REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

SEGURANÇA EM BANCOS DE DADOS PARA PEQUENAS E MÉDIAS EMPRESAS: DIRETRIZES MODERNAS CONTRA AMEAÇAS DIGITAIS E CONFORMIDADE REGULATÓRIA

DATABASE SECURITY FOR SMALL AND MEDIUM-SIZED ENTERPRISES: MODERN GUIDELINES AGAINST DIGITAL THREATS AND REGULATORY COMPLIANCE

Ciências Exatas e da Terra • 27/06/2026

REGISTRO DOI: 10.70773/revistatopicos/782501349

Alberto Aparecido de Almeida
Fernando Araújo Rodrigues
Harley Balduino Saraiva
Leandro dos Santos Mendes
Ricardo César de Paula Filho

RESUMO

A transformação digital expandiu de forma definitiva a utilização da tecnologia da informação para organizações de todos os portes. No cenário macroeconômico contemporâneo, os Bancos de Dados consolidaram-se como ferramentas vitais e centrais para o funcionamento estratégico de Pequenas e Médias Empresas (PMEs), atuando como ativos essenciais responsáveis por armazenar, recuperar e transformar dados brutos em informações de alto valor competitivo. No entanto, a preservação da privacidade organizacional e o tratamento seguro de registros corporativos envolvem complexas barreiras legais, éticas e políticas de mitigação de risco. Este artigo analisa os conceitos fundamentais de Sistemas Gerenciadores de Banco de Dados (SGBDs) e propõe um conjunto integrado de diretrizes práticas de segurança da informação moldadas para a realidade orçamentária e operacional das PMEs. A presente pesquisa considera o severo avanço das ameaças cibernéticas globais documentadas pelo relatório histórico de custos de violação da IBM (2025), a aplicação de ferramentas de design e administração visual como o MySQL Workbench, as recomendações técnicas emitidas pelo CERT.br e as exigências legais de conformidade impostas pela Lei Geral de Proteção de Dados (LGPD). A metodologia adotada caracteriza-se como uma pesquisa bibliográfica aplicada de caráter descritivo, unindo fundamentos clássicos da ciência da computação a dados métricos atuais de controle discricionário de acesso, técnicas de criptografia em trânsito e planos resilientes de continuidade de negócios.

Palavras-chave: Banco de Dados; Segurança da Informação; PMEs; Custos de Violação; IBM (2025); LGPD.

ABSTRACT

Digital transformation has definitively expanded the use of

information technology across organizations of all sizes. In the contemporary macroeconomic scenario, Databases have consolidated as vital and central tools for the strategic operation of Small and Medium Enterprises (SMEs), serving as essential assets responsible for storing, retrieving, and transforming raw data into high-value competitive intelligence. However, preserving organizational privacy and securely handling corporate records involve complex legal, ethical, and risk mitigation barriers. This paper analyzes the fundamental concepts of Database Management Systems (DBMS) and proposes an integrated set of practical information security guidelines tailored to the budgetary and operational realities of SMEs. This research takes into account the severe escalation of global cyber threats documented by the IBM Cost of a Data Breach Report (2025), the application of visual design and administration tools such as MySQL Workbench, technical recommendations issued by CERT.br, and statutory compliance requirements imposed by the General Data Protection Law (LGPD). The adopted methodology is characterized as an applied descriptive literature review, bridging classic computer science foundations with current metrics on discretionary access control, in-transit encryption techniques, and resilient business continuity plans.
Keywords: Database; Information Security; SMEs; Data Breach Costs; IBM (2025); LGPD.

1. INTRODUÇÃO

A informação consolidou-se como um dos principais meios de produção, insumos estratégicos e produtos finais do mercado corporativo moderno, demandando mecanismos altamente eficazes de armazenamento, integridade e proteção para uso subsequente. Paradoxalmente, a crescente dependência tecnológica que as

organizações manifestam deparar-se-á, com acentuada frequência, com a vulnerabilidade sistêmica e a insegurança latente dessas bases de dados. Fatores operacionais internos e vetores de ameaças externos contribuem continuamente para que dados corporativos sigilosos fiquem expostos a acessos desautorizados ou manipulações maliciosas.

