



# SISTEMA GERENCIADOR DE BANCO DE DADOS

AULA 3

Prof. Leonel da Rocha

## CONVERSA INICIAL

Veremos como monitorar o desempenho de um SGBD e suas atividades, isso é importante para garantirmos um acesso eficaz ao servidor e seus dados. Em seguida, vamos ver como é preciso cuidar dos dados armazenados e garantir a confidencialidade deles e, também, saber como podemos garantir sua proteção de ameaças externas.

Outro ponto importante é a gestão de segurança dos dados, implementada por meio de chaves, certificados e criptografia. Vamos estudar a importância e a necessidade de disponibilizar os dados e garantir a sua integridade. Para finalizar, trataremos do assunto de auditoria, no qual veremos procedimentos para entender se tudo está conforme as regras estabelecidas em nosso sistema de gerenciador de banco de dados e os dados armazenados e controlados por ele.

## TEMA 1 – ANÁLISE DE DESEMPENHO E ATIVIDADES

O uso de SGBD cresce junto com o volume de dados e sua produção diária a partir da utilização de vários dispositivos eletrônicos e com os sistemas de informação, e com base nesse panorama, aumentam as dificuldades de gerenciamento e de desempenho dos SGBD. Existem diversos SGBD sendo utilizados em vários tipos de aplicações, e na sua grande maioria, após serem instalados, não são devidamente configurados e são utilizados com todos os seus parâmetros de configuração, tanto de segurança quanto de desempenho, com seus valores padrões, sem nenhum tipo de preocupação sobre como serão utilizados, sistema que darão suporte, o hardware onde foram instalados, memória disponível e em qual o sistema operacional estão rodando. Com toda essa situação, provavelmente o melhor desempenho do SGBD não será alcançado, pelo simples fato de que diversos parâmetros podem ser configurados e modificados.

O objetivo aqui é mostrar algumas dicas que poderão auxiliar na melhora do desempenho de um SGBD de uma forma genérica. Claro que um estudo mais profundo deve ser feito levando em consideração todas as características do ambiente no qual o software será utilizado, sistema que ele apoiará, número de usuários suportados, volume de dados, velocidade de rede, configurações do hardware no qual o software será instalado e até a experiência dos seus futuros administradores, serão parâmetros que devem ser levados em consideração para uma análise de desempenho e as devidas configurações que deverão ser implementadas.

A seguir, mostraremos quatro dicas básicas para otimizar o desempenho de um SGBD:

- **Manter a versão do SGBD atualizada**

Essa dica é bem simples, mas na maioria das instalações de um SGBD as versões estão desatualizadas. Existem muitas vantagens em manter a versão atualizada em relação à performance, a exemplo de:

- Versões mais recentes corrigem as falhas de segurança no software; e
- A última versão sempre será melhor otimizada e, consequentemente, mais rápida.

Às vezes, podemos não saber qual versão do SGBD estamos usando. Esse é um passo importante, que todo administrador deve saber como fazer. Cada SGBD tem sua maneira de verificação da versão. No MySQL, na linha de comando é necessário apenas digitar: mysql -v e a versão será mostrada.

- **Verificar se o banco de dados não contém tabelas órfãs**

Plugins e temas desinstalados do sistema podem deixar os dados sem utilização nas tabelas. Com dados nessas tabelas, que não são utilizadas, pode-se levar a um banco de dados com muitas configurações e dados desnecessários, o que poderá levar a uma lentidão nos acessos e nas consultas, dependendo da capacidade de processamento do servidor.

- **Determin quais dados o MySQL está carregando automaticamente**

Cada banco de dados possui uma ampla variedade de tabelas administrativas. Uma dessas tabelas é a wp\_options, e contém informações gerenciais do SGBD.

- **Revisões de limpeza, dados antigos: expurgo**

Conforme a data de implantação de um banco de dados vai ficando pra trás, muitos dados não utilizados vão se acumulando. Ao longo do tempo, todos esses dados podem lotar o banco de dados, pensando nisso, é uma boa prática limpar esses dados antigos sem utilidade periodicamente. Essa limpeza é conhecida como expurgo, pode acontecer com dados que não são utilizados e com dados antigos, que precisarão ser armazenados em outro banco de dados.



Créditos: Vintage Tone/Shutterstock.

