respectiva tabela, que o define de forma única, evitando duplicatas; chaves estrangeiras contribuem à integridade do banco de dados ao nos permitir definir as relações existentes entre tabelas; constraints como NOT NULL permitem proibir valores nulos em colunas onde isso não faria sentido. Alternativa correta.

B) Reversão (*rollback*) de transações e a manutenção de logs de auditoria não são restrições de integridade. Alternativa incorreta.

C) Restrições de integridade não impedem criação de índices (que servem para acelerar a performance das consultas) nem a criação de chaves primárias compostas ou multivaloradas. Alternativa incorreta.

D) Novamente, nada a ver com restrições de integridade. Alternativa incorreta.

E) Além de não ter nada a ver com restrições de integridade, vale dizer que não é boa prática dar os mesmos privilégios a todos os usuários. Alternativa incorreta.

Gabarito: A

9. (FCC - Pref J Guararapes - 2024) Utilizando SQL ANSI em um banco de dados aberto e em condições ideais, para excluir da tabela "cidadao" o cidadão que possui no conteúdo do campo CPF o valor fictício 158.234.089.12 utiliza-se o comando

A) SELECT * FROM cidadao AND DELETE CPF = '158.234.089.12';

B) DELETE * FROM cidadao WHERE CPF = '158.234.089.12';

C) ERASE FROM cidadao WHERE CPF = '158.234.089.12';

D) DELETE FROM cidadao WHERE CPF = '158.234.089.12';

E) ERASE * FROM cidadao WHERE CPF = '158,234.089,12';

Comentários:

Para excluir uma ou mais linhas, usa-se o comando DELETE. Diferentemente do comando SELECT, em que é preciso especificar quais colunas retornar (ou * para todas), o DELETE sempre exclui a linha inteira. Portanto, grave bem: não se usa * com DELETE!

Vejamos todas as alternativas:

A) DELETE não serve a consultas e, de qualquer modo, SELECT AND DELETE não é uma combinação existente em SQL. Alternativa incorreta.

B) Diferentemente do comando SELECT, em que é preciso especificar quais colunas retornar (ou * para todas), o DELETE sempre exclui a linha inteira. Portanto, grave bem: não se usa * com DELETE! Alternativa incorreta.

C) Não é ERASE, e sim DELETE. Alternativa incorreta.

D) Comando seguindo os padrões SQL. Alternativa correta.

E) Mesmos comentários que os itens C e D, além da presença de vírgulas em vez de pontos no CPF. Alternativa incorreta.

Gabarito: D

10. (FCC - Pref J Guararapes - 2024) Em um banco de dados aberto e em condições ideais. a tabela imposto_cidadao contém os campos Idimposto, CPFCidadao e valorPago (valor numérico real). A chave primária é composta pelos campos Idimposto e CPFCidadao, que são chaves estrangeiras. Para somar o conteúdo do campo valorPago de todos os registros da tabela imposto_cidadao utiliza-se a instrução SQL:

A) SELECT * FROM valorPago IN imposto_cidadao;

B) SUM valorPago FROM imposto_cidadao;

C) SELECT SUM (valorPago) IN impoato_cidadao;

D) SELECT SUM (valorPago) FROM imposto_cidadao;

E) SUM(*) FIELD valorPago FROM imposto_cidadao;

Comentários:

A consulta SELECT SUM(campo) FROM tabela calcula a soma (em inglês, “sum”) dos valores do campo “campo” na tabela “tabela”. Portanto, o item correto é D.

Observação: Apesar do operador IN existir em SQL, ele é usado dentro de um WHERE, e não para informar a tabela na qual o SELECT será aplicado como no item C.

Gabarito: D

11. (FCC - BAHIAGÁS - 2024) Em uma situação hipotética, o Analista Lucas, depois de abrir a ferramenta de Migração do SharePoint (SPMT — SharePoint Migration Tool), primeiro deve autenticar para o destino, que é o locatário para o qual migrará seus arquivos. Fornecer seu nome de usuário e senha ao locatário, associa os trabalhos de migração que Lucas envia a essa conta. Essa funcionalidade permite que ele retome a migração de outro computador, se necessário, fazendo logon com as mesmas credenciais. Essa conta deve ser a do administrador do site do destino para o qual Lucas está migrando. Os seguintes métodos de autenticação são compatíveis: NTLM, Formulários, ADFS, Declarações com base em SAML, Autenticação de certificado de cliente e, também,

A) Dinasty e Multi-factor Authentication.

B) HKerberos e KAMS.

C) KAMS e Doc Authentication.

D) Kerberos e Multi-factor Authentication.

E) LineTrue e SAMR.

Comentários:

A) A resposta a essa questão está na documentação do SPMT, que diz: "O SPMT suporta NTLM, Kerberos, Forms, ADFS, autenticação multifatorial, declarações baseadas em SAML e autenticação de Certificados de cliente". Esses são justamente os cinco métodos já listados no enunciado, mais Kerberos e autenticação multifatorial ("*Multi-factor Authentication*", ou MFA), como no item D.

Ainda que o candidato nunca tivesse ouvido falar em SPMT antes de sua prova, a alternativa D seria um bom "chute", pois Kerberos e MFA são métodos de autenticação muito populares.

Os outros termos nas alternativas não são métodos de autenticação (ou, se são, não são populares).

Fonte: https://learn.microsoft.com/pt-br/sharepointmigration/introducing-the-sharepoint-migration-tool#supported-authentication-methods

Gabarito: D

12. (FCC - TRT 15 - 2023) A orientação da ABNT NBR ISO/IEC 27002:2022 sobre controle de acesso recomenda que

A) seja definida uma política específica por tema, sobre controle de acesso.

B) as regras de controle de acesso não sejam implementadas em diferentes granularidades, focando sempre no sistema inteiro.

C) as regras de controle de acesso não contenham elementos dinâmicos, como, por exemplo, funções que avaliam acessos passados ou valores específicos do ambiente.

D) as formas de controle de acesso sejam detalhadas na Política de Segurança da Informação, sem necessidade de política específica sobre o assunto.

E) as regras para controle de acesso físico incluam métodos como validação por senha, autenticação multifator (MFA) e Single Sign-On (SSO).

Comentários:

Analisemos cada alternativa:

A) A ISO 27002:2002 prevê, além da Política de Segurança da Informação, a existência de políticas específicas para tratar de temas específicos, incluindo o controle de acesso. Item correto.

B) A ISO 27002:2022 prevê que as regras de controle de acesso sejam implementadas com diferentes granularidades, como a necessidade de acesso à informação, o papel do usuário (no caso de controle de acesso baseado em papéis, ou RBAC) e as necessidades de negócios. Item incorreto.

C) A ISO 27002:2022 permite métodos de controle de acesso que fazem uso de elementos dinâmicos. Isso se relaciona ao conceito de controle de acesso baseado em atributos (ABAC), que é abordado pela norma junto de outras técnicas (como o RBAC). Item incorreto.

D) Como vimos ao analisar o item A, a ISO 27002:2022 recomenda que exista política específica sobre controle de acesso. Item incorreto.

E) Percebam que o item fala de controle de acesso físico, para o que a ISO 27002:2022 não prevê SSO (termo que, como seu trecho "Sign-On", aplica-se geralmente ao ambiente digital). Item incorreto.

Gabarito: A

13. (FCC - TRT 15 - 2023) Um Técnico foi designado para implantar um modelo de acordo com Role-Based Access Control (RBAC) que estabelece a separação de tarefas de um Tribunal Regional do Trabalho para dificultar a possibilidade de fraude no setor de compras, criando, assim, os papéis de Requisitante de Gastos e de Autorização de Gastos atribuídos a usuários distintos. O modelo RBAC a ser implantado é o

A) Core.

B) Flat.

C) Hierarchical.

D) Constrained.

E) Asymmetric.

Comentários:

As palavras-chave do enunciado que nos ajudam a resolver a questão são “separação de tarefas” e “fraude”. O modelo RBAC que se propõe a dificultar a possibilidade de fraudes (ou mesmo acidentes) por meio da separação de tarefas é o modelo “Constrained”. Portanto, a resposta correta é o item D.

Aprofundando a implementação do Constrained RBAC, no caso do enunciado, entende-se que um gasto só é concretizado se uma pessoa com o papel de Requisitante de Gastos requisitá-lo e uma pessoa distinta, com o papel de Autorização de Gastos, autorizá-lo, o que dificulta a execução de gastos fraudulentos.

Vale ressaltar que os modelos Flat, Hierarchical, Constrained e Symmetric (perceba que o item E diz **A**symmetric, e não Symmetric) são “cumulativos” (cada um possui todas as características do anterior), de forma que, se houvesse a opção Symmetric, ela também atenderia aos requisitos da questão. Ainda assim, se encontrar um caso desses em sua prova e os requisitos no enunciado forem satisfeitos com o modelo mais simples, então vale a pena escolhê-lo, a não ser que o enunciado explicitamente solicite o modelo mais “completo” possível.

Fonte: https://csrc.nist.gov/CSRC/media/Publications/conference-paper/2000/07/26/the-nist-model-for-role-based-access-control-towards-a-unified-/documents/sandhu-ferraiolo-kuhn-00.pdf

Gabarito: D

14. (FCC - TRT 12 - 2023) Com relação ao uso de hashes criptográficos nas assinaturas digitais, é correto afirmar que

A) os hashes criptográficos são usados para garantir a disponibilidade do serviço de assinatura digital

B) o hash criptográfico permite que o destinatário de uma mensagem verifique a identidade e a assinatura do remetente.

C) os hashes serão idênticos, se dois documentos contiverem o mesmo texto, diferindo apenas na pontuação.

D) a chave pública é usada para criptografar o hash do documento na criação de uma assinatura digital.

E) a assinatura digital é criada em um processo que envolve a criptografia do hash do documento com a chave privada do signatário.

Comentários:

Para resolver a questão, é importante lembrar que o objetivo da assinatura digital é tão somente permitir a qualquer pessoa confirmar se o signatário se responsabiliza por uma dada mensagem ou arquivo e que esse documento não foi alterado (veja bem, não há que falar em confidencialidade nem em disponibilidade, mas integridade).

Portanto, em vez de encriptar o documento inteiro, o que se faz na assinatura digital é primeiro aplicar uma função *hash* sobre o documento (o que resulta em um pequeno *hash*, ou *digest*, de tamanho fixo) e encriptar o *hash*. Como qualquer alteração do documento modificará o *hash* (a probabilidade de dois documentos distintos terem o mesmo *hash* é realmente muito pequena), basta ao destinatário da mensagem recuperar o *hash* da mensagem original com a chave **pública** do signatário, calcular o *hash* da mensagem recebida, e comparar ambas: se forem iguais, então tudo certo!

Portanto, a alternativa correta é E.

Visitemos os outros itens:

A) Assinatura digital não tem nada a ver com o conceito de disponibilidade em cibersegurança.

B) Na verdade, a assinatura digital implica a verificação do *hash* da mensagem, como explicado acima. No mesmo sentido, os *hashes* propriamente ditos não são uma técnica de verificação de identidade. Quem mais se aproxima dessa função no processo de assinatura digital e sua verificação são as chaves pública e privada do signatário, não o *hash* da mensagem.

C) Mudar a pontuação também modifica o *hash*.

D) Como explicado acima, ocorre o oposto.

Gabarito: E

15. (FCC - TRT 12 - 2023) Considere o seguinte caso:
Utilizando comandos SQL, um analista criou uma tabela de cidadão dando permissão de acesso ao usuário Roberto. Posteriormente inseriu dados nessa tabela, mas logo em seguida teve que deletá-los, retirar a permissão de Roberto que estava saindo do tribunal e dar permissão a Carla.

A sequência de comandos SQL utilizada no caso é, correta e respectivamente, categorizada como

A) DML - DCL - DDL - DDL - DCL - DCL

B) DML - DCL - DML - DDL - DML - DCL

C) DDL - DCL - DML - DML - DCL - DCL

D) DDL - DCL - DDL - DML - DML - DCL

E) DCL - DDL - DML - DML - DCL - DCL

Comentários:

A criação de um tabela é uma operação de linguagem de definição de dados (DDL, de *Data Definition Language*). Dar ou remover permissões (*grant* e *revoke*) são operações de linguagem de controle de dados (DCL, de *Data Control Language*). A inserção e a deleção de dados são operações de manipulação de dados (DML, de *Data Manipulation Language*). Em seguida, há mais duas operações de DCL como explicado acima.

Portanto, a boa sequência é DDL - DCL - DML - DML - DCL - DCL (item C).