Embora o ecossistema global de tecnologia da informação apresente uma expansão econômica contínua, em uma parcela expressiva das Pequenas e Médias Empresas (PMEs) a cultura de segurança digital estruturada ainda é incipiente. Para compreender a magnitude do problema e a vulnerabilidade financeira envolvida, torna-se mandatório analisar o panorama macroeconômico dessas organizações no cenário brasileiro através dos indicadores consolidados pelo Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE, 2026). Ao isolar os Microempreendedores Individuais (MEIs) e focar a análise estritamente no ecossistema das Microempresas (MEs) e Empresas de Pequeno Porte (EPPs) — que compõem o universo formal das PMEs com infraestrutura de rede —, observa-se que esse grupo movimenta um faturamento médio mensal estimado em R$ 41 bilhões (SEBRAE, 2024). Individualmente, uma Microempresa (ME) possui o teto de faturamento fixado em até R$ 360 mil anuais, enquanto uma Empresa de Pequeno Porte (EPP) pode faturar de R$ 360 mil até R$ 4,8 milhões por ano (SEBRAE, 2026). A contradição reside no fato de que, embora respondam por cerca de 97% das empresas ativas no país e centralizem o fluxo de Informações de Identificação Pessoal (PII) de milhões de consumidores, a capacidade de investimento dessas organizações em defesas digitais é inversamente proporcional à sua importância econômica. Esse estrangulamento orçamentário delineia o núcleo do problema de pesquisa: como proteger esse volume massivo de

faturamento e dados operacionais diante de ameaças cujos custos de reparação superam a própria capacidade de sobrevivência financeira da empresa?

A escassez crônica de recursos orçamentários dedicados à infraestrutura de TI e a ausência de pessoal especializado de engenharia de dados nessas organizações frequentemente resultam em desastres sistêmicos, sequestros de arquivos e incidentes de segurança de proporções financeiras irreparáveis. Conforme documentado amplamente pela IBM (2025) em suas pesquisas históricas de duas décadas sobre segurança de dados, a introdução acelerada de inovações de software sem a devida governança tem gerado lacunas críticas de supervisão, deixando os ecossistemas empresariais severamente vulneráveis a infiltrações silenciosas.

Diante desse cenário de vulnerabilidade estrutural, consolida-se o problema central desta pesquisa: *Como as PMEs podem preservar as suas informações armazenadas de forma que fiquem protegidas contra incidentes e disponíveis exclusivamente para seus proprietários e usuários autorizados?*

O objetivo geral deste trabalho é apresentar conceitos fundamentais e ferramentas gratuitas viáveis para a implementação imediata de um ambiente de segurança robusto em bancos de dados de PMEs. Especificamente, busca-se validar, por meio de revisão bibliográfica exaustiva e análise de relatórios de risco corporativos globais, os métodos aplicáveis de controle discricionário de acesso, isolamento de tráfego de rede e governança da informação voltados a mitigar os severos impactos financeiros e as sanções jurídicas geradas por incidentes cibernéticos contemporâneos.

2. REFERENCIAL TEÓRICO

2.1. Conceituação de Sistemas de Banco de Dados

Um banco de dados caracteriza-se formalmente como um sistema de armazenamento computadorizado que oferece uma coleção de dados logicamente relacionados, interligados e estruturados, organizados de forma a reduzir drasticamente a redundância operacional e facilitar a manipulação automatizada. Conforme apontam as definições consagradas pela literatura clássica da área:

O banco de dados é um grupo de arquivos relacionados, estruturado para parecer estar em um só local, permitindo o acesso e a utilização por múltiplas aplicações concomitantes (LAUDON; LAUDON, 1997).

Fisicamente, este ecossistema compreende arquivos alocados em dispositivos de armazenamento periféricos destinados à constante consulta, indexação e atualização dinâmica pelos usuários (MEDEIROS, 2006). Em estruturas relacionais tradicionais, as informações são distribuídas de forma analítica em tabelas compostas por colunas (atributos) e linhas (tuplas), onde os registros de fato residem e são operados por meio de linguagens de consulta estruturada (SQL).

