**Pilares da Segurança de Dados para o Novo Banco de Dados de Vendas**

Para garantir a segurança robusta do novo banco de dados de vendas, é crucial considerar os seguintes pilares fundamentais:

**1. Confidencialidade:**

* **Restringir o acesso:** Implementar controles de acesso rígidos para limitar o acesso aos dados apenas aos usuários autorizados e com as permissões adequadas.
* **Criptografia:** Criptografar os dados em repouso e em trânsito para proteger contra acesso não autorizado, mesmo em caso de violação de dados.
* **Mascaramento de dados:** Mascarar informações confidenciais, como dados PII (Informações Pessoais Identificáveis), para reduzir o risco de exposição em caso de violação.

**2. Integridade:**

* **Validação de dados:** Implementar mecanismos de validação de dados para garantir a precisão e confiabilidade das informações armazenadas.
* **Rastreamento de alterações:** Registrar todas as alterações feitas nos dados, incluindo quem as fez, quando e por qual motivo, para facilitar a auditoria e a investigação de incidentes.
* **Cópias de segurança e recuperação de desastres:** Manter backups regulares e atualizados dos dados para garantir a recuperação rápida em caso de perda ou corrupção de dados.

**3. Disponibilidade:**

* **Redundância de infraestrutura:** Implementar redundância em todos os componentes da infraestrutura, como servidores, redes e armazenamento, para garantir a disponibilidade contínua dos dados.
* **Planejamento de recuperação de desastres:** Desenvolver e testar um plano de recuperação de desastres para garantir a rápida restauração dos sistemas e dados em caso de interrupção.
* **Monitoramento e alerta:** Monitorar continuamente a infraestrutura e os dados para detectar e responder rapidamente a problemas que possam afetar a disponibilidade.

**4. Segurança física:**

* **Controle de acesso físico:** Restringir o acesso físico ao local onde o banco de dados está armazenado para proteger contra roubo ou acesso não autorizado.
* **Segurança ambiental:** Implementar medidas de segurança ambiental para proteger o hardware contra danos físicos, como incêndios, inundações ou falhas de energia.
* **Descarte seguro de dados:** Implementar procedimentos adequados para o descarte seguro de dados confidenciais quando não forem mais necessários.

**5. Gerenciamento de riscos:**

* **Identificar e avaliar riscos:** Realizar avaliações regulares de risco para identificar e avaliar potenciais ameaças à segurança do banco de dados.
* **Implementar medidas de controle:** Implementar medidas de controle adequadas para mitigar os riscos identificados.
* **Monitorar e revisar:** Monitorar continuamente a eficácia das medidas de controle e revisar periodicamente as avaliações de risco para garantir que elas estejam atualizadas.

**6. Conscientização e treinamento:**

* **Treinar funcionários:** Treinar os funcionários sobre os riscos de segurança cibernética e as melhores práticas para proteger os dados da empresa.
* **Criar uma cultura de segurança:** Criar uma cultura de segurança na empresa onde a segurança de dados seja vista como uma prioridade para todos os funcionários.
* **Comunicar políticas de segurança:** Comunicar claramente as políticas de segurança de dados da empresa a todos os funcionários e garantir que eles as compreendam e as sigam.

**7. Conformidade:**

* **Atender aos requisitos legais:** Atender a todos os requisitos legais e regulatórios aplicáveis ​​à proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil.
* **Implementar controles de conformidade:** Implementar controles de conformidade adequados para garantir o cumprimento dos requisitos legais.
* **Monitorar mudanças nas leis e regulamentações:** Monitorar as mudanças nas leis e regulamentações relacionadas à proteção de dados e atualizar as políticas e procedimentos da empresa conforme necessário.