Gabarito: C

16. (FCC - TRT 12 - 2023) Considere uma tabela denominada Cidadao e as colunas Nome_Cidadao e Valor_Recebido.
Para obter a média dos valores maiores que 200 recebidos pelos cidadãos, um Analista deve utilizar o comando

A) SELECT AVG (Valor_Recebido > 200) FROM Cidadao;

B) SELECT AVG (Valor_Recebido) FROM Cidadao WHERE Valor_Recebido > 200;

C) SELECT AVG (Valor_Recebido) > 200 FROM Cidadao;

D) SELECT FROM Cidadao AVG (Valor_Recebido) > 200;

E) SELECT Nome Cidadao and AVG (Valor_Recebido) FROM Cidadao WHERE Valor_Recebido > 200;

Comentários:

Primeiro, deve-se pensar em restringir as linhas que serão retornadas pela consulta a somente aquelas em que Valor_Recebido é maior que 200: SELECT [...] FROM Cidadao WHERE Valor_Recebido > 200
Em seguida, pensamos na operação de agrupamento, quando existente (o enunciado pede uma média, ou AVG, de *average*), e nas colunas que devem constar na saída da consulta (o enunciado pede a média do Valor_Recebido).

A consulta correta, portanto, seria SELECT AVG (Valor_Recebido) FROM Cidadao WHERE Valor_Recebido > 200 - item B.

Gabarito: B

17. (FCC - TRT 12 - 2023) Considere as informações a seguir:
Segurança da informação

Aspectos gerais	Definições
1. Severidade	a. Processo de identificação e reconhecimento formal de identidade.
2. Irretratabilidade	b. Reerência de cumprimento das regras e normas estabelecidas.
3. Criticidade	c. Gravidade do impacto geral causado por uma perda.
4. Autenticação	d. Gravidade do dano que determinado ativo pode sofrer.
5. Conformidade	e. Atributo de identificação do emissor de uma informação.

A correta relação entre os aspectos gerais e as definições de segurança da informação é:

A) 1b - 2a - 3d - 4c - 5e

B) 1a - 2c - 3b - 4e - 5d

C) 1d - 2e - 3c - 4a - 5b

D) 1e - 2c - 3b - 4a - 5d

E) 1c - 2b - 3e - 4d - 5a

Comentários:

Vejamos a definição de cada aspecto:

1. Severidade é a "gravidade do dano que determinado ativo pode sofrer" (1-D).

2. Irretratabilidade, ou irrenunciabilidade, é o "atributo de identificação do emissor de uma informação", isto é, uma propriedade possível de um sistema de informação, que significa que o emissor de uma informação não poderá negar sê-lo (2-E).

3. Criticidade é a "gravidade do impacto geral causado por uma perda". A diferença entre severidade e criticidade é que aquela é mais específica, refere-se ao dano propriamente dito, enquanto esta trata dos efeitos do dano no sistema ("impacto geral"). Por exemplo, uma falha em um sistema bancário pode ser crítica, pois pode afetar muitas pessoas, drasticamente (3-C).

4. Autenticação é o "processo de identificação e reconhecimento formal de identidade". Por sinal, não confunda autenticação com autorização, o que é um "prato cheio" para bancas que gostam de "pegadinhas" (4-A).

5. Conformidade é a "referência de cumprimento das regras e normas estabelecidas". Outro termo muito usado é o anglicismo "*compliance*" (5-B).

Gabarito: C

18. (FCC - TJ BA - 2023) Os dois métodos de criptografia mais comuns possuem vantagens e desvantagens no que diz respeito a suas aplicações. Sobre esse tema e os algoritmos de criptografia AES e RSA,

A) o processo de encriptação RSA é mais lento do que criptografia AES.

B) o AES utiliza criptografia assimétrica e RSA, simétrica.

C) o RSA utiliza apenas uma chave pública, enquanto o AES utiliza uma pública e outra privada.

D) o processo de criação de chaves AES ocorre a partir da escolha de dois números primos, quanto maior o número primo menor será o desempenho.

E) os algoritmos de criptografia AES e RSA são exemplos de criptografia assimétrica.

Comentários:

Analisemos cada alternativa:

A) Verdade! Também vale a regra geral de que algoritmos de criptografia assimétrica (como o RSA) costumam ser mais lentos que algoritmos de criptografia simétrica (como o AES). Item correto.

B) É o contrário. Item incorreto.

C) Novamente, o RSA é um algoritmo de criptografia assimétrica e o AES é um algoritmo de criptografia simétrica. Por sinal, ainda que o item tivesse trocado RSA com AES, afirmar que o AES usa "apenas uma chave pública" estaria errado pois, para um algoritmo de criptografia simétrica ser útil, a chave deve ser mantida em segredo pelos interlocutores. Item incorreto.

D) O item descreve o processo de criação das chaves do RSA, ao passo que o algoritmo do AES não tem a ver com primos. Item incorreto.

E) AES é um algoritmo de criptografia simétrica. Item incorreto.

Gabarito: A

19. (FCC - TJ BA - 2023) O Processo de Gestão dos Riscos é um processo contínuo e iterativo constituído de fases e atividades, possibilitando a segurança efetiva em sistemas de Tecnologia da Informação e Comunicação no que tange ao processamento, ao armazenamento e à transmissão de informações. Nesse contexto, a fase que envolve a decisão entre reter, evitar, transferir ou reduzir os riscos é

A) aceitação do risco.

B) apreciação do risco.

C) definição do contexto.

D) tratamento do risco.

E) comunicação do risco.

Comentários:

Pessoal, a questão busca conhecimentos relacionados à ISO/IEC nº 27.005 sobre o processo de tratamento do risco. A fase que envolve a decisão sobre reter, evitar, transferir ou reduzir os riscos é a fase de Tratamento do Risco. Primeiramente há a Definição do Contexto, partindo para a Identificação dos Riscos, posteriormente a Análise dos Riscos, seguida da Avaliação dos Riscos. Depois que vem a fase de Tratamento dos Riscos, que envolve essa etapa de decisão sobre os riscos, como vimos acima, para vir então a Aceitação dos Riscos, seguida da Comunicação e Consulta, para no final haver o Monitoramento e Análise Crítica. Lembrando que é um processo cíclico e contínuo.

Podem ser usados outros termos na fase de Tratamento do Risco, como: Mitigar/Reduzir/Modificar, Aceitar/Reter, Transferir/Compartilhar, Evitar.

Portanto, o gabarito é a alternativa D.

Vamos analisar brevemente cada alternativa.

A) aceitação do risco: alternativa errada. Não é na fase de Aceitação que temos a decisão sobre reter, evitar, transferir ou reduzir os riscos. Na Aceitação, há a decisão formal de aceitar os riscos residuais após o tratamento dos riscos.

B) apreciação do risco: alternativa errada. Não há essa fase de acordo com a ISO/IEC 27.005. O termo "apreciação" pode se aproximar da análise dos riscos, porém, ainda assim não seria a alternativa correta.

C) definição do contexto: alternativa errada. O Estabelecimento do Contexto é a primeira fase de acordo com a ISO/IEC 27005. Portanto, não é nessa fase que há a decisão sobre os riscos.

D) tratamento do risco. Alternativa correta, conforme explicado acima.

E) comunicação do risco: alternativa errada. A Comunicação do Risco ocorre logo após a fase de Aceitação dos riscos e não envolve o processo de decisão descrito no enunciado.

Gabarito: D

20. (FCC - TJ BA - 2023) Um Analista do Tribunal de Justiça avalia o emprego de uma ferramenta para gerenciar o ciclo de vida completo das identidades e direitos do usuário em todos os recursos e que estabeleça o controle básico da segurança tanto para o data center quanto na nuvem, autenticando usuários e regulando o acesso a sistemas, redes e dados. Nesse contexto, a ferramenta mais adequada é:

A) CDN.

B) WAF.

C) Firewall.

D) IAM.

E) vCenter.

Comentários:

Vamos lá, pessoal! Essa questão ab,5orda as ferramentas e conceitos utilizados no gerenciamento de usuários e acessos em recursos tanto de data center quanto na nuvem.

Vamos analisar cada alternativa a seguir:

A) CDN. Alternativa errada. O termo CDN significa "*Content Delivery Network*" (Rede de Distribuição de Conteúdo), sendo uma forma de se obter performance e disponibilidade de conteúdo web com maior eficiência, melhorando a entrega para o usuário final. Não está relacionada ao gerenciamento de usuários conforme busca o enunciado da questão.

B) WAF. Alternativa errada. WAF (*Web Application Firewall*) é uma firewall de aplicações web protegendo aplicativos web e sites de ataques. Monitora e filtra o tráfego de dados; não está relacionado ao gerenciamento de usuários.

C) Firewall. Alternativa errada. Firewall é um filtro de tráfego de dados entre dois pontos, não está relacionado ao gerenciamento de usuários.

D) IAM. Alternativa correta. IAM (*Identity and Access Management*) é uma estrutura completa de políticas, processos e ferramentas de gerenciamento de identidades e acessos de usuários a sistemas, aplicativos, redes e dados, tanto em ambientes de data center quanto em nuvem. Exemplos de ferramentas IAM: AWS IAM, IBM Security Verify e Microsoft Azure Active Directory (rebatizado para Microsoft Entra ID).

E) vCenter. Alternativa errada. É uma ferramenta da VMware para gerenciar servidores e controlar ambientes de máquinas virtuais.

Gabarito: D

21. (FCC - TJ BA - 2023) A Infraestrutura de Chaves Públicas Brasileira da ICP-Brasil é composta por um conjunto de entidades, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais nacionais. Uma dessas entidades é conhecida como Autoridade de Registro tendo como competência:

A) emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, além de expedir, distribuir, revogar e gerenciar os certificados.

B) executar as políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor.

C) realizar auditorias operacionais em entidades subordinadas às autoridades certificadoras.

D) disponibilizar a infraestrutura física e lógica e de recursos humanos especializados às Autoridades Certificadoras.

E) identificar e cadastrar usuários na presença destes e encaminhar solicitações de certificados às Autoridades Certificadoras.

Comentários:

Questão que aborda o tema de certificados digitais, mais especificamente a ICP-Brasil, Infraestrutura de Chaves Públicas Brasileira. Busca saber a competência da entidade conhecida como Autoridade de Registro. Vamos analisar cada alternativa:

A) **ALTERNATIVA ERRADA.** A função de emitir certificados digitais é da Autoridade Certificadora (AC). A Autoridade de Registro (AR) apenas valida e encaminha os dados.

B) **ALTERNATIVA ERRADA.** Executar as políticas de certificados e normas não é uma das funções da Autoridade de Registro (AR), mas sim do Instituto Nacional de Tecnologia da Informação (ITI), que também atua como Autoridade Certificadora Raiz (AC-Raiz).

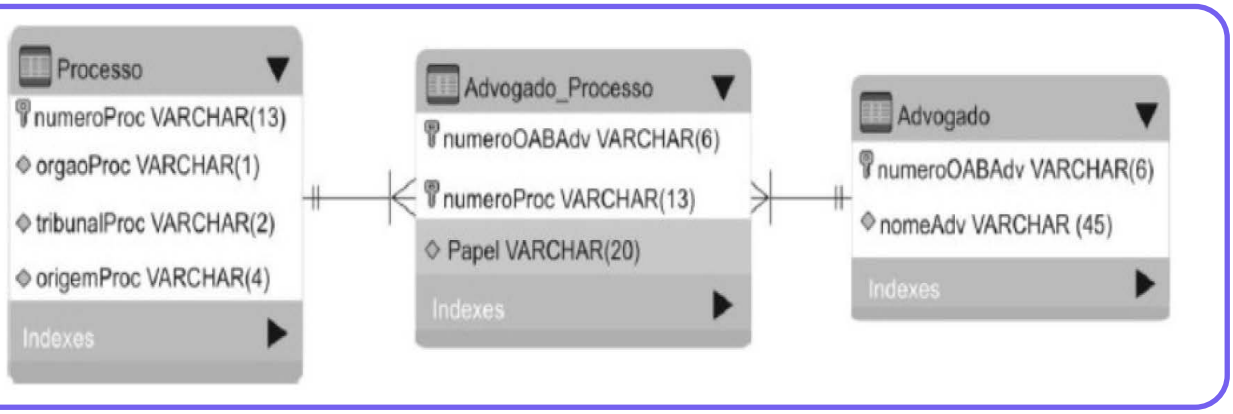
C) **ALTERNATIVA ERRADA.** Realizar auditorias operacionais em entidades subordinadas é uma função da AC-Raiz, não da Autoridade de Registro.

D) **ALTERNATIVA ERRADA.** Disponibilizar a infraestrutura física e lógica e dos recursos humanos especializados às Autoridades Certificadoras não é uma função da Autoridade de Registro. Cada Autoridade Certificadora (AC) é responsável pela sua própria infraestrutura.

E) **ALTERNATIVA CORRETA!** A Autoridade de Registro é responsável por validar a identidade de usuários presencialmente, verificar a documentação exigida, coletar suas informações e encaminhar as solicitações de certificados às Autoridades Certificadoras.

Gabarito: E

22. (FCC - MPE PB - 2023) O banco de dados de um órgão do Judiciário foi modelado conforme imagem abaixo, utilizando o Modelo Entidade-Relacionamento (MER).