No ambiente corporativo, a gestão, manutenção e salvaguarda dessas estruturas envolvem diferentes papéis técnicos de extrema relevância, conforme categorizado por Elmasri e Navathe (2002):

- **Administrador de Banco de Dados (DBA):** Autoridade central e máxima responsável por gerenciar o sistema operacionalmente, autorizar o controle de acesso, monitorar a

performance do servidor e aplicar rigidamente as políticas de segurança.

- **Projetistas:** Profissionais encarregados de identificar os dados a serem armazenados, estabelecer os relacionamentos lógicos e definir a estrutura ideal do esquema antes de sua efetiva implementação física.

- **Usuários Finais:** Indivíduos que interagem com o sistema de forma diária por meio de aplicações para a execução de tarefas operacionais que exigem consultas, inserções, atualizações e geração de relatórios de negócios.

2.2. Níveis de Abstração de Dados e Ferramentas de Design Visual

O design e a arquitetura de um banco de dados são subdivididos na ciência da computação em três modelos e níveis fundamentais de abstração, evoluindo progressivamente do nível conceitual ao físico: o modelo conceitual (independente de SGBD), o modelo lógico (estruturação de tabelas e chaves) e o modelo físico (implementação em disco). Na rotina operacional das PMEs, a transição e tradução entre esses níveis de abstração complexos são otimizadas por ambientes de desenvolvimento integrado e consoles de gerenciamento visual.

Nesse contexto, destaca-se de forma expressiva o **MySQL Workbench,** uma aplicação visual unificada que integra nativamente a modelagem de dados, o desenvolvimento de consultas SQL abrangentes e a administração centralizada de servidores MySQL (ORACLE, 2026). A ferramenta possibilita ao projetista desenhar esquemas de tabelas de forma inteiramente

gráfica (Diagramas Entidade-Relacionamento) e gerar os scripts físicos de forma automatizada (*Forward Engineering*), diminuindo erros humanos de sintaxe que possam expor a estrutura do banco de dados a vulnerabilidades de injeção de código ou falhas lógicas.

2.3. Mecanismos Tradicionais de Segurança em SGBDs e a Regra de Anderson

Em sistemas multiusuários, a segurança envolve diretamente a capacidade técnica do SGBD de fornecer mecanismos restritivos para que indivíduos ou grupos visualizem apenas frações selecionadas da base de dados, preservando campos estritamente confidenciais. A literatura especializada classifica os mecanismos nativos de segurança do SGBD em duas grandes frentes (ELMASRI; NAVATHE, 2002):

Os **Mecanismos Flexíveis de Segurança** são focados no controle discricionário de acesso (DAC — *Discretionary Access Control*). Operam concedendo ou revogando privilégios específicos (operações de leitura, inserção, exclusão ou modificação estrutural) diretamente sobre arquivos, visões (*views*), tabelas ou campos a determinados usuários e papéis organizacionais. Por outro lado, os **Mecanismos Obrigatórios de Segurança** são utilizados para impor segurança multinível (MAC — *Mandatory Access Control*). Eles categorizam os elementos de dados e os usuários do sistema em classes hierárquicas rígidas de segurança (ex: público, confidencial, secreto), impedindo por completo que usuários acessem itens de classificação superior à de sua conta.

Ademais, os SGBDs exigem mecanismos de **Controle de Acesso** baseados na validação rigorosa de identidades (contas e senhas

lógicas) e a **Criptografia,** algoritmo matemático de codificação utilizado para proteger informações sensíveis durante a transmissão em redes de comunicação ou em repouso nos discos de armazenamento, limitando o entendimento do conteúdo apenas a portadores das chaves criptográficas adequadas.

Contudo, a aplicação prática de tais mecanismos impõe um clássico desafio operacional conhecido no campo da cibersegurança como a **Regra de Anderson.** Conforme analisa o referencial técnico corporativo da IBM (2025), a proteção de um ecossistema de banco de dados é uma tarefa complexa que confronta diretamente os pilares da segurança e da usabilidade. O axioma dita que quanto mais acessível, rápido e utilizável for um banco de dados, mais vulnerável ele se tornará a ameaças de intrusão; em contrapartida, quanto mais invulnerável e restritivo for o sistema, mais difícil, lento e complexo será o acesso legítimo por parte dos usuários da empresa (IBM, 2025). O papel fundamental da equipe de dados em PMEs consiste em equilibrar essa balança.