## TEMA 2 – CONFIDENCIALIDADE E AMEAÇAS

A confidencialidade de um dado tem a ver com a privacidade dos usuários que acessam e se cadastram em um banco de dados. É um conceito que se relaciona às ações tomadas para garantir que informações confidenciais não sejam disponibilizadas ou caiam em mãos erradas, seja por meio de ciberataques, espionagem e outros tipos de delitos relacionados ao roubo de informações digitais.

Para que a confidencialidade funcione, medidas preventivas devem ser implementadas, como permitir o acesso dessas informações somente para usuários autorizados e com senhas fortes. Essa restrição de acesso pode ser definida por níveis. Dentro de uma organização, usuários com cargos gerenciais, por exemplo, terão acesso a todos os dados, por consequência, usuários com cargos operacionais terão acessos restritos somente a dados que não sejam confidenciais. Outra maneira é

limitar o acesso aos conteúdos, que precisam ser liberados conforme as áreas que o usuário trabalha, a exemplo de marketing, vendas, financeiro, recursos humanos, tecnologia da informação, e assim por diante.

Os dados podem ser categorizados como forma de aumentar a segurança e a confidencialidade, levando em consideração critérios específicos, como potencial de impacto nas operações da organização, caso eles vazem. E conforme o grau de confidencialidade, poderão ser adotadas medidas mais rigorosas, ou não, para a proteção das informações. Em relação a isso, é bom treinar os colaboradores que possuem acesso a esses dados mais críticos para que façam manipulações em locais seguros e com maior cuidado, e tenham maior conhecimentos sobre os riscos e que algumas ações podem facilitar o ataque a esses dados, como acesso aos dados via wi-fi público, senhas fracas, senhas compartilhadas etc.

É possível implantar sistemas de criptografia de dados, autenticação de dois fatores e verificação biométrica na infraestrutura de gerenciamento dos dados. A utilização de token é uma medida de segurança que poderá ser aplicada para garantir que somente usuários autorizados accessem os dados confidenciais do banco de dados e de outros dispositivos de armazenamento, se existirem. Lembrando que informações confidenciais não são apenas os da organização, mas de funcionários, clientes, fornecedores e outros que estejam sob sua responsabilidade. A perda ou vazamento desses dados pode acarretar prejuízos financeiros e processos judiciais contra a organização.

Agora vamos ver o que é uma ameaça e exemplos de como ela se transforma em um ataque bem-sucedido. Uma ameaça em segurança da informação pode ser definida como uma ação capaz causar danos aos dados de alguém ou algo, comprometendo sua integridade, confidencialidade, autenticidade e disponibilidade.

A seguir, podemos verificar alguns exemplos de ameaça em segurança da informação e alguns fatores que podem ser tomados para evitá-las:

**Falhas humanas:** representam uma das maiores ameaças à segurança da informação, pois têm relação direta com o comportamento dos usuários no manuseio de dados sensíveis, na displicência com itens de segurança importantes, como senhas e conexões não seguras. E na maioria das vezes são ameaças internas, ou seja, estão dentro da organização. Questões como acesso direto aos dados, com possibilidades de copiar esses dados, ou informando senhas de acesso e outras tantas situações que podem expor os dados. Para prevenir essas falhas, a contratação de profissionais de TI

especializados em segurança e a retenção deles na organização é fundamental. Além de treinamento e conscientização dos usuários. Também, implementação de políticas de senhas e assinatura digital podem ser algumas das alternativas a serem implantadas para reduzir ao máximo falhas humanas.

**Malware:** é um software malicioso que infecta os computadores, corrompendo arquivos e acessando dados sigilosos. Geralmente ele é enviado via anexos de e-mail, links suspeitos e arquivos infectados.