Foi criado um banco de dados chamado MPEPB123 com as tabelas referentes ao modelo e os dados abaixo foram cadastrados. Considere para todas as questões que o banco de dados está aberto e em condições ideais.

Tabela Processo			
numeroProc	**orgaoProc**	**tribunalProc**	**origemProc**
0001842672017	5	01	0246
0045613912014	8	19	0004
0056712432022	6	14	0023
0002347652022	8	02	0341

Tabela Advogado	
numeroOABAdv	**nomeAdv**
28H418	Marcos Vieira Dias
34.443	Fabiana Duque Zanon

Tabela Advogado Processo		
numeroOABAdv	**numeroProc**	**papel**
28H418	0001842672017	Defesa
34.443	0045613912014	Defesa
28H418	0056712432022	Acusação
28H418	0045613912014	Acusação
34.443	0056712432022	Acusação
34.443	0001842672017	Acusação

Considerando o uso do sistema gerenciador de banco de dados MySQL, para criar a tabela Advogado_Processo, utiliza-se a instrução SQL:

A) CREATE TABLE Advogado_Processo (

numeroOABAdv VARCHAR(6) NOT NULL,
numeroProc VARCHAR(13) NOT NULL,
papel VARCHAR(20),
PRIMARY KEY (numeroOABAdv, numeroProc),
FOREIGN KEY (numeroOABAdv)
REFERENCE Advogado(numeroOABAdv),
FOREIGN KEY (numeroProc)
REFERENCE Processo(numeroProc)
);

B) CREATE TABLE Advogado_Processo (

numeroOABAdv VARCHAR(6) NOT NULL,
numeroProc VARCHAR(13) NOT NULL,
papel VARCHAR(20),
PRIMARY KEY (numeroOABAdv, numeroProc),
FOREIGN KEY (numeroOABAdv)
CONSTRAINT Advogado(numeroOABAdv),
FOREIGN KEY (numeroProc)
CONSTRAINT Processo(numeroProc)
);

C) CREATE TABLE Advogado_Processo (

numeroOABAdv VARCHAR(6) NOT NULL,
numeroProc VARCHAR(13) NOT NULL,
papel VARCHAR(20),
PRIMARY KEY (numeroOABAdv, numeroProc),
FOREIGN KEY (numeroOABAdv)
REFERENCES Advogado(numeroOABAdv),
FOREIGN KEY (numeroProc)
REFERENCES Processo(numeroProc)
);

D) CREATE TABLE Advogado_Processo (

numeroOABAdv VARCHAR(6) NOT NULL,
numeroProc VARCHAR(13) NOT NULL,
papel VARCHAR(20),
PRIMARY KEY (numeroOABAdv, numeroProc),
FOREIGN KEY (numeroOABAdv)
FROM Advogado(numeroOABAdv),
FOREIGN KEY (numeroProc)
FROM Processo(numeroProc)
);

E) CREATE TABLE Advogado_Processo (

numeroOABAdv VARCHAR(6) NOT NULL,
numeroProc VARCHAR(13) NOT NULL,
idPet INT NOT NULL,
PRIMARY KEY (numeroOABAdv, numeroProc),
FOREIGN KEY (numeroOABAdv),
FOREIGN KEY (numeroProc)
);

Comentários:

Temos o caso de uma tabela associativa, também conhecida como tabela de junção ou tabela intermediária. É construída para modelar um relacionamento muitos-para-muitos (N:N) entre duas tabelas principais. Utiliza-se das chaves primárias das duas tabelas como chaves estrangeiras; a combinação das duas chaves estrangeiras forma a sua chave primária composta. Em alguns casos, pode conter colunas adicionais com informações complementares. Veremos as alternativas a seguir:

A) Há um erro na sintaxe da linguagem SQL, pois está escrito REFERENCE (sem o "S" no final), quando deveria ser REFERENCES. Isso causaria um erro ao executar o script SQL. Entretanto, todo o restante está correto. Alternativa incorreta.

B) Há um erro também na sintaxe da linguagem SQL, porém, esse erro é mais grotesco. A palavra-chave CONSTRAINT está sendo usada de maneira errônea. Em seu lugar deveria ser usado "REFERENCES". CONSTRAINT é usada para nomear uma restrição, não para definir a referência da chave estrangeira.

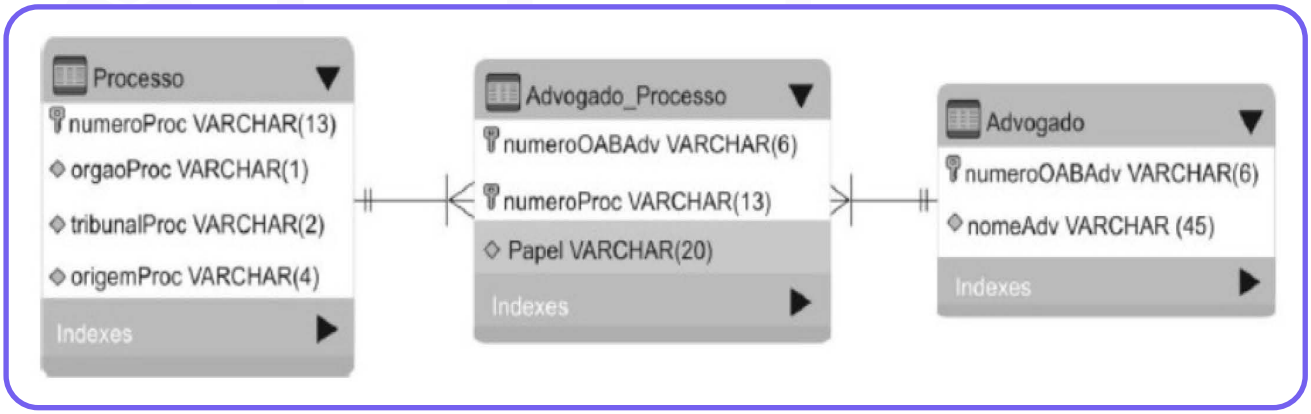
C) Alternativa correta! Temos aqui um código correto em SQL. Toda a sintaxe está sendo utilizada corretamente, assim como as referências das chaves estrangeiras. Há a definição da chave primária como uma chave composta e posteriormente há a definição das chaves estrangeiras referenciando corretamente as demais tabelas.

D) Uso errado da palavra FROM após a declaração da chave estrangeira. Deveria ter sido utilizado REFERENCES para referenciar a origem da chave estrangeira. FROM é utilizado em comandos como SELECT e DELETE indicando a origem dos dados. Alternativa incorreta.

E) Alternativa incorreta. As declarações de FOREIGN KEY estão incompletas. Há um erro, pois não são indicadas as referências de cada chave estrangeira. As cláusulas REFERENCES estão ausentes.

Gabarito: C

23. (FCC - MPE PB - 2023) O banco de dados de um órgão do Judiciário foi modelado conforme imagem abaixo, utilizando o Modelo Entidade-Relacionamento (MER).



Foi criado um banco de dados chamado MPEPB123 com as tabelas referentes ao modelo e os dados abaixo foram cadastrados. Considere para todas as questões que o banco de dados está aberto e em condições ideais.

Tabela Processo			
numeroProc	orgaoProc	tribunalProc	origemProc
0001842672017	5	01	0246
0045613912014	8	19	0004
0056712432022	6	14	0023
0002347652022	8	02	0341

Tabela Advogado	
numeroOABAdv	nomeAdv
28H418	Marcos Vieira Dias
34.443	Fabiana Duque Zanon

Tabela Advogado Processo		
numeroOABAdv	numeroProc	papel
28H418	0001842672017	Defesa
34.443	0045613912014	Defesa
28H418	0056712432022	Acusação
28H418	0045613912014	Acusação
34.443	0056712432022	Acusação
34.443	0001842672017	Acusação

Considere os comandos SQL abaixo.

I. INSERT INTO Advogado (numeroOABAdv, nomeAdv) VALUES ('59.445', 'Paulo Vieira Lima');

II. INSERT INTO Advogado VALUES ('28E418', 'Ana Maria Fonseca');

III. INSERT INTO Advogado ('21X400', 'Marcos Moreira Costa');

IV. INSERT INTO Advogado FIELDS(numeroOABAdv, nomeAdv) VALUES ('01.342', 'Mariana Freitas Caetano');

Os comandos que inserem corretamente dados na tabela Advogado são os que constam APENAS em

A) I e II.

B) I, II e III.

C) I e IV.

D) II e III.

E) III e IV.

Comentários:

Vamos analisar cada comando SQL:

I. INSERT INTO Advogado (numeroOABAdv, nomeAdv) VALUES ('59.445', 'Paulo Vieira Lima');

- **CORRETO.** Esse comando está inserindo valores específicos nas colunas numeroOABAdv e nomeAdv da tabela Advogado.

II. INSERT INTO Advogado VALUES ('28E418', 'Ana Maria Fonseca');

- **CORRETO.** Esse comando está inserindo valores nas colunas da tabela Advogado na ordem em que foram definidas, e as colunas são fornecidas na ordem correta.

III. INSERT INTO Advogado ('21X400', 'Marcos Moreira Costa');

- **INCORRETO.** Esse comando possui uma sintaxe incorreta. O correto seria fornecer os valores após a cláusula VALUES, como em I e II.

IV. INSERT INTO Advogado FIELDS(numeroOABAdv, nomeAdv) VALUES ('01.342', 'Mariana Freitas Caetano');

- **INCORRETO.** A sintaxe correta seria utilizar a palavra-chave VALUES para fornecer os valores, sem a necessidade da palavra-chave FIELDS.

Portanto, os comandos que inserem corretamente dados na tabela Advogado são aqueles que constam APENAS em: a) I e II.

Gabarito: A

24. (FCC - MPE PB - 2023) O banco de dados de um órgão do Judiciário foi modelado conforme imagem abaixo, utilizando o Modelo Entidade-Relacionamento (MER).

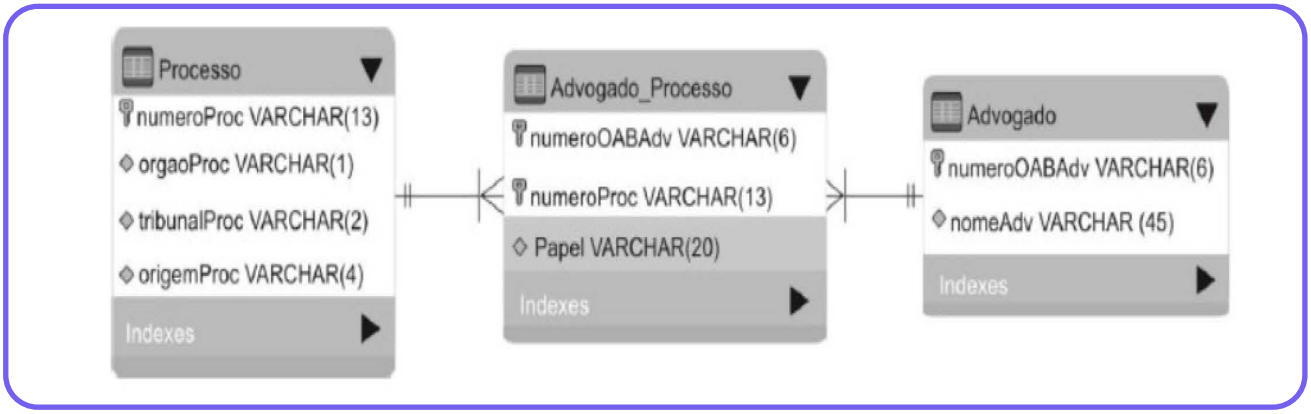


Tabela Processo			
numeroProc	**orgaoProc**	**tribunalProc**	**origemProc**
0001842672017	5	01	0246
0045613912014	8	19	0004
0056712432022	6	14	0023
0002347652022	8	02	0341

Tabela Advogado	
numeroOABAdv	**nomeAdv**
28H418	Marcos Vieira Dias
34.443	Fabiana Duque Zanon

Tabela Advogado Processo		
numeroOABAdv	**numeroProc**	**papel**
28H418	0001842672017	Defesa
34.443	0045613912014	Defesa
28H418	0056712432022	Acusação
28H418	0045613912014	Acusação
34.443	0056712432022	Acusação
34.443	0001842672017	Acusação

Um analista digitou uma *query* SQL para exibir os processos em que a advogada com número de OAB 34.443, Fabiana Duque Zanon atua no papel de Acusação. A consulta retornou o seguinte resultado:

Processo	Advogado
0001842672017	Fabiana Duque Zanon
0056712432022	Fabiana Duque Zanon

O comando SQL digitado foi

A) SELECT numeroProc AS Processo, (SELECT nomeAdv FROM Advogado) AS Advogado FROM Advogado_Processo WHERE numeroOABAdv = '34.443' AND papel = "Acusação";