3. A EVOLUÇÃO DO CENÁRIO DE RISCOS E OS CUSTOS REAIS DA PERDA DE DADOS

As ameaças enfrentadas pelas organizações de pequeno e médio porte sofreram mutações drásticas nas últimas décadas. Conforme documentado ativamente pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, o ecossistema corporativo atual lida diariamente com vazamentos massivos de dados gerados por ataques persistentes e negligência nas configurações de TI (CERT.br, 2024).

3.1. Vetores de Ataque Iniciais e Causas Raiz

As vulnerabilidades que afetam as bases de dados corporativas originam-se de diferentes fraquezas de processos e de tecnologia. Dados estatísticos globais publicados pela IBM (2025) revelam que os ataques maliciosos ou criminosos — sejam eles arquitetados por agentes externos ou por ameaças internas (*insider threats*) — continuam dominando as estatísticas macros, representando 51% de todas as causas raiz de violações de dados no mercado. O erro humano e as falhas nativas de infraestrutura de TI completam os índices de incidentes de segurança.

Entre os principais vetores de ataque utilizados por cibercriminosos para obter o acesso inicial ilícito a servidores de bancos de dados, destacam-se três categorias críticas mapeadas em ambientes corporativos (IBM, 2025):

Tabela 1. Principais Vetores de Ataque Inicial e Ciclo de Vida do Incidente

Vetor de Ataque Inicial	Frequência Estatística	Tempo Médio de Identificação (MTTI)	Tempo Médio de Contenção (MTTC)
Campanhas de Phishing	Alta (Causa Raiz Comum)	192 dias	62 dias
Credenciais Comprometidas	51% (Agrupado com Maliciosos)	186 dias	60 dias
Exploração de Vulnerabilidades	Expressiva	180 dias	65 dias

Os dados apresentados na Tabela 1 expõem um panorama alarmante para PMEs: o ciclo de vida total de uma violação (a soma

do MTTI e do MTTC) ultrapassa frequentemente a marca de 240 dias (IBM, 2025). Durante este longo período em que a invasão permanece oculta, os criminosos realizam movimentos laterais na rede, coletam privilégios elevados e realizam a exfiltração silenciosa de tabelas inteiras contendo informações confidenciais de clientes.

3.2. Ransomware e a Interrupção Crítica de Negócios

O *ransomware* consolidou-se como o ataque cibernético de maior impacto financeiro direto para PMEs. Conforme a Cartilha do CERT.br (2023), este código malicioso sequestra a infraestrutura tecnológica ao aplicar algoritmos fortes de criptografia sobre os arquivos de dados e binários do SGBD, paralisando por completo os serviços lógicos. O restabelecimento do acesso legítimo é condicionado pelos criminosos ao pagamento de resgates em criptoativos.

Para além do custo da extorsão, a IBM (2025) aponta que o verdadeiro prejuízo financeiro reside na interrupção nos negócios. PMEs afetadas por desastres ou ataques de *ransomware* sofrem com a perda direta de receitas por inatividade, custos elevados com perícia forense digital para descobrir a origem da quebra de segurança, despesas legais e notificações obrigatórias a clientes afetados, e um severo desgaste reputacional que provoca a migração de consumidores para concorrentes diretos.

3.3. Impacto Legal e Sanções Regulatórias: A LGPD no Brasil

A conformidade com legislações de proteção à privacidade de dados pessoais tornou-se mandatória no Brasil com a vigência plena da Lei Geral de Proteção de Dados (LGPD — Lei nº 13.709/2018). Sob o escopo desta lei, toda e qualquer empresa, independentemente de

seu porte econômico ou volume de faturamento, que armazene e trate dados de identificação pessoal (PII) é considerada controladora ou operadora de dados e responde civil e administrativamente por qualquer incidente de segurança. Complementarmente, a literatura jurídica destaca que a proteção de dados pessoais exige um dever de cuidado proativo e transparência por parte dos controladores (MENDES; DONEDA; SARLET, 2021).