**Ransomware:** tipo de ataque em que usuários sequestram dados corporativos, liberando-os após pagamento de resgate.

**Spyware:** espiona computadores para coletar informações de relevância.

Existem alguns tipos de ameaça em segurança da informação, vamos ver a seguir:

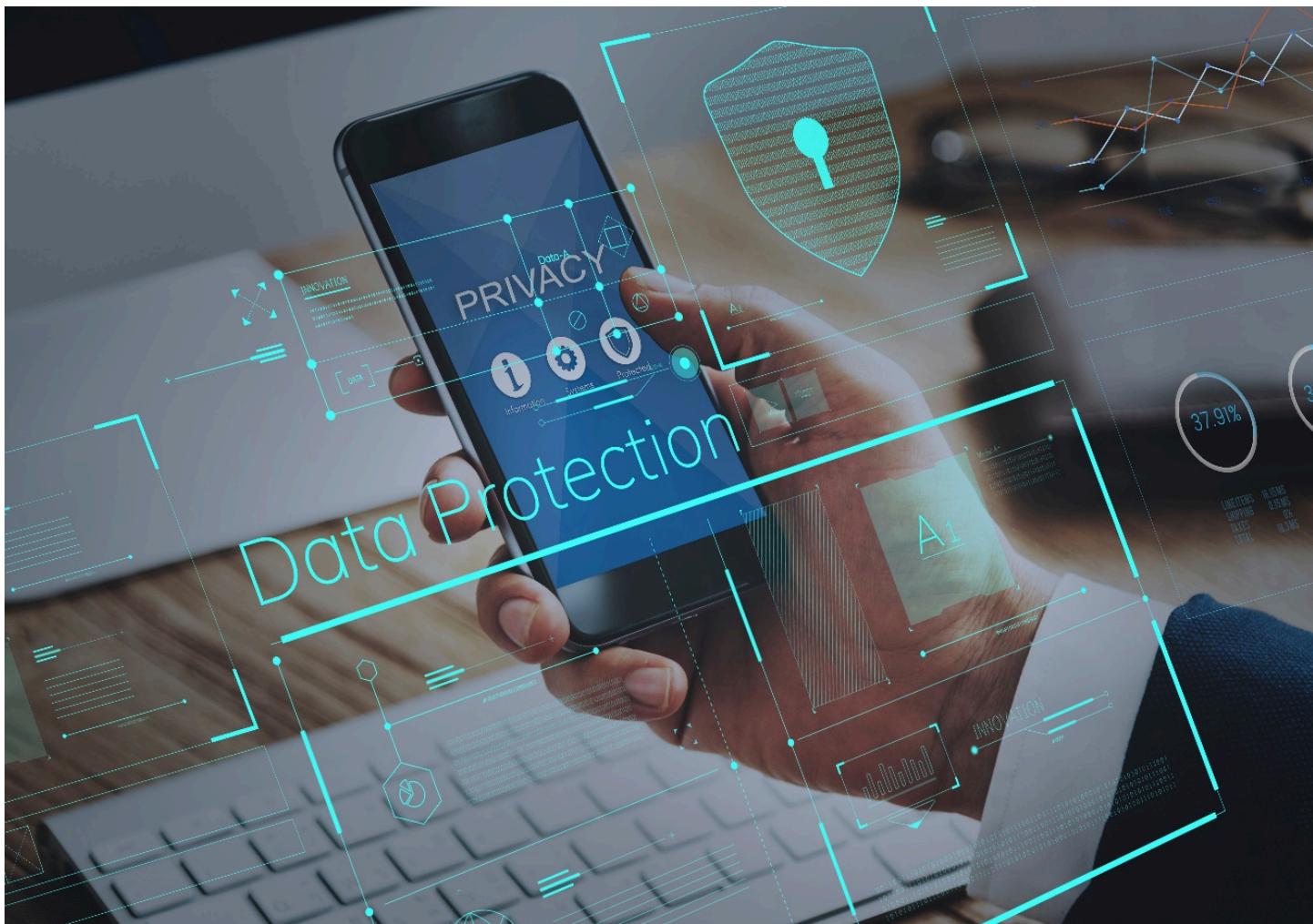
- **Ataques direcionados:** são coletadas informações específicas sobre uma organização, com técnicas de engenharia social para executar um ciberataque.
- **Ataques persistentes avançados:** ameaça com foco na espionagem on-line e essas tentativas de ataque só param quando o objetivo é alcançado.
- **Ataque DDoS (*Distributed Denial of Service*):** são enviadas múltiplas solicitações para o sistema invadido para sobrecarregá-lo e torná-lo indisponível.

Para calcular o impacto de uma ameaça à segurança da informação, deve-se levar em consideração às consequências de determinado evento que compromete a segurança dos ativos.