B) SELECT numeroProc AS Processo FROM Advogado_Processo INNER JOIN Advogado ON nomeAdv AS Advogado WHERE numeroOABAdv = '34.443' AND papel = "Acusação";

C) SELECT numeroProc AS Processo, (SELECT * FROM Advogado WHERE numeroOABAdv = '34.443') AS Advogado FROM Advogado_Processo WHERE numeroOABAdv = '34.443' AND papel = "Acusação";

D) SELECT numeroProc AS Processo, nomeAdv AS Advogado FROM Advogado_Processo WHERE numeroOABAdv = '34.443' AND papel = "Acusação";

E) SELECT numeroProc AS Processo, (SELECT nomeAdv FROM Advogado WHERE numeroOABAdv = '34.443') AS Advogado FROM Advogado_Processo WHERE numeroOABAdv = '34.443' AND papel = "Acusação";

Comentários:

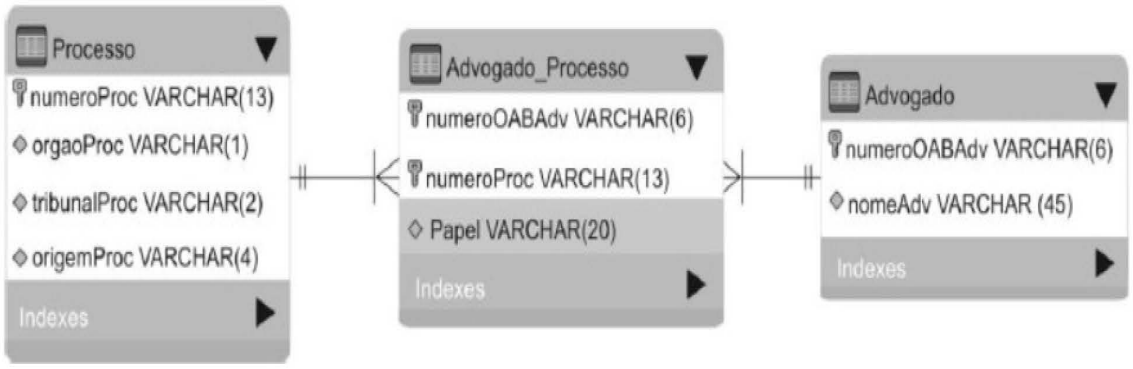
Vamos analisar a opção E para verificar a resposta correta:

E) SELECT numeroProc AS Processo, (SELECT nomeAdv FROM Advogado WHERE numeroOABAdv = '34.443') AS Advogado FROM Advogado_Processo WHERE numeroOABAdv = '34.443' AND papel = 'Acusação';

Essa consulta está usando uma subconsulta para obter o nome do advogado da tabela Advogado cujo número da OAB é “34.443”, e a coluna Advogado_Processo está sendo renomeada como Advogado. Portanto, essa consulta está correta.

Gabarito: E

25. (FCC - MPE PB - 2023) O banco de dados de um órgão do Judiciário foi modelado conforme imagem abaixo, utilizando o Modelo Entidade-Relacionamento (MER).



Foi criado um banco de dados chamado MPEPB123 com as tabelas referentes ao modelo e os dados abaixo foram cadastrados. Considere para todas as questões que o banco de dados está aberto e em condições ideais.

Tabela Processo			
numeroProc	**orgaoProc**	**tribunalProc**	**origemProc**
0001842672017	5	01	0246
0045613912014	8	19	0004
0056712432022	6	14	0023
0002347652022	8	02	0341

Tabela Advogado	
numeroOABAdv	**nomeAdv**
28H418	Marcos Vieira Dias
34.443	Fabiana Duque Zanon

Tabela Advogado Processo		
numeroOABAdv	**numeroProc**	**papel**
28H418	0001842672017	Defesa
34.443	0045613912014	Defesa
28H418	0056712432022	Acusação
28H418	0045613912014	Acusação
34.443	0056712432022	Acusação
34.443	0001842672017	Acusação

Uma analista utilizou um comando que selecionou e exibiu os dados, na forma abaixo, de todo processo que tem advogado a ele associado.

numeroProc	tribunalProc	nomeAdv	papel
0001842672017	01	Marcos Vieira Dias	Defesa
0001842672017	19	Marcos Vieira Dias	Acusação
0056712432022	14	Marcos Vieira Dias	Acusação
0001842672017	01	Fabiana Duque Zanon	Acusação
0045613912014	19	Fabiana Duque Zanon	Defesa
0056712432022	14	Fabiana Duque Zanon	Acusação

A instrução SQL utilizada pela analista foi

A) SELECT Advogado_Processo.numeroProc, Processo.tribunalProc, Advogado.nomeAdv, Advogado_Processo.papel FROM Advogado_Processo (LEFT JOIN Processo ON Advogado_Processo.numeroProc = Processo.numeroProc, RIGHT JOIN Advogado ON Advogado_Processo.numeroOABAdv = Advogado.numeroOABAdv);

B) SELECT Advogado_Processo.numeroProc, Processo.tribunalProc, Advogado.nomeAdv, Advogado_Processo.papel FROM Advogado_Processo FULL JOIN Processo ON Advogado_Processo.numeroProc = Processo.numeroProc AND Advogado ON Advogado_Processo.numeroOABAdv = Advogado.numeroOABAdv);

C) SELECT Advogado_Processo.numeroProc, Processo.tribunalProc, Advogado.nomeAdv, Advogado_Processo.papel FROM Advogado_Processo INNER JOIN Processo ON Advogado_Processo.numeroProc = Processo.numeroProc, INNER JOIN Advogado ON Advogado_Processo.numeroOABAdv = Advogado.numeroOABAdv;

D) SELECT Advogado_Processo.numeroProc, Processo.tribunalProc, Advogado.nomeAdv, Advogado_Processo.papel FROM ((Advogado_Processo INNER JOIN Processo ON Advogado_Processo.numeroProc = Processo.numeroProc) INNER JOIN Advogado ON Advogado_Processo.numeroOABAdv = Advogado.numeroOABAdv);

E) SELECT Advogado_Processo.numeroProc, Processo.tribunalProc, Advogado.nomeAdv, Advogado_Processo.papel FROM Advogado_Processo JOIN Processo ON Advogado_Processo.numeroProc = Processo.numeroProc AND JOIN Advogado ON Advogado_Processo.numeroOABAdv = Advogado.numeroOABAdv;

Comentários:

Vamos analisar cada opção de instrução SQL:

A) SELECT Advogado_Processo.numeroProc, Processo.tribunalProc, Advogado.nomeAdv, Advogado_Processo.papel FROM Advogado_Processo (LEFT JOIN Processo ON Advogado_Processo.numeroProc = Processo.numeroProc, RIGHT JOIN Advogado ON Advogado_Processo.numeroOABAdv = Advogado.numeroOABAdv);

- **INCORRETO.** A mistura de LEFT JOIN e RIGHT JOIN em uma única instrução não é válida. Além disso, faltam as condições de junção para a tabela Advogado_Processo.

B) SELECT Advogado_Processo.numeroProc, Processo.tribunalProc, Advogado.nomeAdv, Advogado_Processo.papel FROM Advogado_Processo FULL JOIN Processo ON Advogado_Processo.numeroProc = Processo.numeroProc AND Advogado ON Advogado_Processo.numeroOABAdv = Advogado.numeroOABAdv);

- **INCORRETO.** A cláusula ON deveria ser usada apenas após o FULL JOIN, mas nesse caso, ela está sendo usada após o JOIN com Advogado.

C) SELECT Advogado_Processo.numeroProc, Processo.tribunalProc, Advogado.nomeAdv, Advogado_Processo.papel FROM Advogado_Processo INNER JOIN Processo ON Advogado_Processo.numeroProc = Processo.numeroProc, INNER JOIN Advogado ON Advogado_Processo.numeroOABAdv = Advogado.numeroOABAdv;

- **INCORRETO.** O uso de vírgulas para separar as condições INNER JOIN está incorreto. Deveria ser usado AND ou WHERE para unir as condições.

D) SELECT Advogado_Processo.numeroProc, Processo.tribunalProc, Advogado.nomeAdv, Advogado_Processo.papel FROM ((Advogado_Processo INNER JOIN Processo ON Advogado_Processo.numeroProc = Processo.numeroProc) INNER JOIN Advogado ON Advogado_Processo.numeroOABAdv = Advogado.numeroOABAdv);

- **CORRETO.** Essa instrução utiliza INNER JOIN corretamente para unir as três tabelas.

E) SELECT Advogado_Processo.numeroProc, Processo.tribunalProc, Advogado.nomeAdv, Advogado_Processo.papel FROM Advogado_Processo JOIN Processo ON Advogado_Processo.numeroProc = Processo.numeroProc AND JOIN Advogado ON Advogado_Processo.numeroOABAdv = Advogado.numeroOABAdv;

- **INCORRETO.** O uso de AND JOIN não é uma sintaxe válida. Deveria ser apenas JOIN.

Portanto, a opção correta é a letra D: "SELECT Advogado_Processo.numeroProc, Processo.tribunalProc, Advogado.nomeAdv, Advogado_Processo.papel FROM ((Advogado_Processo INNER JOIN Processo ON Advogado_Processo.numeroProc = Processo.numeroProc) INNER JOIN Advogado ON Advogado_Processo.numeroOABAdv = Advogado.numeroOABAdv);"

Gabarito: D

26. (FCC - MPE PB - 2023) O banco de dados de um órgão do Judiciário foi modelado conforme imagem abaixo, utilizando o Modelo Entidade-Relacionamento (MER).

Foi criado um banco de dados chamado MPEPB123 com as tabelas referentes ao modelo e os dados abaixo foram cadastrados. Considere para todas as questões que o banco de dados está aberto e em condições ideais.

Tabela Processo			
numeroProc	**orgaoProc**	**tribunalProc**	**origemProc**
0001842672017	5	01	0246
0045613912014	8	19	0004
0056712432022	6	14	0023
0002347652022	8	02	0341

Tabela Advogado	
numeroOABAdv	**nomeAdv**
28H418	Marcos Vieira Dias
34.443	Fabiana Duque Zanon

Tabela Advogado Processo		
numeroOABAdv	numeroProc	papel
28H418	0001842672017	Defesa
34.443	0045613912014	Defesa
28H418	0056712432022	Acusação
28H418	0045613912014	Acusação
34.443	0056712432022	Acusação
34.443	0001842672017	Acusação

Em um banco de dados Oracle, um analista utilizou um comando que retornou, da tabela Processo, os dados mostrados abaixo.

Ano

2017

2022

2014

2022

O comando utilizado pelo analista foi

A) SELECT SUBSTR(numeroProc,-4,4) AS Ano FROM Processo;

B) SELECT SUBSTRING(-4,4,numeroProc) AS Ano FROM Processo;

C) SELECT SUBSTR(numeroProc,4,10) AS Ano FROM Processo;

D) SELECT SUBSTRING(10,4,numeroProc) AS Ano FROM Processo;

E) SELECT SUBSTRING(numeroProc from 9 for 4) AS Ano FROM Processo;

Comentários:

O comando utilizado pelo analista para extrair o ano da tabela Processo foi:

A) SELECT SUBSTR(numeroProc,-4,4) AS Ano FROM Processo;

- **CORRETO.** A função SUBSTR é usada para extrair uma parte específica de uma string. Nesse caso, ela está extraindo os últimos 4 caracteres (o ano) da coluna numeroProc e renomeando a coluna resultante como "Ano".

B) SELECT SUBSTRING(-4,4,numeroProc) AS Ano FROM Processo;

- **INCORRETO.** Há um erro na sintaxe. A função correta no Oracle é SUBSTR, não SUBSTRING, e os parâmetros estão fora de ordem.

C) SELECT SUBSTR(numeroProc,4,10) AS Ano FROM Processo;

- **INCORRETO.** A função SUBSTR espera a posição inicial e o comprimento como parâmetros, e aqui parece haver uma confusão nos parâmetros.

D) SELECT SUBSTRING(10,4,numeroProc) AS Ano FROM Processo;

- **INCORRETO.** Novamente, há um erro na sintaxe. A função correta é SUBSTR no Oracle, e os parâmetros estão fora de ordem.