O estudo analítico da IBM (2025) reforça que as multas ou penalidades por não conformidade regulatória têm aumentado globalmente, representando um componente de custo devastador para empresas que negligenciam a segurança de dados. O Fascículo de Proteção de Dados do CERT.br (2024) adverte que a adoção de posturas preventivas e controles de segurança lógicos transparentes nas bases de dados é essencial para mitigar os riscos de fiscalização e aplicação de sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD).

3.4. Assimetria Financeira: O Faturamento das PMEs Versus os Custos de Violação

A construção de um paralelo direto entre a capacidade de geração de receita das PMEs e o impacto financeiro real de um incidente cibernético revela um cenário de insustentabilidade operacional. De acordo com os dados métricos publicados no relatório global *Cost of a Data Breach* da IBM (2025), o custo médio consolidado de uma única violação de dados para empresas operando no Brasil atingiu a marca histórica de R$ 7,19 milhões. Quando essa métrica de prejuízo é confrontada de forma analítica com os tetos de faturamento estabelecidos pelo SEBRAE (2026) para o ambiente de pequenos

negócios (desconsiderando a figura do MEI), a severidade do risco é evidenciada através de uma assimetria matemática alarmante.

Para uma Empresa de Pequeno Porte (EPP) que opere no limite máximo de sua categoria, faturando R$ 4,8 milhões por ano, o custo financeiro estimado de um único vazamento ou sequestro de banco de dados (R$ 7,19 milhões) excede o seu faturamento bruto de um ano inteiro em aproximadamente 49,7%. O panorama assume contornos ainda mais devastadores ao analisar uma Microempresa (ME) situada no teto anual de R$ 360 mil: para esta organização, o impacto financeiro de uma falha de segurança mensurado pela IBM (2025) equivale a mais de 19 anos de faturamento bruto integral de suas atividades, tornando o incidente estatisticamente terminal.

Essa inviabilidade financeira decorre da composição do cálculo do prejuízo estruturado pela IBM (2025), o qual demonstra que os custos não se limitam à perda imediata de ativos tecnológicos. O montante total é impulsionado de forma crônica por quatro fatores agravantes mapeados no ecossistema corporativo: (a) a interrupção crítica dos negócios e a consequente perda de receitas por inatividade operacional; (b) os custos elevados com contratação de perícia forense digital para identificação da causa raiz; (c) despesas jurídicas com notificações obrigatórias e defesas processuais; e (d) o desgaste reputacional severo, que provoca a migração imediata de clientes para concorrentes.

Adicionalmente, o longo ciclo de vida de uma violação — que frequentemente ultrapassa a marca de 240 dias entre a infiltração inicial, identificação (MTTI) e contenção (MTTC) (IBM, 2025) — agrava o volume de dados exfiltrados dos Sistemas Gerenciadores de Banco de Dados (SGBDs). Conforme apontado pela literatura de

conformidade, ao passar mais de oito meses sob monitoramento silencioso de agentes maliciosos, as tabelas relacionais contendo dados sensíveis são inteiramente copiadas. Sob a égide da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a materialização desse volume de dados perdidos obriga a empresa controladora a responder administrativa e civilmente (MENDES; DONEDA; SARLET, 2021). Portanto, a convergência entre o faturamento limitado mapeado pelo SEBRAE e as penalidades pecuniárias da ANPD consolida a segurança de banco de dados não como um gasto opcional de infraestrutura, mas como uma estratégia mandatória de salvaguarda e continuidade de mercado.

4. DIRETRIZES MODERNAS DE SEGURANÇA PARA PMES APLICADAS VIA SGBD

Para mitigar a probabilidade de ocorrência de incidentes severos e reduzir drasticamente os custos operacionais de uma violação sem demandar investimentos financeiros proibitivos, propõe-se um conjunto integrado de diretrizes administrativas aplicáveis por meio do console unificado MySQL Workbench e boas práticas nacionais.

