**Relatório de Avaliação de Vulnerabilidade**

**1st de Janeiro 2025**

# **Descrição do sistema**

O hardware do servidor consiste em um processador de CPU poderoso e 128 GB de memória. Ele roda na versão mais recente do sistema operacional Linux e hospeda um sistema de gerenciamento de banco de dados MySQL. Ele é configurado com uma conexão de rede estável usando endereços IPv4 e interage com outros servidores na rede. As medidas de segurança incluem conexões criptografadas SSL/TLS.

# **Escopo**

O escopo desta avaliação de vulnerabilidade se relaciona aos controles de acesso atuais do sistema. A avaliação cobrirá um período de três meses, de junho de 2025 a agosto de 2025. O NIST SP 800-30 Rev. 1 é usado para orientar a análise de risco do sistema de informações.

# **Propósito**

O servidor de banco de dados é um componente fundamental para a operação da empresa, pois armazena dados críticos, como informações de clientes, transações financeiras e dados operacionais. A proteção dessas informações é essencial para garantir a continuidade dos negócios e a confiança dos clientes. Caso o servidor seja desabilitado, haveria impactos imediatos, como a interrupção de serviços e a perda de dados, afetando não apenas as operações internas, mas também a reputação da empresa perante seus clientes e parceiros

# **Avaliação de risco**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Fonte de ameaça** | **Evento de ameaça** | **Probabilidade** | **Gravidade** | **Risco** |
| *Concorrentes / hackers* | *Obter informações confidenciais por meio de exfiltração* | *3* | *3* | *9* |
| *Funcionário* | *Interromper operações críticas* | *2* | *3* | *6* |
| *Fornecedor* | *Acesso não autorizado ao sistema* | *2* | *2* | *4* |
| *Cliente* | *Alterar/Excluir informações críticas* | *1* | *3* | *3* |

# **Abordagem**

A avaliação de risco foi conduzida analisando as ameaças e vulnerabilidades relacionadas ao controle de acesso e à segurança do servidor de banco de dados. O foco principal foram eventos que envolvem o acesso não autorizado e a manipulação indevida de dados sensíveis. Para determinar a probabilidade de cada ameaça, levamos em conta o nível de exposição do sistema, como as permissões de acesso configuradas, e o histórico de incidentes de segurança. A gravidade dos riscos foi medida com base no impacto potencial que cada evento poderia ter nas operações diárias da empresa e na confiança dos clientes. As pontuações finais foram definidas levando em consideração tanto os aspectos técnicos do sistema quanto a gestão operacional de segurança já implementada.

# **Estratégia de Remediação**

Para reduzir os riscos identificados, recomendamos a implementação de medidas que reforçam a segurança do sistema. Isso inclui a adoção de autenticação multifatorial (MFA) e controle de acesso baseado em funções (RBAC), garantindo que apenas usuários autorizados tenham acesso ao banco de dados, com permissões restritas de acordo com suas responsabilidades. Além disso, é fundamental revisar periodicamente as permissões de acesso, sempre seguindo o princípio do menor privilégio. A criptografia de dados em trânsito deve ser feita utilizando TLS em vez de SSL, garantindo maior segurança nas comunicações. Para limitar ainda mais os riscos, sugerimos aplicar uma lista de IPs permitidos (whitelist), restringindo o acesso ao banco de dados a endereços confiáveis, como os de escritórios corporativos. Essas medidas, junto com um sistema de auditoria contínua, ajudarão a detectar atividades suspeitas rapidamente e facilitarão investigações caso ocorram incidentes de segurança.