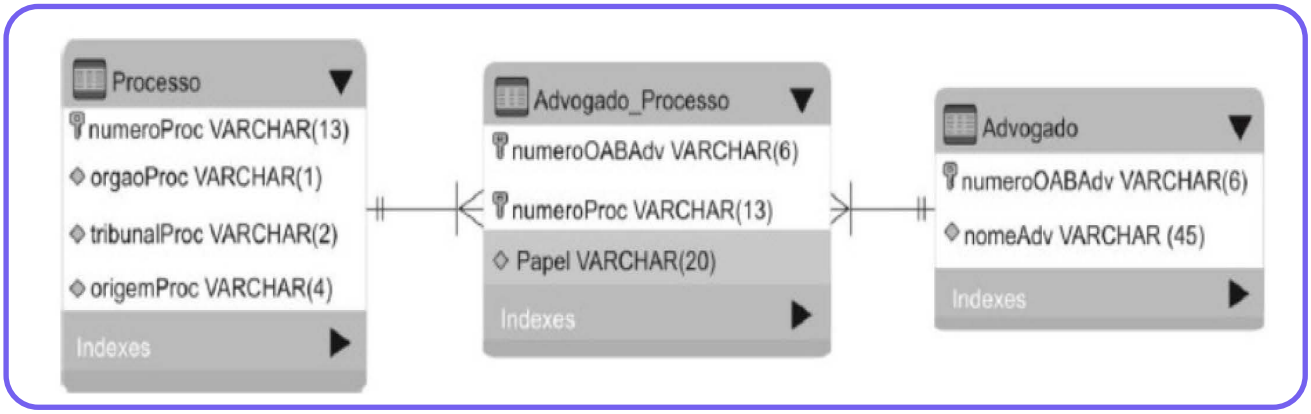
E) SELECT SUBSTRING(numeroProc from 9 for 4) AS Ano FROM Processo;

- **INCORRETO.** A sintaxe correta para SUBSTRING no Oracle é SUBSTR, e os parâmetros estão fora de ordem.

Portanto, a opção correta é a letra A: "SELECT SUBSTR(numeroProc,-4,4) AS Ano FROM Processo;".

Gabarito: A

27. (FCC - MPE PB - 2023) O banco de dados de um órgão do Judiciário foi modelado conforme imagem abaixo, utilizando o Modelo Entidade-Relacionamento (MER).



Foi criado um banco de dados chamado MPEPB123 com as tabelas referentes ao modelo e os dados abaixo foram cadastrados. Considere para todas as questões que o banco de dados está aberto e em condições ideais.

Tabela Processo			
numeroProc	**orgaoProc**	**tribunalProc**	**origemProc**
0001842672017	5	01	0246
0045613912014	8	19	0004
0056712432022	6	14	0023
0002347652022	8	02	0341

Tabela Advogado	
numeroOABAdv	**nomeAdv**
28H418	Marcos Vieira Dias
34.443	Fabiana Duque Zanon

Tabela Advogado Processo		
numeroOABAdv	**numeroProc**	**papel**
28H418	0001842672017	Defesa
34.443	0045613912014	Defesa
28H418	0056712432022	Acusação
28H418	0045613912014	Acusação
34.443	0056712432022	Acusação
34.443	0001842672017	Acusação

A instrução SQL utilizada para exibir o número de valores distintos cadastrados no campo papel da tabela Advogado_Processo é

A) SELECT DISTINCT COUNT(papel) FROM Advogado_Processo;

B) SELECT NUMBER(DISTINCT papel) FROM Advogado_Processo;

C) SELECT COUNT(DISTINCT papel) FROM Advogado_Processo;

D) COUNT (DISTINCT papel) FROM Advogado_Processo;

E) SELECT SUM(DISTINCT papel) FROM Advogado_Processo;

Comentários:

A instrução SQL correta para exibir o número de valores distintos cadastrados no campo "papel" da tabela Advogado_Processo é:

C) SELECT COUNT(DISTINCT papel) FROM Advogado_Processo;

- A função DISTINCT é usada para garantir que apenas valores distintos sejam considerados.
- A função COUNT é usada para contar o número de valores distintos.

Portanto, a instrução correta é aquela que utiliza COUNT(DISTINCT papel) para contar os valores distintos na coluna "papel" da tabela Advogado_Processo.

Analisando as demais alternativas, temos:

A) Erro de ordem de aplicação das funções COUNT e DISTINCT.

B) NUMBER não é uma função SQL. A função para contar á COUNT( ).

D) Erro por não utilizar o comando SELECT no início da consulta.

E) Erro por utilizar a função SUM( ), que retorna a soma dos valores, mas não a contagem de valores distintos como solicitado no enunciado.

Gabarito: C

28. (FCC - MPE PB - 2023) O banco de dados de um órgão do Judiciário foi modelado conforme imagem abaixo, utilizando o Modelo Entidade-Relacionamento (MER).

Foi criado um banco de dados chamado MPEPB123 com as tabelas referentes ao modelo e os dados abaixo foram cadastrados. Considere para todas as questões que o banco de dados está aberto e em condições ideais.

Tabela Processo			
numeroProc	orgaoProc	tribunalProc	origemProc
0001842672017	5	01	0246
0045613912014	8	19	0004
0056712432022	6	14	0023
0002347652022	8	02	0341

Tabela Advogado	
numeroOABAdv	nomeAdv
28H418	Marcos Vieira Dias
34.443	Fabiana Duque Zanon

Tabela Advogado Processo		
numeroOABAdv	numeroProc	papel
28H418	0001842672017	Defesa
34.443	0045613912014	Defesa
28H418	0056712432022	Acusação
28H418	0045613912014	Acusação

Tabela Advogado Processo		
numeroOABAdv	numeroProc	papel
34.443	0056712432022	Acusação
34.443	0001842672017	Acusação

Para alterar o papel do advogado com OAB 28H418 no processo 0001842672017 para Acusação, utiliza-se a instrução SQL:

A) ALTER TABLE Advogado_Processo SET papel = 'Acusação' WHERE numeroOABAdv = '28H418' AND numeroProc = '0001842672017';

B) UPDATE Advogado_Processo SET papel = 'Acusação' WHERE numeroOABAdv = '28H418' AND numeroProc = '0001842672017';

C) ALTER COLUMN papel TO 'Acusação' FROM Advogado_Processo WHERE numeroOABAdv = '28H418' AND numeroProc = '0001842672017';

D) UPDATE (papel) FROM Advogado_Processo VALUE('Acusação') WHERE numeroOABAdv = '28H418' AND numeroProc = '0001842672017';

E) UPDATE papel TO 'Acusação' FROM Advogado_Processo WHERE numeroOABAdv = '28H418' AND numeroProc = '0001842672017';

Comentários:

A instrução SQL correta para alterar o papel do advogado com OAB 28H418 no processo 0001842672017 para "Acusação" é:

B) UPDATE Advogado_Processo SET papel = 'Acusação' WHERE numeroOABAdv = '28H418' AND numeroProc = '0001842672017';

A instrução UPDATE é usada para modificar os dados em uma tabela.

SET papel = 'Acusação' define o novo valor para o campo "papel".

A cláusula WHERE especifica as condições para selecionar a linha a ser atualizada, garantindo que apenas o advogado com OAB 28H418 e o processo 0001842672017 sejam afetados.

Portanto, a instrução correta é a opção B.

Analisando as demais alternativas, temos:

A) ALTER TABLE é utilizado para modificar a estrutura da tabela, não os dados contidos nela. Alternativa incorreta.

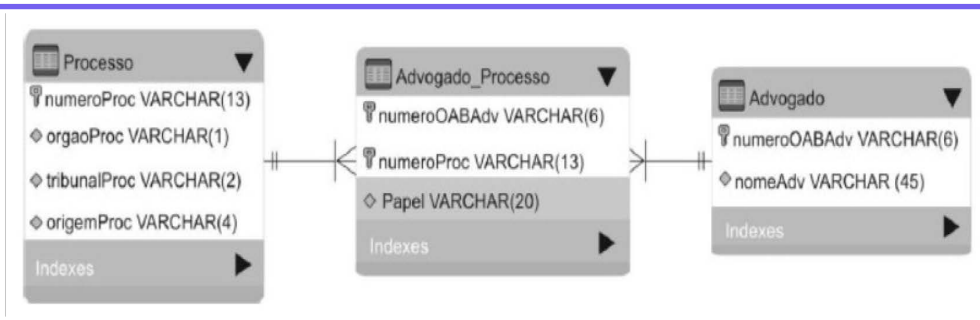
C) ALTER COLUMN é utilizado para modificar a coluna de uma tabela, não os dados contidos nela, além de ter erro de sintaxe no comando. Alternativa incorreta.

D) Erro de sintaxe do comando, misturando parâmetros da sintaxe do comando INSERT.

E) Erro de sintaxe do comando, misturando parâmetros da sintaxe de outros comandos (TO e FROM)."

Gabarito: B

29. (FCC - MPE PB - 2023) O banco de dados de um órgão do Judiciário foi modelado conforme imagem abaixo, utilizando o Modelo Entidade-Relacionamento (MER).



Foi criado um banco de dados chamado MPEPB123 com as tabelas referentes ao modelo e os dados abaixo foram cadastrados. Considere para todas as questões que o banco de dados está aberto e em condições ideais.

Tabela Processo			
numeroProc	**orgaoProc**	**tribunalProc**	**origemProc**
0001842672017	5	01	0246
0045613912014	8	19	0004
0056712432022	6	14	0023
0002347652022	8	02	0341

Tabela Advogado	
numeroOABAdv	**nomeAdv**
28H418	Marcos Vieira Dias
34.443	Fabiana Duque Zanon

Tabela Advogado Processo		
numeroOABAdv	**numeroProc**	**papel**
28H418	0001842672017	Defesa
34.443	0045613912014	Defesa
28H418	0056712432022	Acusação
28H418	0045613912014	Acusação

Em uma transação Oracle, uma analista criou um ponto de salvamento chamado pontoA e inseriu 3 novos advogados na tabela Advogado. Em seguida, criou um ponto de salvamento chamado pontoB e inseriu mais 2 advogados. Se esta analista quiser reverter a inserção dos 2 últimos advogados, mantendo somente as 3 primeiras inserções, ela poderá utilizar o comando

A) ROLLBACK TRANSACTION UNTIL pontoB;

B) RESTORE DATABASE to pontoB;

C) ROLLBACK TO pontoB;

D) RESTORE TRANSACTION TO pontoB;

E) ROLLBACK UNTIL pontoB WITH REVERT STATE;

Comentários:

Vamos lá, pessoal! A questão aborda conhecimentos de transações, linguagem SQL e savepoints em Banco de Dados. Vamos analisar cada alternativa a seguir:

A) A cláusula ROLLBACK TRANSACTION UNTIL não existe. O correto seria apenas ROLLBACK TO <savepoint>. Alternativa incorreta.

B) RESTORE DATABASE não é um comando SQL da Oracle para retornar a um savepoint de um banco de dados. Queremos retornar a um savepoint, não a um banco de dados, como informado pela cláusula DATABASE. Alternativa incorreta.

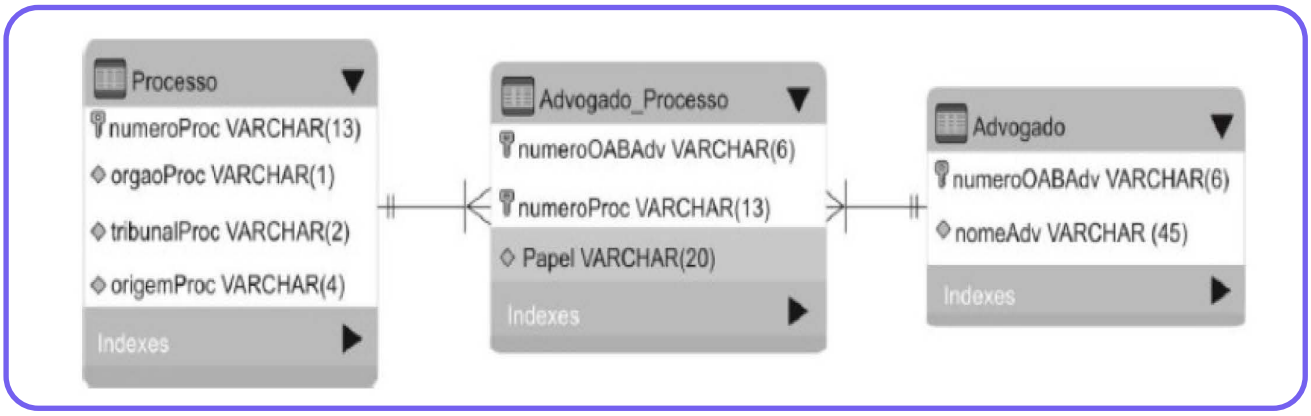
C) ROLLBACK TO pontoB. Temos aqui a nossa alternativa correta. O comando foi corretamente indicado, com a sintaxe SQL correta ROLLBACK TO <savepoint>, indicando o pontoB, já quequeríamos desfazer apenas os 2 últimos, mantendo as 3 primeiras inserções do savepoint pontoA. Também estaria correto dizer ROLLBACK TO SAVEPOINT pontoB, mas o SAVEPOINT não é necessário. Alternativa correta.

D) RESTORE TRANSACTION TO não é um comando SQL válido. O correto é ROLLBACK. Alternativa incorreta.

E) ROLLBACK UNTIL pontoB WITH REVERT STATE. O comando está incorreto, não há a cláusula UNTIL após ROLLBACK, assim como não há WITH REVERT STATE. Alternativa incorreta.