4.1. Gestão Centralizada de Usuários e Aplicação do Menor Privilégio

Para combater de forma direta o vetor de "credenciais comprometidas" (IBM, 2025), o administrador de dados deve exercer controle analítico sobre as contas corporativas.**A evolução das técnicas de gestão de dados reforça a necessidade de aplicar privilégios granulares em ambientes modernos (ELMASRI; NAVATHE, 2018).** O MySQL Workbench provê o módulo administrativo *Users and Privileges*, que simplifica graficamente a

execução das quatro ações básicas de gestão descritas na literatura clássica (ELMASRI, 2002):

Essa gestão fundamenta-se no Princípio do Menor Privilégio (*Principle of Least Privilege*), garantindo que cada identidade digital (seja um funcionário ou uma aplicação de software) possua estritamente os privilégios mínimos necessários para a execução de suas funções de negócio. Na prática, anula-se a cultura insegura de utilizar a conta master root para conexões diretas de aplicações de software ou consultas rotineiras.

O bloco de código abaixo exemplifica a tradução técnica dessa diretriz, isolando os escopos de rede e aplicando restrições criptográficas em nível de banco de dados:

```
================================================================-
DIRETRIZ 4.1: CRIAÇÃO DE USUÁRIOS E ISOLAMENTO DE ESCOPO DE REDE
================================================================

-- Criação do usuário para o analista de TI ou administrador local
-- O escopo '@localhost' restringe o acesso exclusivamente à máquina local
CREATE USER 'analista_ti'@'localhost'
IDENTIFIED BY 'Senha_Forte_@2026_T1#';
-- Criação do usuário utilizado exclusivamente pela aplicação Web (ERP/Vendas)
-- O escopo '@192.168.1.50' garante que o SGBD rejeite conexões vindas
```

-- de qualquer outro IP que não seja o do servidor de aplicação dedicado
CREATE USER 'app_vendas_user'@'192.168.1.50'
IDENTIFIED BY 'App_Secure_Pass_#2026_v4!';
-- Exigência de conexões criptografadas (SSL/TLS) para o usuário da aplicação
-- Mitiga o risco de ataques de interceptação de dados em trânsito (Man-in-the-Middle)
ALTER USER 'app_vendas_user'@'192.168.1.50' REQUIRE SSL;

Na sequência, a aplicação do Controle de Acesso Discricionário (DAC) é realizada por meio da linguagem de controle de dados (DCL), segmentando o que cada conta pode manipular e banindo comandos genéricos e perigosos como GRANT ALL PRIVILEGES:

==========
==========-
DIRETRIZ 4.1.1: ATRIBUIÇÃO DE PRIVILÉGIOS DISCRICIONÁRIOS
==========
==========

-- Atribuição de privilégios restritos para a aplicação web (Apenas DML necessário)
GRANT SELECT, INSERT, UPDATE ON db_corporativo.tb_clientes TO 'app_vendas_user'@'192.168.1.50';
GRANT SELECT, INSERT, UPDATE ON db_corporativo.tb_pedidos TO 'app_vendas_user'@'192.168.1.50';
-- Restrição: A aplicação NÃO possui privilégios de deleção (DELETE) e nem
-- de modificação estrutural (DROP, ALTER), anulando o impacto de SQL Injections.

```
-- Atribuição de privilégios para o analista (Apenas consulta analítica)
GRANT SELECT ON db_corporativo.* TO 'analista_ti'@'localhost';
-- Atualização imediata dos privilégios na memória do servidor
FLUSH PRIVILEGES;
```

Para complementar a segurança de dados sensíveis e atender de forma estrita às exigências de privacidade impostas pela LGPD (MENDES; DONEDA; SARLET, 2021), o administrador não deve expor tabelas físicas nativas. O mascaramento de Informações de Identificação Pessoal (PII) é viabilizado por meio da criação de Visões (*Views*) lógicas no MySQL Workbench:

```
SQL
-
==========
-- DIRETRIZ 4.1.2: MASCARAMENTO DE DADOS VIA VISÕES (CONFORMIDADE LGPD)
--
==========

USE db_corporativo;
-- Criação de View que omite dados sensíveis (hashes de senhas, CPFs ou cartões)
-- Exibindo dados parciais e mascarados para o ecossistema de negócios
CREATE VIEW vw_pedidos_analise AS
SELECT
  p.id_pedido,
  p.data_compra,
```

```
  c.nome_cliente,
    CONCAT(SUBSTRING(c.email_cliente, 1, 4), '***@dominio.com') AS email_protegido,
  p.valor_total
FROM tb_pedidos p
INNER JOIN tb_clientes c ON p.id_cliente = c.id_cliente;
-- Concessão de privilégio de leitura unicamente sobre a View e não sobre a tabela-mãe
GRANT SELECT ON db_corporativo.vw_pedidos_analise TO 'analista_ti'@'localhost';
FLUSH PRIVILEGES;
```

