**FUNDAÇÃO ESCOLA DE COMÉRCIO ALVARES PENTEADO**

**Lucca Brandão RA: 23024740**

**Murrilo Lopes RA:24026183**

**Rodrigo Cruz RA: 24026578**

**Vinicius Kingo RA: 24026141**

# Levantamento de riscos e vulnerabilidade

## Cibersegurança

**São Paulo**

**2025**

**INTRODUÇÃO:**

Nesse documento será realizada uma análise completa de riscos, vulnerabilidades e ameaças relacionadas ao nosso projeto, com o objetivo de identificar pontos críticos de segurança, como possíveis vazamentos de dados, e propor medidas para preveni-los.

**OBJETIVO:**

Estabelecer uma compreensão aprofundada e organizada dos riscos de cibersegurança que afetam diretamente o projeto, abrangendo sistemas, ativos, dados e pessoas. O propósito central é construir uma base sólida de proteção, permitindo a detecção antecipada de vulnerabilidades e a definição de medidas eficazes de mitigação.

## ATIVOS CRÍTICOS DO PROJETO

**Banco de Dados** – Repositório central contendo informações de usuários, registros de eventos/cursos e transações financeiras.

**API / Backend (Node.js + JWT)** – Responsável pela lógica de negócio e autenticação, sendo um ponto sensível para ataques de injeção, manipulação de tokens e acessos não autorizados.

**Frontend (React)** – Interface de interação com o usuário, que pode ser alvo de ataques de injeção de scripts (XSS) e manipulação de dados de entrada.

**Credenciais de Autenticação** – Conjunto de chaves, tokens e senhas utilizadas no acesso a serviços internos e externos, representando um dos maiores vetores de risco caso sejam expostas.

**Servidor / Infraestrutura (Azure ou local)** – Ambiente de hospedagem e execução dos serviços, sujeito a vulnerabilidades de configuração, falhas de atualização e indisponibilidade.

**PRINCIPAIS RISCOS IDENTIFICADOS:**

**Exposição de Dados Sensíveis:** Vazamento de credenciais, informações pessoais e históricos de usuários, comprometendo privacidade e conformidade regulatória.

**Indisponibilidade do Sistema:** Interrupções ou falhas críticas que possam paralisar totalmente as operações, afetando diretamente a continuidade do negócio.

**Uso Indevido de Perfis Privilegiados:** Exploração de contas administrativas ou perfis de alto nível para executar ações não autorizadas e causar impactos significativos.

**Falhas de Integração com APIs Externas:** Problemas de comunicação com serviços de terceiros (como bancos de pagamento), que podem gerar inconsistências ou interrupções nos processos.

## CATEGORIAS DE AVALIAÇÃO (FRAMEWORK NIST)

**ID.AM (Asset Management):** Identificação e gestão de ativos críticos do ambiente tecnológico.

**ID.BE (Business Environment):** Compreensão do ambiente de negócios e das dependências tecnológicas estratégicas.

**ID.GV (Governance):** Estruturação de governança, definição clara de papéis, responsabilidades e políticas de segurança.

**ID.RA (Risk Assessment):** Processo sistemático de avaliação e priorização dos riscos de cibersegurança.

**ID.RM (Risk Management Strategy):** Formulação de estratégias práticas e sustentáveis de mitigação de riscos.

**EXEMPLO DE IMPLEMENTAÇÃO DE MELHORIA:**

Elaborar um inventário abrangente de todos os ativos críticos da organização (incluindo servidores, endpoints, sistemas em nuvem e APIs expostas), classificando-os por nível de criticidade. Esse processo deve ser revisado periodicamente, garantindo a visibilidade contínua do ambiente tecnológico e priorizando a proteção dos elementos mais sensíveis.

**PRINCIPAIS MEDIDAS IMPLEMENTADAS:**

**1- Gestão de Identidades e Acessos (IAM):**

Diferenciação clara de perfis (Clientes e Administradores).

Autenticação baseada em **JWT** com expiração de sessão e uso de *refresh token*.

Armazenamento seguro de credenciais utilizando **bcrypt + salt** para fortalecer a proteção de senhas.

**2- Proteção de Dados:**

Criptografia em trânsito através de protocolos **TLS 1.2/1.3**.

Criptografia em repouso para dados sensíveis com **AES-256**.

Definição de **políticas de backup** e versionamento seguro para garantir a disponibilidade e a integridade da informação.

**3- Segurança no Desenvolvimento:**

Implementação de **prepared statements/ORM** para evitar injeções SQL.

**Sanitização de inputs** para mitigar riscos de ataques de injeção de código.

Integração de **pipelines CI/CD** com *scanners* de vulnerabilidades, promovendo segurança contínua durante o ciclo de desenvolvimento.