Gabarito: C

30. (FCC - MPE PB - 2023) O banco de dados de um órgão do Judiciário foi modelado conforme imagem abaixo, utilizando o Modelo Entidade-Relacionamento (MER).



Foi criado um banco de dados chamado MPEPB123 com as tabelas referentes ao modelo e os dados abaixo foram cadastrados. Considere para todas as questões que o banco de dados está aberto e em condições ideais.

Tabela Processo			
numeroProc	orgaoProc	tribunalProc	origemProc
0001842672017	5	01	0246
0045613912014	8	19	0004
0056712432022	6	14	0023
0002347652022	8	02	0341

Tabela Advogado	
numeroOABAdv	nomeAdv
28H418	Marcos Vieira Dias
34.443	Fabiana Duque Zanon

Tabela Advogado Processo		
numeroOABAdv	numeroProc	papel
28H418	0001842672017	Defesa
34.443	0045613912014	Defesa
28H418	0056712432022	Acusação
28H418	0045613912014	Acusação

Considere a Stored Procedure abaixo, criada no banco de dados MySQL.

```
delimiter //
    I
BEGIN
SELECT nomeAdv INTO nome FROM Advogado
WHERE numeroOABAdv = oab;
END//
delimiter;
CALL obterNome('28H418', @nome);
SELECT @nome AS NomeAdvogado;
```

Para que, ao executar esta sequência de comandos, seja exibido corretamente o nome do advogado Marcos Vieira Dias, cujo número OAB é 28H418, a lacuna I deve ser preenchida com

A) CREATE STORED PROCEDURE obterNome(CHAR(6) oab, CHAR(45) nome OUT)

B) CREATE PROCEDURE obterNome(IN oab VARCHAR(6), OUT nome VARCHAR(45))

C) CREATE PROCEDURE obterNome(VARCHAR(6) oab, VARCHAR(45) nome)

D) CREATE STORED PROCEDURE obterNome(IN oab CHAR(6), OUT nome CHAR(45))

E) CREATE PROCEDURE obterNome(String oab, String nome)

Comentários:

Segundo a documentação do MySQL, a sintaxe para definir uma stored procedure é ***CREATE PROCEDURE nome_do_stored_procedure (parâmetros)***, em que cada parâmetro é descrito como ***[IN | OUT | INOUT] nome tipo*** (os colchetes significam que essa parte é opcional; sua omissão equivale a IN).

Analisando a chamada à stored procedure (CALL obterNome(...)), vemos que seu nome é **obterNome**. O corpo da stored procedure revela os nomes dos parâmetros:

- SELECT nomeAdv INTO nome → parâmetro de saída chamado **nome**, provavelmente do tipo VARCHAR(45), pois este é o tipo de nomeAdv na tabela Advogados.
- WHERE numeroOABAdv = oab → parâmetro de entrada chamado **oab**, provavelmente do tipo VARCHAR(6), pois esse é o tipo de numeroOABAdv na tabela Advogados.

Analisando mais uma vez a linha de chamada do procedimento, CALL obterNome('28H418', @nome), vê-se que o parâmetro de entrada foi declarado antes do de saída.

Portanto, a lacuna I deve ser preenchida por CREATE PROCEDURE obterNome(IN oab VARCHAR(6), OUT nome VARCHAR(45)), como no item B.

Adendo: As linhas "*delimiter //*" e "*delimiter ;*" servem para que os operadores "ponto e vírgula" (";") não sejam interpretados pelo mysql até o fim da declaração do procedimento, já que o ";" tem, em MySQL, assim como na maioria dos sistemas gerenciadores de banco de dados, o papel de "avisar" ao sistema que o comando mais recente está pronto para ser executado.

Fonte: https://dev.mysql.com/doc/refman/8.4/en/create-procedure.html

Gabarito: B

31. (FCC - MPE PB - 2023) No PostgreSQL, para conceder o privilégio de ser membro do papel analistas à usuária Paula, utiliza-se a instrução

A) ENABLE ACCESS FOR analistas TO Paula;

B) CREATE ROLE analistas TO Paula;

C) GRANT ROLE('analistas') TO USER('root');

D) GRANT analistas TO Paula;

E) ENABLE analistas TO Paula;

Comentários:

Questão que aborda conhecimentos sobre PostgreSQL e comandos de elevação de privilégio a usuários. Vamos analisar cada alternativa a seguir:

A) Erro de instrução no PostgreSQL. ENABLE ACCESS FOR não é um comando existente em SQL. A banca tentou persuadir ao inventar um comando com dizeres da linguagem natural em inglês como se fossem SQL. Alternativa incorreta.

B) O comando CREATE ROLE cria um novo papel, mas não concede essa criação a alguém. Não há a cláusula TO, como indicado. Alternativa incorreta.

C) Alternativa mais próxima de estar correta, porém, ainda incorreta. Após o comando GRANT não se deve utilizar ROLE para indicar o papel, nem USER após TO para indicar o usuário. ROLE é usado após CREATE na criação, por exemplo. Alternativa incorreta.

D) Sintaxe correta do comando solicitado no enunciado. “GRANT” indica a concessão de um papel a um usuário indicado após “TO”. GRANT <role> TO <usuario> é a sintaxe correta do comando solicitado. Portanto, temos aqui a nossa alternativa correta.

E) Não existe o comando ENABLE em SQL para conceder privilégios. Alternativa incorreta.

Gabarito: D

32. (FCC - MPE PB - 2023) Um analista está usando uma ferramenta de gerenciamento de migrações de banco de dados que ajuda a manter a consistência dos esquemas em várias instâncias. Nessa ferramenta, em condições ideais, ele digitou o comando abaixo.

I -user=mppb -password=justice -url=jdbc:mysql://localhost:3306/mppbdb -locations=filesystem:/mppb/bd/data II

Para aplicar todas as migrações disponíveis que ainda não foram aplicadas ao banco de dados MySQL mppbdb usando o nome de usuário mppb e a senha justice, as lacunas I e II devem ser corretamente preenchidas por

A) expdp e commit.

B) flyway e migrate.

C) flyway e commit.

D) swagger e migrate.

E) deploy e and commit.

Comentários:

Essa questão busca conhecimento sobre uma ferramenta de gerenciamento de migrações de banco de dados, mantendo a consistência dos esquemas em várias instâncias. Há características da ferramenta Flyway. Logo, podemos excluir algumas alternativas já. Porém, vamos analisar cada alternativa a seguir:

A) “expdp” referencia a ferramenta Oracle Data Pump Export, não a ferramenta Flyway. Assim como “commit” não seria um subcomando da ferramenta de migração. Alternativa incorreta.

B) Flyway é o nome correto da ferramenta de gerenciamento de migrações de banco de dados, gerenciando o versionamento e mantendo a consistência. O subcomando “migrate” ao final está correto, buscando aplicar todas as migrações disponíveis que ainda não foram executadas no banco de dados. Portanto, temos aqui a nossa alternativa correta.

C) Flyway é o nome correto da ferramenta de gerenciamento de migrações de banco de dados, gerenciando o versionamento e mantendo a consistência. Porém, está incorreto o uso de “commit” nessa etapa. “Commit” não é um subcomando da ferramenta Flyway. Alternativa incorreta.

D) Swagger é usado para documentação de APIs REST, não sendo relacionada a gerenciamento de migrações de banco de dados. Portanto, alternativa incorreta.

E) Deploy não é uma ferramenta de gerenciamento de migrações de banco de dados, assim como “and commit” não seria um subcomando dessa ferramenta. Alternativa incorreta.

Gabarito: B

33. (FCC - MPE PB - 2023) Uma analista está trabalhando em ambiente Linux (Ubuntu), funcionando em condições ideais, e deseja conectar-se ao banco de dados PostgreSQL, bem como verificar a versão instalada. Para isso deve utilizar o(s) comando(s):

A) sudo -su postgres psql

SHOW postgre_version()

B) sudo -u postgres psql -c "SELECT version();"

C) sudo -su postgresql

SELECT version()

D) sudo -su postgresql -exec "SHOW version();"

E) sudo -u postgres

psql –-postgre_version();

Comentários:

Vamos lá, pessoal! Essa questão exige conhecimentos sobre temas como Linux e PostgreSQL. Em sistemas Linux como Ubuntu, há a possibilidade de chamar o usuário padrão responsável pelo PostgreSQL e executar comandos SQL diretamente da linha de comando. Para isso, geralmente esse usuário é chamado de postgres (e não postgresql). A questão busca um comando para conectar-se ao banco de dados bem como verificar a versão instalada. Sendo assim, vamos analisar as alternativas a seguir.

A) **ALTERNATIVA INCORRETA.** Há um erro de sintaxe do comando inicial, não sendo "sudo -su", mas sim "sudo -u", uma vez que o comando é sudo -u postgres, para indicar que o usuário (-u) postgres será chamado. Também há erro no comando SHOW postgre_version( ), por não existir.

B) "sudo -u postgres" executa o comando como o usuário "postgres". Até aqui está correto o comando, uma vez que chama corretamente o usuário e utiliza seu nome corretamente. Há a escrita correta da função psql que permite comandos SQL diretamente da linha de comando. Há o parâmetro "-c" utilizado corretamente, o qual vem de "command" e diz ao psql para executar o comando entre aspas a seguir e encerrar. Posteriormente, vem o comando entre aspas de maneira correta, "SELECT version( );" para saber a versão do PostgreSQL instalada. **ALTERNATIVA TOTALMENTE CORRETA!**

C) Há um erro por usar "sudo -su", quando o correto seria "sudo -u", para indicar o usuário a ser utilizado. Outro erro é chamar o usuário "postgresql", quando o correto seria "postgres". Ainda, SELECT version( ) está fora de qualquer comando psql (deveria ser psql -c "SELECT version();", como vimos acima), não funcionando também. Portanto, **ALTERNATIVA INCORRETA**.

D) Novamente "sudo -su" de maneira incorreta, quando deveria ser "sudo -u", para indicar o usuário que executará o comando a seguir. O nome do usuário "postgresql" está errado também, quando deveria ser "postgres". Não há o parâmetro -exec antes do comando. **ALTERNATIVA INCORRETA**.

E) O comando apresentado nessa alternativa começa correto: temos "sudo -u" e chama o usuário "postgres" corretamente. Há o comando psql correto também, para chamar funções SQL diretamente da linha de comando. Porém, está ausente o parâmetro -c para chamar comandos psql diretamente da linha de comando, e o comando SQL "--postgre_version( )" não existe. Portanto, **ALTERNATIVA INCORRETA**.

Gabarito: B

34. (FCC - MPE PB - 2023) Um analista utilizou o comando Create Role na administração do banco de dados PostgreSQL 14. Dentre outras, são opções desse comando:

A) INROLE, SYSDB, INGROUP e COMMIT.

B) DESPITE, GET ROLE, INGROUP e SYSDB.

C) NOLOGON, UNTIL VALIDATE, CREATEDBA e NOCREATEID.

D) INHERIT, IN ROLE, IN GROUP e SYSID.

E) INGROUP, INHERIT, PERMIT e XCUTEDB.

Comentários:

No PostgreSQL, o comando CREATE ROLE é usado para criar novos papéis (roles). Dentre as opções fornecidas, as opções comumente utilizadas nesse contexto são:

- INHERIT: Permite que o novo papel herde as permissões do papel pai.
- IN ROLE: Permite especificar papéis aos quais o novo papel será associado.
- IN GROUP: Também relacionado à associação do papel a grupos.

Portanto, a opção correta seria D: INHERIT, IN ROLE, IN GROUP e SYSID.

Gabarito: D

35. (FCC - MPE PB - 2023) No PostgreSQL 14, as funções de controle de recuperação fornecem informações sobre o status atual de um servidor em espera e podem ser executadas tanto durante a recuperação quanto durante o funcionamento normal. É uma função de controle de recuperação:

A) pg_current_wal_flush_lsn ().

B) pg_last_wal_receive_lsn ().

C) pg_reload_conf ().

D) pg_export_snapshot ().

E) pg_is_in_recovery.extension ().

Comentários:

A função correta de controle de recuperação no PostgreSQL 14 é: b) pg_last_wal_receive_lsn().

Essa função retorna o número de sequência do log de gravação (LSN) do ponto até o qual a última mensagem WAL foi recebida pelo servidor.

Analisando as demais alternativas, temos:

A) Não é uma função utilizada no controle de recuperação.

C) Não é uma função utilizada no controle de recuperação, mas para recarregar os arquivos de configuração.

D) Não é uma função utilizada no controle de recuperação, mas para exportar um snapshot de uma transação.

E) Questão mais próxima da correta, porém errada também. Há erro de sintaxe, além de que a função retornaria se o servidor está em modo de recuperação, mas não forneceria informações mais detalhadas para um real controle de recuperação. Isso caso estivesse com a sintaxe correta.