O cálculo do impacto é feito com a combinação dos seguintes fatores:

- Valor do ativo;
- Valor da ameaça; e
- Valor da vulnerabilidade.

Lembrando que, quanto maior for o valor do ativo, da ameaça e da vulnerabilidade, maior tende a ser o impacto.



Créditos: Rawpixel.com/Shutterstock.

## TEMA 3 – GESTÃO DE SEGURANÇA, CERTIFICADOS E CRIPTOGRAFIA

### 3.1 GESTÃO DE SEGURANÇA

Os bancos de dados são utilizados para armazenar diversos tipos de dados. A segurança do banco de dados herda as mesmas dificuldades que a segurança da informação enfrenta, que é garantir a integridade, a disponibilidade e a confidencialidade. Um SGBD deve fornecer mecanismos que auxiliem nesta tarefa.

A criação e manutenção de ambientes seguros na área de TI tornou-se preocupação comum entre administradores de redes, de sistemas operacionais e de bancos de dados. E o pior é que evidências mostram que a maioria dos ataques, roubos de informações e acessos não autorizados são feitos por usuários da organização-alvo.

Essas ameaças aos bancos de dados e seus dados resultam na perda ou degradação de alguns ou de todos os objetivos de segurança aceitos, que são: integridade, disponibilidade, confidencialidade.

A integridade do banco de dados é o requisito de que a informação seja protegida contra modificação não autorizada. A disponibilidade do banco de dados é a sua capacidade de tornar disponível os objetos a um usuário ou a um sistema ao qual eles têm um direito legítimo. A confidencialidade do banco de dados é a proteção dos dados contra a exposição não autorizada. O impacto da exposição não autorizada de informações confidenciais pode resultar em perda de confiança pública, constrangimento e ação legal contra a organização.

### 3.2 CERTIFICADOS

O certificado digital é a identidade eletrônica de uma pessoa física ou jurídica. Funciona como uma carteira de identidade virtual, permitindo assinar documentos a distância com o mesmo valor jurídico da assinatura manual no papel, sem necessidade de reconhecimento de firma em cartório.

O certificado digital comprova a identidade de uma pessoa e é praticamente inviolável, sendo aceito legalmente. O sistema utiliza um par de chaves criptografadas, que não se repete. Essas chaves são:

- **Chave privada** — criptografa os dados que atestam a identidade sobre a pessoa, tanto para acesso a um sistema quanto para assinatura de um documento eletrônico;
- **Chave pública** — é compartilhada com quem precisa decodificar a criptografia que atesta a identidade de uma pessoa. A chave pública só serve para decodificar o que foi criptografado por uma chave privada.

Para validar uma assinatura digital, o certificado vincula a ela um arquivo eletrônico com dados sobre a pessoa para atestar a quem ela pertence e que foi feita por quem pode utilizá-la legalmente. A assinatura digital e o arquivo são protegidos por criptografia pelo certificado digital, que precisa ter sido emitido, obrigatoriamente, por uma autoridade certificadora credenciada pelo Instituto Nacional de Tecnologia da Informação — ITI.

Os certificados digitais podem ser armazenados em um banco de dados como um dado normal. A maioria dos SGBD armazenam os certificados digitais em campos do tipo BLOB, que são tipos de dados que suportam um número grande de caracteres e caracteres especiais, que geralmente fazem parte dos certificados digitais. Quando do desenvolvimento de um sistema que necessite da certificação digital, ele fará acesso à tabela que armazena os dados do certificado digital para utilizá-la.

### 3.3 CRIPTOGRAFIA

Criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada de sua forma original para uma forma ilegível, de maneira que ela possa ser lida apenas por seu destinatário legítimo, tornando a mensagem difícil de ser lida por outra pessoa, que não seja autorizada. Assim sendo, só o destinatário legítimo da mensagem pode ler a informação com facilidade.



Créditos: Rawpixel.com/Shutterstock.

Provavelmente, a criptografia é um dos aspectos mais importante da segurança das comunicações e cada vez mais se torna importante como um componente básico para a segurança computacional. O uso crescente dos computadores e dos sistemas de comunicação pelas organizações aumentou o risco de roubo de informações sigilosas. Mesmo que essas ameaças necessitem de diversas contramedidas, a criptografia ainda é um dos principais métodos para

proteger informações eletrônicas valiosas. Podemos dizer que a criptografia é a ferramenta automatizada mais importante para a segurança da rede e das comunicações.

