1. Destacar a importância dos SGBD’s

Ele auxilia no gerenciamento de dados estruturados para garantir fácil acesso e compartilhamento. Ele também libera você de tarefas demoradas de processamento manual, como encontrar um ponto de dados específico e compartilhá-lo com os funcionários.

Além disso, o software de gerenciamento de banco de dados garante que os dados corporativos sejam compartilhados apenas com partes interessadas internas ou externas relevantes. Isso ajuda a reduzir riscos como perda de informações ou acesso não autorizado.

Aqui estão alguns benefícios da implementação de um sistema de banco de dados em seus processos de trabalho:

Aumenta a produtividade devido a menos erros relacionados a dados

Acelera a tomada de decisões com acesso oportuno e ininterrupto aos dados

Melhora o compartilhamento e a segurança de dados, permitindo o acesso apenas a usuários autorizados

A necessidade da sua empresa por software de gerenciamento de banco de dados depende de como seus funcionários usam os dados. Por exemplo, alguns podem usá-lo para pesquisa diária (prioridade normal), enquanto outros podem usá-lo para desenvolver ferramentas de software (alta prioridade). Tenha esses cenários de uso em mente ao decidir se deseja ou não usar sistemas de gerenciamento de banco de dados.

SRIVASTAVA, S. **What Is a Database Management System? And Why You Need One**. Disponível em: <https://www.capterra.com/resources/database-management-system/>. Acesso em: 25 ago. 2023.

1. Sua segurança

Os bancos de dados atuais podem dificilmente resolver os problemas com duplicação de dados, inconsistência e dependências de aplicativos de dados desaparecendo.  
Por outro lado, ameaças de segurança mais perigosas podem aparecer. Assim, o projeto de um SGBD seguro e de alto desempenho precisa da identificação adequada dos possíveis riscos de segurança e da seleção das políticas e procedimentos certos para a neutralização de todos esses perigos.

Qualquer sistema de gerenciamento de banco de dados seguro deve atender a três requisitos fundamentais de proteção de dados: segurança, integridade e disponibilidade.

– Garantir a segurança dos dados – Isso ocorre detectando, dissuadindo ou impedindo qualquer divulgação indevida de dados. Isso é crucial em ambientes de dados altamente protegidos e confidenciais, como defesa, finanças, tecnologia de saúde.

– Garantir a integridade dos dados é detectar, dissuadir ou quaisquer alterações impróprias ou indesejáveis nos dados fornecidos. O funcionamento bem-sucedido de qualquer empresa é baseado na disponibilidade de dados precisos.

– Garantir a disponibilidade – A disponibilidade dos sistemas é outro aspecto crucial para determinar a eficácia do banco de dados. A disponibilidade adequada evitará qualquer negação indesejada dos serviços oferecidos pelo SGBD aos usuários.

**Políticas de segurança** de dados ou informações são as diretrizes fundamentais que descrevem todas as ações desejáveis e indesejáveis sobre um sistema de informação empresarial. O gerenciamento de controle de acesso lógico pertence a isso e, portanto, as políticas de segurança devem definir os princípios nos quais um DBMS protegido está alojado. Geralmente, as políticas de segurança de dados devem dar respostas satisfatórias às questões fundamentais relacionadas à segurança. As políticas de segurança podem ser divididas em dois tipos, como privilégios mínimos e máximos. Um sistema com privilégios mínimos é fechado, e aqueles com privilégios máximos são chamados de sistemas abertos.

Ao considerar o controle de acesso para segurança do banco de dados, diferentes administrações das regras de acesso devem ser determinadas com antecedência. Algumas delas são:

* Acesso descentralizado hierárquico – Nesse modelo, um autorizador distribuirá os dependentes (usuários).
* Acesso baseado em propriedade – O autor (proprietário) de um objeto específico pode determinar a quem acessar o item.
* Autorização cooperativa – O membro pode aprovar a aprovação do direito específico para os recursos do conjunto personalizado do grupo predefinido.

Mecanismos de segurança de banco de dados

Os mecanismos de segurança são externos e internos, como sugerido pelo RemoteDBA. Vamos explorar diferentes mecanismos de controle como abaixo.

Controle de fluxo

Esse modelo de mecanismo de controle regulará a distribuição, ou seja, o fluxo dos dados ou informações entre os diferentes objetos disponíveis. Por exemplo, ler dados do objeto X e gravá-los diretamente no objeto Y. As políticas para controle de fluxo precisam de uma lista personalizada de fluxos de informações úteis e as restrições dos mesmos. Essas restrições de fluxo são geralmente baseadas nas classificações dos elementos do sistema e na definição dos fluxos aceitáveis em diferentes níveis.