Gabarito: B

36. (FCC - MPE PB - 2023) Um analista deseja executar um procedimento previamente armazenado em um banco de dados, quando da ocorrência de um evento SQL do tipo delete. Essa execução está corretamente relacionada ao conceito de

A) Broker.

B) Instanciação.

C) Trigger.

D) Generalização.

E) Docker.

Comentários:

A execução de um procedimento armazenado em um banco de dados quando ocorre um evento SQL do tipo DELETE está corretamente relacionada ao conceito de trigger.

- Uma trigger (ou gatilho) é um conjunto de instruções associadas a uma tabela em um banco de dados, que é acionado automaticamente quando ocorre um evento específico, como uma operação DELETE.

- No contexto da pergunta, a trigger pode ser configurada para executar um procedimento armazenado quando um DELETE é realizado em uma determinada tabela. Isso permite que ações específicas sejam tomadas automaticamente em resposta a determinados eventos no banco de dados.

Gabarito: C

37. (FCC - MPE PB - 2023) No âmbito da segurança da informação em bancos de dados, as dimensões privacidade de comunicação, armazenamento seguro de dados sensíveis, autenticação de usuários e controle de acesso granular são pertinentes ao aspecto

A) confidencialidade.

B) rastreabilidade.

C) integridade.

D) permissibilidade.

E) disponibilidade.

Comentários:

As dimensões citadas no enunciado, como privacidade de comunicação, autenticação de usuários, controle de acesso e armazenamento seguro de dados sensíveis, estão todas relacionadas ao conceito de "acesso à informação" na busca por manter a privacidade da informação, garantindo que apenas pessoas autorizadas tenham acesso à informação. Assim, esses conceitos estão ligados ao aspecto da confidencialidade.

Agora, vamos analisar todas alternativas.

A) Aqui temos a nossa alternativa correta conforme explicado acima.

B) A rastreabilidade é um aspecto mais ligado à auditoria, logs e trilhas de auditoria. Não está relacionada à privacidade e ao controle de acesso conforme descrito no enunciado. Alternativa incorreta.

C) A integridade busca garantir que os dados não sejam alterados indevidamente, mas não está diretamente relacionada à privacidade e ao controle de acesso. Alternativa incorreta.

D) A permissibilidade não é um aspecto ou pilar da segurança da informação. Alternativa incorreta.

E) A disponibilidade busca garantir que os dados estejam disponíveis sempre que for necessário, porém, não está relacionado à privacidade e ao controle de acesso. Alternativa incorreta.

Gabarito: A

38. (FCC - MPE PB - 2023) Considere a prática de tuning no PostgreSQL 14. Na criação do banco de dados e especialmente na criação das consultas, é muito importante atentar para um bom planejamento, normalização e consultas otimizadas. Para tanto, é importante e adequada a orientação obtida com o uso do recurso combinado

A) SELECT DISTINCT.

B) EXPLAIN ANALYZE.

C) ANALYZE WHEN.

D) ORDER BY INDEX.

E) EXPLAIN AVERAGE.

Comentários:

A prática de tuning no PostgreSQL 14 envolve o uso do recurso combinado EXPLAIN ANALYZE. A instrução EXPLAIN ANALYZE é utilizada para analisar e otimizar consultas, fornecendo informações detalhadas sobre o plano de execução e o tempo de execução real. Isso ajuda na identificação de gargalos e no ajuste do desempenho das consultas. Portanto, a opção correta é a letra B.

Analisando as demais alternativas, temos:

A) DISTINCT elimina duplicatas, mas não é uma prática de tunning, além de não trazer uma orientação conforme solicitado pelo enunciado. Alternativa incorreta.

B) Alternativa correta, conforme explicado acima.

C) Erro de sintaxe. Não há a combinação de ANALYZE e WHEN. Alternativa incorreta.

D) Comando inexistente. Há o comando ORDER BY, porém, sem o INDEX. Alternativa incorreta.

E) Comando inexistente. Não existe a combinação de EXPLAIN e AVERAGE. Alternativa incorreta.

Gabarito: B

39. (FCC - MPE PB - 2023) Considere, por exemplo, que contadora seja um usuário e conta seja uma tabela. No PostgreSQL 14, a remoção do privilégio para atualizar conta dado à contadora é feita com o comando

A) REVOKE ACCESS TO conta ON contadora;

B) REVOKE UPDATE ON conta FROM contadora;

C) DELETE PREVILEGES ON conta TO contadora;

D) DELETE UPDATE TO conta FROM contadora;

E) e) GRANT REVOKE TO conta UPDATE TO contadora;

Comentários:

Vamos lá, pessoal! A questão aborda temas relacionados a controle de acesso e privilégios em banco de dados, assim como a linguagem SQL. Vamos analisar cada alternativa a seguir:

A) O comando REVOKE está correto para realizar a remoção de um privilégio, entretanto, a sua sintaxe está errada. Os privilégios válidos para serem removidos com REVOKE são SELECT, INSERT, UPDATE, DELETE, entre outros. Não há ACCESS como privilégio SQL. Assim como há um erro de sintaxe pois a cláusula correta do REVOKE é ON <objeto> FROM <usuário>. Alternativa incorreta.

B) O comando REVOKE está correto. O enunciado pede a remoção do privilégio para atualizar, logo está correto usar REVOKE UPDATE no comando. Além disso, o restante da cláusula está corretamente informado, ON conta FROM contadora. O comando está inteiramente correto: REVOKE UPDATE ON conta FROM contador. Temos aqui a nossa alternativa correta.

C) A remoção de privilégios não é feita com o comando DELETE. Ainda, há um erro de ortografia em "PREVILEGES", quando o correto seria PRIVILEGES (Porém, não seria usado esse termo nesse comando). Alternativa incorreta.

D) A remoção de privilégios não é feita como comando DELETE. DELETE é usado para a exclusão de linhas de tabelas, não de privilégios. Alternativa incorreta.

E) A alternativa fez uma mistura com os comandos de controle de privilégios. GRANT e REVOKE são comandos distintos e não são usados juntos. GRANT adiciona privilégios, quando REVOKE remove. Alternativa incorreta.

Gabarito: B

40. (FCC - MPE PB - 2023) No PostgreSQL 14, um novo proprietário chamado novoprop pode ser atribuído à tabela tabela1 com o comando

A) GRANT TABLE tabela1 OWNER ON novoprop;

B) UPDATE TABLE FOR tabela1 OWNER TO novoprop;

C) ALTER TABLE tabela1 NEWOWNER novoprop;

D) GRANT TABLE tabela1 NEWOWNER novoprop;

E) ALTER TABLE tabela1 OWNER TO novoprop;

Comentários:

A questão aborda conhecimentos da linguagem SQL no PostgreSQL 14 para alterar o proprietário de uma tabela em um banco de dados. Vamos analisar cada alternativa a seguir:

A) O comando GRANT é utilizado para a atribuição de permissões de uso/privilégios, não para alterar as propriedades de uma tabela. Alternativa incorreta.

B) O comando UPDATE é utilizado para alterar/atualizar os dados de uma linha da tabela, não sua estrutura, nem suas propriedades. Alternativa incorreta.

C) O comando ALTER TABLE é utilizado para alterar propriedades de uma tabela, logo, está correto utilizarmos nesse caso. Logo após, é informado "tabela1" como a tabela em que queremos alterar algo, correto também. Depois temos o uso de NEWOWNER que não é uma palavra reconhecida na linguagem SQL. Portanto, comando incorreto.

D) O comando GRANT é utilizado para atribuição de permissões de uso/privilégios, não para alterar as propriedades de uma tabela. Alternativa incorreta.

E) O comando ALTER TABLE foi utilizado corretamente, e temos a indicação da tabela1 como a tabela a ser alterada. Logo, após temos OWNER TO que especifica a transferência de propriedade, seguido de "novoprop" que traz a indicação do novo proprietário da tabela. Portanto, temos aqui o nosso comando correto.

Gabarito: E

41. (FCC - MPE PB - 2023) Um analista necessitou atualizar o salário (salario_emp) do empregado de nome Claude Manaru (nome_emp) para 100, na tabela Empregado. No PostgreSQL 14 ele escreveu corretamente a expressão

A) GET Empregado SET salario_emp BY 100 WHERE nome_emp = 'Claude Manaru';

B) UPDATE Empregado SET salario_emp = 100 WHERE nome_emp = 'Claude Manaru';

C) UPDATE Empregado WHERE nome_emp = 'Claude Manaru' ON salario_emp = 100;

D) SET Empregado ALTER salario_emp = 100 WHERE nome_emp = 'Claude Manaru';

E) CHANGE Empregado WHERE nome_emp = 'Claude Manaru' ON salario_emp = 100;

Comentários:

A expressão correta para atualizar o salário (salario_emp) do empregado de nome Claude Manaru para 100 na tabela Empregado no PostgreSQL 14 é:

B) UPDATE Empregado SET salario_emp = 100 WHERE nome_emp = 'Claude Manaru';

Explicação:

A instrução UPDATE é usada para modificar os registros existentes em uma tabela.

Em seguida, especificamos a tabela que queremos atualizar (Empregado).

A cláusula SET define os campos que serão atualizados, neste caso, salario_emp é definido como 100.

A cláusula WHERE filtra os registros que devem ser atualizados, nesse caso, onde o nome do empregado é Claude Manaru.

Gabarito: B

42. (FCC - TRT 18 - 2023) Considerando um banco de dados Oracle 19 aberto e funcionando em condições ideais, uma Analista foi solicitada a remover o tablespace tbs_trt18a, eliminando todas as restrições de integridade referencial que se referem às chaves primárias e únicas dentro de tbs_trt18a. Tendo os privilégios para tal ação, ela utilizou o comando:

A) DROP TABLESPACE tbs_trt18a REMOVING CONSTRAINTS KEEPING CONTENTS AND DATAFILES;

B) DELETE TABLESPACE tbs_trt18a INCLUDING CONTENTS AND CONSTRAINTS;

C) DROP TABLESPACE tbs_trt18a WITH CONTENTS AND CONSTRAINTS ON CASCADE;

D) DROP TABLESPACE tbs_trt18a INCLUDING CONTENTS CASCADE CONSTRAINTS;

E) DELETE TABLESPACE tbs_trt18a ADDING CONTENTS ON CASCADE CONSTRAINTS;

Comentários:

O comando correto para remover um tablespace no Oracle, incluindo todas as restrições de integridade referencial associadas a ele, é DROP TABLESPACE tbs_trt18a INCLUDING CONTENTS CASCADE CONSTRAINTS;

DROP TABLESPACE é o comando para remover um tablespace.

INCLUDING CONTENTS indica que o conteúdo do tablespace (ou seja, as tabelas e outros objetos) deve ser removido.

CASCADE CONSTRAINTS especifica que as restrições de integridade referencial associadas a tabelas no tablespace também devem ser removidas.

Portanto, a opção correta é a letra D.

Gabarito: D

43. (FCC - TRT 18 - 2023) Em um banco de dados PostgreSQL 13 aberto e funcionando em condições ideais, deseja-se criar a tabela Tab_TRT18 utilizando o comando SELECT, com o valor 1 no campo Vara, o valor Juiz1 no campo NomeJuiz e o valor vt1goiania@trt18.jus.br no campo Email. O comando correto é:

A) SELECT Vara AS 1, NomeJuiz AS 'Juiz1', Email AS 'vt1goiania@trt18.jus.br' INTO Tab_TRT18;

B) SELECT 1 AS Vara, 'Juiz1' AS NomeJuiz, 'vt1goiania@trt18.jus.br' AS Email INTO Tab_TRT18;

C) SELECT INTO Tab_TRT18 (1 AS Vara, 'Juiz1' AS NomeJuiz, 'vt1goiania@trt18.jus.br' AS Email);

D) SELECT INTO Tab_TRT18 Vara AS 1, NomeJuiz AS 'Juiz1', Email AS 'vt1goiania@trt18.jus.br';

E) SELECT VALUES (1 AS Vara, 'Juiz1' AS NomeJuiz, 'vt1goiania@trt18.jus.br' AS Email) INTO Tab_TRT18;

Comentários:

Vamos analisar cada uma das alternativas a seguir:

A) Erro de sintaxe e de lógica. Houve inversão entre "Vara" e "1" no uso de AS. Alternativa incorreta.

B) Temos aqui a nossa alternativa correta. Essa opção utiliza o comando para criar a tabela Tab_TRT18 e insere os valores específicos nas colunas correspondentes. Alternativa correta!

C) Erro de sintaxe ao colocar as colunas nomeadas entre parênteses. Alternativa incorreta.

D) Erro de sintaxe e de lógica também invertendo a ordem. Alternativa incorreta.

E) Erro de sintaxe no uso de VALUES no comando. Alternativa incorreta.