Podemos citar quatro objetivos principais da criptografia:

- **Confidencialidade da mensagem:** só o destinatário autorizado deve extrair o conteúdo da mensagem da sua forma cifrada;
- **Integridade da mensagem:** o destinatário deve ser capaz de determinar se a mensagem foi ou não alterada no momento da transmissão;
- **Autenticação do remetente:** o destinatário deve identificar o remetente e verificar que foi ele quem enviou a mensagem;
- **Não repúdio ou irretratabilidade do emissor:** não deverá ser possível ao emissor negar a autoria da mensagem enviada.

## TEMA 4 – DISPONIBILIDADE E INTEGRIDADE DOS DADOS

### 4.1 DISPONIBILIDADE DOS DADOS

Disponibilidade de dados é a garantia que os dados estarão disponíveis para usuários e sistemas no momento que eles precisarem. A disponibilidade de dados é usada, entre outras coisas, para criar contratos de nível de serviço (SLA), que definem e garantem o serviço. A disponibilidade de dados exige a implementação de serviços, regras e procedimentos que garantam que os dados estejam disponíveis em operações normais e em recuperação de desastres. A realização desse processo se dá por meio da implementação de redundância de dados e de armazenamento, segurança de dados, otimização da rede de transmissão e outros itens que garantam a comunicação e o acesso aos dados.

A indisponibilidade da informação é prejudicial para os negócios de uma organização, porque a disponibilidade da informação é um dos requisitos de compliance, que é o ato de estar em conformidade com determinadas leis, normas e regras. Um site, aplicativo ou uma plataforma fora do ar está normalmente atrelado a ineficiências de infraestrutura tecnológica ou ataques cibernéticos.



Créditos: Alfa Photo/Shutterstock.



Créditos: Metamorworks/Shutterstock.

Nesses casos, os usuários se sentem lesados e passam a confiar menos nos serviços prestados pela empresa. Além de paralisar suas atividades, principalmente dos colaboradores e usuários internos.

Como já vimos, os ataques cibernéticos podem ter o objetivo de roubar dados, manipular informações e quebrar outras barreiras de segurança. Por exemplo, acessar dados que são utilizados, como senhas, ou perguntas de segurança, para posterior recuperação de senhas.

As causas da indisponibilidade podem afetar diretamente a imagem do negócio, compliance, competitividade, trazendo prejuízos e comprometendo a imagem da empresa.



Créditos: Alexander Supertramp/Shutterstock.

## 4.2 INTEGRIDADE DOS DADOS

Quando todas as informações da empresa estão registradas em um banco de dados e, sem saber quando e quem, elas foram alteradas ou excluídas, muitos impactos podem ocorrer na empresa. É para evitar a ocorrência de problemas, que esse tipo de ação pode acarretar nos negócios, que a integridade de dados é tratada como assunto primordial dentro da segurança da informação.

A integridade dos dados é referente à confiabilidade e consistência das informações ao longo do seu ciclo de vida. Tem por objetivo preservar o dado para que nada seja comprometido ou perdido, prejudicando, assim, todo o planejamento da empresa.

A integridade dos dados, devido a sua importância, é o foco principal de várias soluções de segurança. Existem diversas ferramentas de proteção, devido a sua importância, para que o conteúdo disponibilizado em sistemas seja preservado ao máximo.



Créditos: LeoWolfert/Shutterstock.

## TEMA 5 – AUDITORIA

Os bancos de dados são essenciais para que as organizações mantenham seus dados seguros. Contudo, para garantir a qualidade do seu funcionamento, é preciso contar com uma auditoria em banco de dados.

É por meio da auditoria em um banco de dados que é possível à organização detectar e prevenir eventuais meios de invasão e garantir a segurança dos seus processos e dados, e ainda atestar sua conformidade com as leis.



Créditos: Deemerwha studio/Shutterstock.

A auditoria em banco de dados é um componente de conformidade dentro de uma organização. Diz respeito à análise e entendimento das atividades de um banco de dados, com o objetivo de obter informações sobre falhas ou inconformidades.

Em virtude do surgimento e popularização dos sistemas de informação, as organizações passaram a armazenar seus dados eletronicamente, delegando-os ao setor de Tecnologia da Informação.