4.2. Monitoramento de Performance, Auditoria e Isolamento de Rede

O MySQL Workbench integra módulos visuais de monitoramento contínuo como o *Performance Dashboard*, que exibe métricas em tempo real de conexões ativas, execução de queries e tráfego de rede (ORACLE, 2026). Deve-se utilizar estas interfaces gráficas para detectar picos anômalos de leitura e requisições SQL, que configuram fortes indicadores de tentativas de exfiltração de dados ou ataques de negação de serviço (DDoS).

Em conformidade com as diretrizes de segurança de infraestrutura emitidas pela Cartilha do CERT.br (2023), os servidores de bancos de dados das PMEs jamais devem possuir endereços de IP públicos expostos diretamente à internet. As conexões efetuadas remotamente por administradores ou filiais da empresa devem ser encapsuladas obrigatoriamente através do protocolo seguro *SSH Tunneling* configurado na aba de conexão do MySQL Workbench, ou

mediadas por Redes Virtuais Privadas (VPNs) com criptografia forçada habilitada na aba SSL da ferramenta (ORACLE, 2026).

Do ponto de vista administrativo do SGBD, o acompanhamento e a auditoria dos privilégios concedidos devem ser rotineiros, permitindo a revogação célere ou o bloqueio de contas suspeitas:

```
SQL
--
============================================================
==========
-- DIRETRIZ 4.2: ROTINAS DE AUDITORIA, REVOGAÇÃO E BLOQUEIO
DE CONTAS
--
============================================================
==========

-- Inspeção periódica dos privilégios vigentes para identificação de
desvios
SHOW GRANTS FOR 'app_vendas_user'@'192.168.1.50';
-- Revogação imediata de privilégios em caso de reestruturação de
escopo
REVOKE UPDATE ON db_corporativo.tb_clientes FROM
'app_vendas_user'@'192.168.1.50';
-- Bloqueio preventivo de conta de funcionário desligado ou sob
suspeita de invasão
ALTER USER 'analista_ti'@'localhost' ACCOUNT LOCK;
FLUSH PRIVILEGES;
```

4.3. Plano de Continuidade e Resiliência: A Regra de Backup Imutável 3-2-1

Uma vez que o risco zero é inexistente na ciência da computação, a principal salvaguarda de uma organização contra desastres físicos ou lógicos reside em sua capacidade de recuperação acelerada. O utilitário *Data Export* contido nas ferramentas de administração do MySQL Workbench possibilita a geração simplificada e a automação de dumps lógicos completos dos esquemas de dados (ORACLE, 2026).

O CERT.br (2023) enfatiza que possuir cópias de segurança confiáveis é o único método seguro de restabelecer a continuidade dos negócios diante de incidentes de ransomware sem financiar redes criminosas. Para garantir a eficácia absoluta dessa estratégia, as PMEs devem adotar estritamente a Regra de Backup 3-2-1 (CERT.br, 2024):

1. **Manter 3 cópias dos dados:** Sendo 1 cópia de produção ativa e funcional no servidor principal e pelo menos 2 cópias de segurança (backups) atualizadas diariamente;

2. **Armazenar em 2 mídias diferentes:** Utilizando tecnologias com isolamento físico distinto, por exemplo, um storage de discos rígidos (NAS) local e um bucket de armazenamento em nuvem híbrida;

3. **Garantir que 1 cópia esteja offline:** Pelo menos uma das cópias de backup deve ser armazenada em um local totalmente isolado e desconectado da rede local da empresa (backup imutável, offline ou em nuvem com extensão de retenção lógica trancada). Esse isolamento impede que um código malicioso de ransomware infecte e criptografe

simultaneamente os backups lógicos da empresa, permitindo a restauração limpa da base de dados (CERT.br, 2024).