**4- Controle de Dependências:**

Monitoramento sistemático de **CVE (Common Vulnerabilities and Exposures)**.

**Atualizações periódicas** de bibliotecas e pacotes para reduzir riscos relacionados a softwares de terceiros.

## CATEGORIAS DE PROTEÇÃO

**PR.AC (Access Control):** Gestão de acessos baseada em MFA e princípio de privilégios mínimos.

**PR.AT (Awareness & Training):** Conscientização contínua e treinamentos em segurança da informação.

**PR.DS (Data Security):** Proteção de dados críticos com criptografia e ferramentas de DLP (*Data Loss Prevention*).

**PR.IP (Information Protection Processes & Procedures):** Processos formais e documentados de proteção da informação.

**PR.MA (Maintenance):** Práticas de manutenção segura para atualização e suporte de sistemas.

**PR.PT (Protective Technology):** Utilização de tecnologias de proteção como **firewalls, WAFs (Web Application Firewall)** e soluções **EDR (Endpoint Detection and Response)**.

## PRINCIPAIS CAPACIDADES DE DETECÇÃO:

### Monitoramento e Logging:

- Registro centralizado de logs de autenticação.
- Identificação automática de múltiplas tentativas de login suspeitas.
- Geração de alertas automáticos para atividades fora do padrão.

### Ferramentas de Detecção:

- Implementação de **rate limiting** para conter ataques de força bruta e requisições abusivas.
- Análise de **padrões de tráfego** para detectar anomalias e acessos não autorizados.
- Planejamento de integração futura com soluções de **SIEM (Security Information and Event Management)**.

**CATEGORIAS DE DETTECÇÃO (FRAMEWORK NIST):**

**DE.CM (Security Continuous Monitoring):** Monitoramento contínuo de logs, tráfego de rede e comportamento dos usuários.

**DE.DP (Detection Processes):** Definição de processos claros e acionáveis para detecção e resposta a incidentes.

## PLANOS DE RESPOSTA:

### Procedimentos de reposta a incidentes:

- **Identificação:** Localização da origem do incidente e análise inicial.
- **Contenção:** Adoção de medidas imediatas para impedir a propagação do ataque.
- **Erradicação:** Remoção completa da ameaça identificada.
- **Recuperação:** Restauração dos serviços afetados, garantindo sua operação normal e segura.

### Comunicação:

- Registro detalhado do incidente em sistema centralizado.
- Escalonamento para os responsáveis técnicos e gestores.
- Comunicação interna e, quando necessário, externa, de forma clara e objetiva.

### Categorias (NIST):

- **RS.RP (Response Planning):** Estruturação de planos de resposta a incidentes.
- **RS.CO (Communications):** Estratégias de comunicação interna e externa durante crises.
- **RS.AN (Analysis):** Análise aprofundada das causas e impactos do incidente.
- **RS.MI (Mitigation):** Adoção de ações para neutralizar ataques em andamento.
- **RS.IM (Improvements):** Atualizações e melhorias contínuas nos planos de resposta.

## PLANO DE RECUPERAÇÃO:

### Principais Práticas de Recuperação:

- **Backup & Restore:** Definição de políticas de backup diário e semanal, acompanhadas de testes regulares de restauração.
- **Plano de Continuidade:** Estabelecimento de métricas de **RTO (Recovery Time Objective)** e **RPO (Recovery Point Objective)** para definir prazos aceitáveis de recuperação.
- **Lições Aprendidas:** Registro sistemático dos incidentes e definição de melhorias constantes no processo.

### Categorias (NIST):

- **RC.RP (Recovery Planning):** Estruturação de planos formais de recuperação.
- **RC.IM (Improvements):** Ajustes e reforços pós-incidente para fortalecer o ambiente.
- **RC.CO (Communications):** Comunicação efetiva com clientes, parceiros e órgãos reguladores em situações de crise.

## CONCLUSÃO:

A aplicação do **NIST Cybersecurity Framework (CSF)** no projeto demonstrou a viabilidade de estruturar um plano de cibersegurança robusto, contemplando as etapas de prevenção, detecção, resposta e recuperação. A análise realizada permitiu identificar riscos críticos, como vazamento de dados e ataques de força bruta, propondo controles adequados, incluindo **criptografia, autenticação JWT e monitoramento contínuo de logs**.

Tais medidas reforçam os princípios de **confidencialidade, integridade e disponibilidade (CIA)** dos dados e serviços, fundamentais para a segurança da informação.

Além disso, a utilização prática do framework em um contexto acadêmico contribui diretamente para a formação de profissionais capazes de atuar em ambientes reais de cibersegurança. As recomendações e controles sugeridos não apenas fortalecem a resiliência do sistema, mas também estabelecem uma cultura de melhoria contínua, alinhada às melhores práticas internacionais.