Esses dados são armazenados em um conjunto estruturado, que recebe o nome de banco de dados.

Para garantir e manter a proteção desse banco de dados, contudo, a organização deve contar com a atuação da segurança da informação e seus processos. E, dentre vários outros processos, está a auditoria.



Créditos: 3rdtimeluckydataset/Shutterstock.

Uma auditoria pode ser definida como um exame ou análises sistemáticas das atividades realizadas por determinada empresa ou setor.

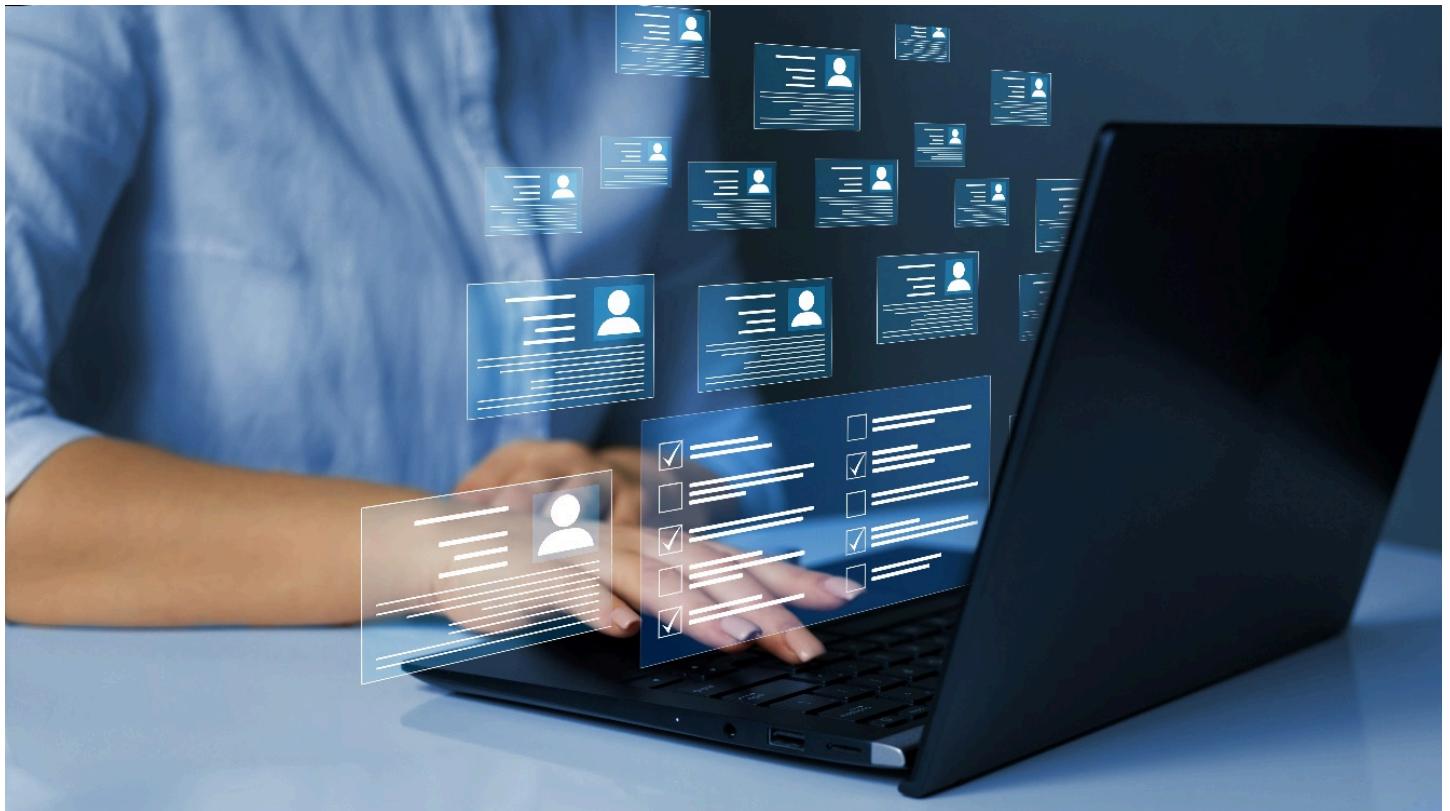
Seu objetivo é verificar se as atividades auditadas estão em conformidade com as diretrizes pré-estabelecidas pela política da empresa ou por uma legislação específica, e se a sua implementação foi realizada de maneira adequada para cumprir com seus objetivos.