5. CONCLUSÃO

A governança e a segurança em ambientes de bancos de dados para pequenas e médias empresas deixaram de ser um diferencial competitivo para tornarem-se um requisito crítico de sobrevivência mercadológica e conformidade jurídica. Conforme demonstrado ao longo desta pesquisa, a implementação de uma barreira defensiva robusta não está estritamente vinculada à aquisição de ferramentas proprietárias de altíssimo custo financeiro.

A proteção eficaz fundamenta-se na aplicação rigorosa e metódica de conceitos clássicos de controle discricionário de acesso e criptografia descritos na literatura de computação, instrumentalizados por meio de consoles de administração gratuitos e amplamente acessíveis, como o MySQL Workbench. Quando essas ações técnicas são alinhadas às recomendações institucionais de segurança do CERT.br e contrastadas com os dados macroeconômicos de faturamento do SEBRAE (2024; 2026), as limitações orçamentárias das PMEs são superadas pela eficiência de processos preventivos. Diante do cenário exposto pelas métricas reais de prejuízos mapeados no relatório de violações globais da IBM (2025), fechar as lacunas de supervisão e proteger as bases de dados torna-se a única salvaguarda viável contra incidentes que poderiam ser financeiramente letais para microempresas e empresas de pequeno porte.

Em suma, ao adotar as diretrizes propostas — controle estrito de privilégios com base no menor privilégio, mascaramento de dados

por meio de visões, tráfego de rede criptografado via *SSH Tunneling*/SSL e uma política resiliente de backup automatizado offline sob a regra 3-2-1 —, as organizações reduzem de forma expressiva sua superfície de ataque. Dessa maneira, as PMEs salvaguardam com sucesso a confidencialidade e a integridade de suas informações, atendem plenamente às exigências legais trazidas pela LGPD e garantem a continuidade sustentável de suas operações no dinâmico mercado digital contemporâneo.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 jun. 2026.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Autenticação: Fascículo Autenticação.** Cartilha de Segurança para Internet. São Paulo: Comitê Gestor da Internet no Brasil, 2022. Disponível em: https://cartilha.cert.br/fasciculos/. Acesso em: 15 jun. 2026.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Banco via Internet: Fascículo Banco via Internet.** Cartilha de Segurança para Internet. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: https://cartilha.cert.br/fasciculos/. Acesso em: 15 jun. 2026.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Proteção de Dados: Fascículo Proteção de Dados.** Cartilha de Segurança para Internet. São Paulo: Comitê

Gestor da Internet no Brasil, 2024. Disponível em: https://cartilha.cert.br/fasciculos/. Acesso em: 15 jun. 2026.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de Banco de Dados.** 3. ed. São Paulo: LTC, 2002.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de Banco de Dados.** 7. ed. São Paulo: Pearson, 2018.

IBM. **Relatório do custo das violações de dados 2025:** A lacuna na supervisão da IA. IBM Think Report, IBM Corporation, 2025.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de Informação Gerenciais.** 4. ed. Rio de Janeiro: LTC, 1997.

MEDEIROS, Maurício. **Banco de Dados para Sistemas de Informação.** Florianópolis: Visual Books, 2006.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang. **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021.

ORACLE Corporation. **MySQL Workbench:** Relational Database Design and Administration tool. Disponível em: https://www.mysql.com/products/workbench/. Acesso em: 15 jun. 2026.

SEBRAE. Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. **Atlas dos Pequenos Negócios 2024.** Brasília, DF: Sebrae Nacional, 2024. Disponível em: https://www.sebrae.com.br. Acesso em: 19 jun. 2026.

SEBRAE. Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. **Critérios de Classificação de Empresas: Faturamento e Porte.** São Paulo: Sebrae-SP, 2026. Disponível em: https://www.sebrae.com.br. Acesso em: 19 jun. 2026.