Gabarito: B

44. (FCC - TRT 18 - 2023) Considere a expressão PL/SQL de um banco de dados Oracle 19 aberto e funcionando em condições ideais:

CASE WHEN expr1 IS NOT NULL THEN expr1 ELSE expr2 END
A função equivalente a essa expressão é:

A) COALESCE(expr1, expr2)

B) CHR(expr1, expr2)

C) COMPOSE(expr1, expr2)

D) COLLATION(expr1, expr2)

E) COLLECT(expr1, expr2)

Comentários:

A questão aborda conhecimentos sobre expressão PL/SQL em banco de dados Oracle. Busca-se uma função equivalente à expressão CASE WHEN expr1 IS NOT NULL THEN expr1 ELSE expr2 END. Podemos notar que essa expressão avalia expr1. Se expr1 não for nulo, retorna expr1. Se for nulo, retorna expr2. Sendo assim, vamos analisar cada alternativa a seguir:

A) A função COALESCE retorna o primeiro valor não nulo de uma lista de expressões. Logo, é exatamente a lógica da expressão indicada no enunciado. Temos aqui a nossa alternativa correta.

B) A função CHR associa um número ao caractere que possui a mesma representação binária que aquele número. Por exemplo, para caracteres ASCII, CHR(69) retorna 'E'. Alternativa incorreta.

C) A função COMPOSE combina caracteres em uma única forma composta, por exemplo, 'a' + '~' (til) → 'ã' (a com til). Utilizada para normalização de strings. Alternativa incorreta.

D) COLLATION não é uma função válida em Oracle. Portanto, alternativa incorreta.

E) A função COLLECT agrega valores em coleções (mais precisamente, em tabelas aninhadas, isto é, temos uma coluna cujo tipo é outra tabela). Alternativa incorreta.

Gabarito: A

45. (FCC - TRT 18 - 2023) Em um banco de dados PostgreSQL 13 aberto e funcionando em condições ideais, existe uma tabela denominada TRT18_temp. Um Técnico foi solicitado a esvaziar todos os dados dessa tabela. Para isso, ele utilizou o comando

A) TRUNCATE TRT18_temp CASCADE;

B) DROP TABLE IF_EXISTS TRT18_temp;

C) DROP TABLE TRT18_temp;

D) TRUNCATE TABLE TRT18_temp;

E) EMPTY TABLE TRT18_temp;

Comentários:

Vamos analisar cada uma das alternativas a seguir:

A) Questão quase correta, porém, ainda incorreta. Houve o uso de CASCADE, o que não foi solicitado no enunciado e poderia afetar outras tabelas que possuíssem chave estrangeira para a tabela TRT18_temp. Alternativa incorreta.

B) O comando DROP TABLE remove completamente a tabela, o que não foi solicitado no enunciado. Busca-se esvaziar todos os dados dessa tabela, não excluir a tabela como um todo. Alternativa incorreta.

C) O comando DROP TABLE remove completamente a tabela, o que não foi solicitado no enunciado. Busca-se esvaziar todos os dados dessa tabela, não excluir a tabela como um todo. Alternativa incorreta.

D) Temos aqui a nossa alternativa correta. Esse comando remove todos os dados da tabela TRT18_temp, mantendo a estrutura da tabela intacta. Alternativa correta!

E) Comando inexistente. Alternativa incorreta.

Gabarito: D

46. (FCC - COPERGÁS - 2023) O comando SQL que está correto, sem erros de sintaxe, é:

A) SELECT Servicos.ServicoID, Clientes.NomeCliente FROM Servicos INNER JOIN Clientes ON Servicos.ClienteID = Clientes.ClienteID;

B) SELECT COUNT(DISTINCT Cidade) FROM TABLE Clientes;

C) SELECT * FROM Clientes WHERE Cidade IS LIKE 'Recife';

D) UPDATE Clientes TO NomeCliente = 'Maria da Silva' AND City= 'Caruaru' WHERE ClienteID IS 11234;

E) DELETE FROM Clientes WHERE NomeCliente=*.*;

Comentários:

A opção que contém um comando SQL correto, sem erros de sintaxe, é:

A) SELECT Servicos.ServicoID, Clientes.NomeCliente FROM Servicos INNER JOIN Clientes ON Servicos.ClienteID = Clientes.ClienteID;

Explicações:

A) Utiliza a cláusula INNER JOIN para realizar uma junção entre as tabelas Serviços e Clientes, usando a condição Servicos.ClienteID = Clientes.ClienteID.
Seleciona as colunas Servicos.ServicoID e Clientes.NomeCliente da junção.

B) Possui um erro de sintaxe. A função de agregação COUNT não requer a palavra-chave TABLE, e o operador * não é utilizado dessa forma em COUNT(DISTINCT Cidade).

C) Contém um erro na cláusula IS LIKE. A forma correta seria LIKE 'Recife' sem o IS.

D) Possui um erro de sintaxe na cláusula UPDATE. A correção seria UPDATE Clientes SET NomeCliente = 'Maria da Silva', City = 'Caruaru' WHERE ClienteID = 11234;.

E) Contém um erro de sintaxe. A forma correta seria DELETE FROM Clientes WHERE NomeCliente='*'.

Portanto, a opção correta é a letra A: "SELECT Servicos.ServicoID, Clientes.NomeCliente FROM Servicos INNER JOIN Clientes ON Servicos.ClienteID = Clientes.ClienteID;".

Gabarito: A

47. (FCC - COPERGÁS - 2023) Considere as seguintes medidas de segurança:

I. Centralizar o controle de acesso para todos os ativos corporativos por meio de um serviço de diretório ou provedor de SSO, onde houver suporte.

II. Usar Single-Factor Authentication (SFA) para todas as contas de acesso administrativo, em todos os ativos corporativos, sejam estes gerenciados no site local ou por meio de um provedor terceirizado, pois esta é a medida de acesso seguro mais usada atualmente nas organizações.

III. Definir e manter o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da organização para cumprir com sucesso suas funções atribuídas.

IV. Estabelecer e seguir um processo, de preferência manual, para manter o acesso aos ativos corporativos, por meio da ativação de contas antigas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário.

São medidas recomendadas e adequadas para a gestão do controle de acesso o que se afirma APENAS em

A) I e III.

B) II e IV.

C) I.

D) III e IV.

E) II.

Comentários:

Vamos analisar cada item e posteriormente veremos qual alternativa se encaixa no que se pede no enunciado.

ITEM I: CORRETO. A centralização do controle de acesso é uma prática recomendada, uma vez que facilita o gerenciamento de permissões, reduz erros e acessos indevidos e melhora a auditoria e a conformidade com políticas internas.

ITEM II: INCORRETO. SFA (*Single-Factor Authentication*) é a autenticação por um único fator. O recomendado é o uso da 2FA (Autenticação por dois fatores) ou de MFA (Autenticação por múltiplos fatores), especialmente para contas de alto valor.

ITEM III: CORRETO. É um modelo de controle de acesso baseado em funções (RBAC), altamente recomendado. Reduz privilégios excessivos, melhora as auditorias e as revisões de acesso.

ITEM IV: INCORRETO. É altamente recomendado desativar ou excluir imediatamente contas antigas ou de usuários desligados. Além de que processos manuais são mais suscetíveis a falhas, recomendando-se seguir processos automatizados de provisionamento e desprovisionamento de contas.

Sendo assim, temos que os itens I e III estão corretos. Logo, a alternativa correta é a letra A.

Gabarito: A

48. (FCC - COPERGÁS - 2023) Segundo a norma ABNT NBR ISO/IEC 27001:2013, quem deve estabelecer a política de segurança da informação, atribuir responsabilidades e autoridade para assegurar que o Sistema de Gestão da Segurança da Informação (SGSI) esteja em conformidade com os requisitos dessa norma e, ainda, relatar sobre o desempenho do sistema de gestão da segurança da informação é

A) o setor de Qualidade.

B) a área de Infraestrutura.

C) a área de Tecnologia da Informação.

D) a Alta Direção.

E) a área de Compliance.

Comentários:

A questão abrange conhecimentos da norma ABNT ISO/IEC 27001:2013 e as responsabilidades de cada área. Vamos analisar as alternativas a seguir:

A) O setor de Qualidade não é o responsável direto pela liderança do SGSI, garantindo que esse esteja em conformidade com os requisitos da norma. Pode apoiar na estruturação de processos que garantam maior qualidade nas conformidades da norma, mas não é o responsável direto. **ALTERNATIVA INCORRETA**.

B) A área de Infraestrutura está ligada à infraestrutura necessária (tecnologia física e redes) ao SGSI, mas não possui as competências que estão elencadas no enunciado da questão. **ALTERNATIVA INCORRETA**.

C) A área de Tecnologia da Informação executa e implementa as políticas, mas não possui a responsabilidade de estabelecer a política de segurança da informação, nem de atribuir responsabilidades e autoridade para assegurar que o SGSI esteja em conformidade com a norma. **ALTERNATIVA INCORRETA**.

D) A Alta Direção possui as responsabilidades elencadas: estabelecer a política de segurança da informação, assegurar que responsabilidades e autoridades estejam claramente definidas e atribuídas, garantir a conformidade do SGSI com os requisitos da norma, avaliar e reportar o desempenho do SGSI regularmente. Temos aqui a nossa **ALTERNATIVA CORRETA**.

E) A área de Compliance busca garantir a aderências a normas e leis, mas não possui as responsabilidades elencadas no enunciado da questão. **ALTERNATIVA INCORRETA**.

Gabarito: D

49. (FCC - COPERGÁS - 2023) O tipo de certificado digital com validade de um ano, utilizado para garantir sigilo à transação como, por exemplo, para criptografar um e-mail para ser acessível somente com a utilização de um certificado digital autorizado, é o certificado digital do tipo

A) A1.

B) T1.

C) S3.

D) S1.

E) A3.

Comentários:

Vamos lá, pessoal! Questão aborda temas como certificados digitais dentro de Segurança da Informação. A questão busca um tipo de certificado digital que criptografe um e-mail, tenha validade de 1 ano e garanta sigilo a essa transação. Com base nessas características, vamos analisar cada alternativa:

A) Os certificados do tipo A1 somente assinam, não criptografam. Portanto, não garantem sigilo à transação por não criptografar o e-mail. Atenderia ao quesito de ter validade de um ano, porém, não pode ser a nossa alternativa correta.

B) Certificados T são para carimbo de tempo (*timestamping*). Alternativa incorreta.

C) Os certificados S3 garantem o sigilo à transação, uma vez que também criptografam além de permitirem a assinatura. Entretanto, a validade deles é de 3 anos. Portanto, alternativa incorreta.

D) Os certificados do tipo S1, assinam e criptografam, permitindo, assim, o sigilo à transação. A sua validade é de 1 ano. Portanto, temos aqui a nossa alternativa correta.

E) Os certificados do tipo A3 apenas assinam, não criptografam. Além de que, sua validade é de 3 anos. Portanto, **ALTERNATIVA INCORRETA**.

Gabarito: D

50. (FCC - COPERGÁS - 2023) Em uma tabela chamada user de um banco de dados aberto e em condições ideais, para selecionar todos os registros que possuem nomes (campo nome) iniciados com a letra E e terminados com a letra l utiliza-se a instrução SQL SELECT * FROM user

A) LIKE = 'E*l';

B) WHERE nome = 'E%l';

C) LIKE nome CONTAINS 'E%l';

D) WHERE nome LIKE 'E*l';

E) WHERE nome LIKE 'E%l';

Comentários:

Essa questão aborda conhecimentos de consultas em banco de dados utilizando a linguagem SQL para que tenhamos como retorno todos os registros que possuem nomes iniciados pela letra E e terminados com a letra I. Vamos analisar cada alternativa a seguir:

A) Após o operador LIKE não se deve utilizar o sinal "=". A sintaxe está errada. Alternativa incorreta. Além disso, o uso do coringa * está errado, pois deveria ser %. Alternativa incorreta.

B) Erro ao utilizar o sinal "=", pois quando se utiliza o sinal "=" busca-se o valor exato, sem interpretar os curingas. Portanto, tentaria encontrar de forma literal o nome "E%l". Alternativa incorreta.

C) Erro de sintaxe, não existe esse comando em SQL. Há uma mistura de LIKE com CONTAINS o que a torna incorreta.

D) Alternativa mais próxima da correta até o momento, porém falhou no uso do curinga. O curinga correto nesse caso seria % e não *, como indicado nessa alternativa. Vale mencionar que em outros sistemas com funcionalidade de "expressões regulares", o asterisco costuma, de fato, ter o papel que o % tem no LIKE do SQL. Alternativa incorreta.

E) Temos aqui a nossa alternativa correta! Busca onde nome comece com E e termine com I, tendo qualquer quantidade de caracteres entre eles (inclusive zero). Temos o correto uso de WHERE, seguido do nome. Logo após, temos LIKE, seguido dos termos que buscamos, com o correto uso do curinga para a situação solicitada.

Gabarito: E


Estratégia
Concursos