No caso da auditoria de dados, essa análise é feita única e exclusivamente na base de dados de uma empresa.

Uma de suas funções é o monitoramento de quando e como um dado foi inserido em um banco de dados, com a finalidade de prevenir ou identificar possíveis problemas.

A auditoria em base de dados é responsável por definir tabelas para armazenar logs, que é o processo de registro de eventos realizados em um sistema computacional, com informações referentes à utilização das bases de dados, tais como data e hora, usuário que realizou o acesso e equipamento em que foi realizado os comandos.

Com o tempo e necessidade, é possível definir quais tabelas, colunas e linhas devem ser revisadas e analisadas.



Créditos: Miha Creative/Shutterstock.

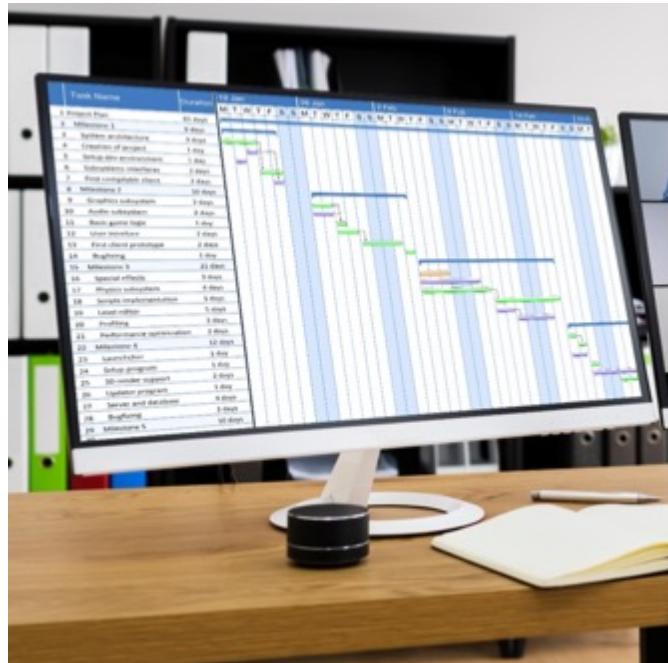
As metodologias utilizadas para a auditoria em dados são definidas de maneira única pela organização, visando atender da melhor maneira possível cada uma de suas necessidades.

A empresa optará, então, por um dos dois tipos de auditoria: a tradicional ou a exclusão de riscos.

A auditoria tradicional é realizada por meio de uma lista de conferência. Por meio dessa lista, o auditor obterá informações sobre a política de bancos de dados, como:

- Logins de acesso;
- Permissões dos usuários;
- Autorizações de acesso; e
- Direitos dos usuários.

Assim, por meio dessas informações será possível a identificação de possíveis falhas.



Créditos: Andrey\_Popov/Shutterstock.

A lista de conferência de um auditor deve abranger questões relacionadas com as atividades desenvolvidas para assegurar a segurança dos dados, isto é, uma conferência daquilo que está ou não está sendo feito.

A seguir, podemos observar alguns exemplos dessa lista de conferência para a realização de auditoria de dados:

- As atividades realizadas no banco de dados são armazenadas em log para futura análise?
- O desempenho do banco de dados é analisado constantemente?
- Há controle sobre as inserções, alterações e exclusões realizadas no banco de dados?
- As responsabilidades da administração da base de dados são devidamente definidas e documentadas?
- O SGBD é monitorado frequentemente?
- É utilizado algum dispositivo de segurança para o acesso à base de dados?
- Existem procedimentos de *backup* e *restore* no banco de dados, a fim de garantir sua segurança?
- A instalação e configuração do SGBD foi realizada em conformidade com as normas técnicas de segurança pré-estabelecidas?



Créditos: Timofeev Vladimir/Shutterstock.

Diante dessas respostas, o auditor saberá o que está sendo desenvolvido ou não pela empresa e pela área de segurança da informação, para garantir a conformidade da base de dados de acordo com suas diretrizes ou legislação.