Controle de inferência

O objetivo do controle de inferência é erradicar o risco de qualquer divulgação indireta de dados. Por exemplo, o conjunto de dados X pode ser lido pelo usuário autorizado, que pode ser usado para determinar o conjunto de dados Y. Normalmente, existem três maneiras diferentes de divulgar dados não autorizados, como:

– Dados correlacionados – os dados X visíveis estão semanticamente relacionados aos dados Y invisíveis.

– Dados ausentes – A consulta retorna valores NULL, que mascararão os dados mais confidenciais. No entanto, isso pode denotar a existência de dados.

– Inferência estatística – para os DBs que fornecem informações estatísticas sobre as entidades nele.

As bases de dados estatísticos geralmente não permitem qualquer acesso direto aos dados subjacentes, onde os usuários podem consultar apenas informações estatísticas. Os ataques potenciais em tais sistemas de gerenciamento de banco de dados podem ser abordados através de duas abordagens diferentes, como:

– Perturbação de dados – neste, dados confiáveis são substituídos pela interpretação estatística dos mesmos.

– Controle de consulta – Como o mecanismo de controle mais utilizado, ele se baseia no número mínimo e máximo de itens relacionados à consulta dada. Isso pode garantir um melhor controle, mas o controle de consulta é mais caro e difícil na administração.

O objetivo da modelagem de segurança de banco de dados com controle de acesso é criar um modelo abstrato, conceitual e independente baseado na especificação de requisitos dada para projeção de banco de dados. Qualquer modelo de segurança desse tipo deve ser capaz de fornecer uma representação semântica que permita a descrição das propriedades estruturais e funcionais do sistema de segurança. Ele também precisa fornecer definições adequadas para os requisitos de segurança e as diretivas do sistema. Também é fato que o nível de controle de acesso que estamos decidindo descrever pode diferir amplamente com base no caso de uso.

Modelos de controle de acesso

Os modelos de segurança de banco de dados podem ser classificados com base em diferentes aspectos. Digamos, por exemplo, que você crie um modelo de segurança com base no tipo de políticas de segurança seguidas, partes já abordadas de segurança, os tipos de controle necessários e muito mais.

Dois dos modelos básicos de controle vão surgindo logo que o conceito entrou em cena. São controles discricionários e obrigatórios. O proprietário dos dados controla o acesso ao modelo de controle discricionário. Esta é adotada como a administração de autorização mais comum (baseada em propriedade, como vimos acima). Com isso, a política se torna flexível, mas difícil de controlar de uma perspectiva universal. O modelo de controle de acesso obrigatório, por outro lado, destina-se a impor uma política global baseada no controle de fluxo, como vimos acima, entre vários níveis de segurança diferentes que são atribuídos a vários objetos.

Diferentes modelos de controle de acesso são acomodados por várias novas definições de assuntos, objetos e direitos de acesso com base nos modelos de dados OO de herança e objetos compostos. Acima de tudo isso, a matriz de acesso, ideal para o modelo de relacionamento de gerenciamento de dados, também ficou, mas isso pode não estar fazendo nada com o modelo de objeto. Por exemplo, o modelo ORION pertence a esse tipo. O modelo ORION foi introduzido em 1991 por Rabitti, que impõe um controle de acesso discricionário ao considerar as características como herança, objetos versionados, objetos compostos, etc.

Ao explorar isso ainda mais, você pode encontrar quaisquer outros modelos de controle de acesso, que podem atender a diferentes objetivos com base em vários objetivos de banco de dados corporativos. Ao considerar isso, é essencial uma análise e avaliação completa de requisitos para identificar o modelo certo para você.

LARS KOUDAL. **Access Control for Database Management System Security**. Disponível em: <https://wpsecurityninja.com/understanding-access-control-in-terms-of-database-management-system-security/>. Acesso em: 26 ago. 2023.

‌

1. O que pode ocasionar as falhas de segurança.
2. Procurar os preços reais dos SGBD’s mais utilizados
3. A quantidade de registros que cada SGBD suporta em suas entidades (tabelas) e fazer um comparativo.
4. Levante questionamentos sobre qual SGBD usar para determinados clientes de pequeno, médio e grande porte.