A segunda metodologia a ser aplicada é a de exclusão de risco, que tem como característica principal a identificação dos riscos que envolvem a base de dados para que possam ser eliminados ou ao menos diminuídos.



Créditos: Photon photo/Shutterstock.

Em resumo, essa metodologia procura identificar o objetivo do controle e definir estratégias e técnicas para alcançá-lo.

Os objetivos podem ter diferentes formas de serem alcançados. As técnicas utilizadas para se chegar a um determinado objetivo podem ser preventivas ou corretivas. Para exemplificar, podemos utilizar o objetivo de confiabilidade dos dados.

As técnicas para conseguir essa confiabilidade partem do estabelecimento de perfis de tipos de usuários e quais requisitos mínimos são necessários para controlar o acesso ao banco de dados.

Com a identificação desse objetivo e a definição da estratégia que será utilizada, é realizada a verificação do funcionamento de determinada estratégia. E essa verificação é possível de ser feita por meio de provas de cumprimento.

Dependendo do resultado alcançado na prova de cumprimento, talvez seja necessária a realização de novas provas, como a prova substantiva.



Créditos: adayeva Sviatlana/Shutterstock.

Qual a importância da auditoria em banco de dados? Como já dito, a auditoria é um componente de conformidade essencial dentro de uma organização.

É por meio dela que uma organização é capaz de identificar falhas em seus bancos e corrigi-las, bem como garantir a conformidade do banco de dados com as diretrizes impostas pela própria empresa e pela legislação.

Portanto, esse é um processo para detectar aquilo que possivelmente pode ser um motivo de preocupação para a organização, como suspeitas de violação e alteração de dados. O que pode significar prejuízos para a empresa.

Dessa maneira, a auditoria em banco de dados faz parte da saúde da organização, especialmente quando analisamos o cenário das organizações, em que os dados são insumos valiosos para os negócios.

E quais devem ser as atividades que precisam ser auditadas em um banco de dados? Além dos aspectos já citados, existem atividades específicas que precisam ser auditadas em um banco de

dados. A seguir, podemos verificar quais são elas:

- Acesso e autenticação dos usuários;
- Objetos do banco de dados; e
- Rede de comunicação.

A segurança de acesso precisa obrigatoriamente ser analisada pelo auditor, uma vez que por meio de um acesso fácil ao banco de dados é possível realizar alterações ou mesmo extrair informações confidenciais.

Portanto, a auditoria da segurança de dados procura auxiliar a empresa na identificação de uma possível violação dos dados antes que um incidente maior de segurança possa ocorrer.

## FINALIZANDO

Esperamos que tenham gostado de monitoramento de SGBD. Nesta discussão, foi visto como monitorar o desempenho de um SGBD e suas atividades, isso é importante para garantirmos um acesso eficaz ao servidor e seus dados. Em seguida, vimos como é preciso cuidar dos dados armazenados e garantir a confidencialidade deles e como podemos garantir sua proteção contra ameaças externas.

Outro ponto importante que foi visto foi a gestão de segurança dos dados, implementada por meio de chaves, certificados e criptografia. Estudamos a importância e a necessidade de disponibilizar os dados e garantir a sua integridade. No final, tratamos do assunto de auditoria, que são os procedimentos para entender se tudo está em conformidade com as regras estabelecidas em nosso sistema de gerenciador de banco de dados e os dados armazenados e controlados por ele.

## REFERÊNCIAS

BARRIE, H. **Dominando Firebird**: uma referência para desenvolvedores de bancos de dados. [S.I.]: Ciência Moderna, 2006.

CARNEIRO, A. P.; MOREIRA, J. L.; CASTRO, A. L. de. **Tuning**: técnicas de otimização de bancos de dados, um estudo comparativo: MySQL e PostgreSQL. Universidade Federal do Rio Grande, 2009.

LEITE, M. **Acessando bancos de dados com ferramentas RAD**. Rio de Janeiro: Brasport, 2007.

PIRES, C. E. S.; NASCIMENTO, R. O. do; SALGADO, A. C. Comparativo de desempenho de bancos de dados de código aberto. **ResearchGate**, jan. 2008.

SILBERSCHATZ, A.; KORT, H. F.; SUDARSHAM, S. **Sistemas de bancos de dados**. 5. Ed. Rio de Janeiro: Campus, 2006.