FUNDAÇÃO ESCOLA DE COMÉRCIO ÁLVARES PENTEADO
FECAP

CENTRO UNIVERSITÁRIO ÁLVARES PENTEADO

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

ALEXANDRA CHRISTINE SILVA RAIMUNDO – 24026156
CARLOS AUGUSTO SANTOS DE ALMEIDA - 20010535
HEBERT DOS REIS ESTEVES - 24026079
JOSÉ BENTO ALMEIDA GAMA - 24026127

Levantamento de Riscos e Vunerabilidades e Ameaças Baseadas no NIST

São Paulo
2025

Sumário

1. Introdução

Este documento apresenta uma análise detalhada de riscos, vulnerabilidades e ameaças relacionados ao Projeto Integrador (PI), estruturada com base nas funções do NIST Cybersecurity Framework (CSF).

O objetivo é identificar os pontos críticos de segurança do Cannoli Intelligence, estabelecer controles eficazes de mitigação e propor medidas alinhadas às melhores práticas internacionais de cibersegurança.

Além disso, este documento se conecta às etapas anteriores do projeto:

- Descrição de Dados e Exploração/Qualidade, que revelaram lacunas de preenchimento e inconsistências críticas para segurança.
- Implementação de IA/ML, que exige proteção contra manipulação de dados e integridade nos modelos preditivos.

2. Identificação de Riscos

Objetivo: Desenvolver uma compreensão organizacional dos riscos de cibersegurança, incluindo sistemas, ativos, dados e pessoas, para estabelecer uma base sólida de proteção.

Ativos do Projeto:

1. Banco de Dados.
2. API/Backend (Node.js + JWT).
3. Frontend (React).
4. Credenciais de autenticação.
5. Servidor/Infraestrutura (Azure ou local).

Riscos Principais:

- Exposição de dados sensíveis (credenciais, históricos, dados pessoais).
- Indisponibilidade do sistema (paralisação total de operações).
- Uso indevido de perfis privilegiados (administrador).
- Falhas de integração com APIs externas (pagamentos, WhatsApp).
- Lacunas de preenchimento em dados críticos (ex.: gênero e badge), impactando segmentações e segurança de relatórios.

Categorias:

- **ID.AM (Asset Management):** Gerenciamento de ativos críticos.
- **ID.BE (Business Environment):** Definição do ambiente de negócios e dependências tecnológicas.
- **ID.GV (Governance):** Estruturas de governança, papéis e responsabilidades.
- **ID.RA (Risk Assessment):** Avaliação sistemática dos riscos cibernéticos.
- I**D.RM (Risk Management Strategy):** Estratégia de gerenciamento de riscos.

Exemplo de possivel implementação de melhoria: Inventário de todos os ativos críticos da organização (servidores, endpoints, sistemas em nuvem, APIs expostas) e classificação por criticidade.

3. Medidas de Proteção

- **Gestão de Identidades e Acessos (IAM):** Perfis diferenciados (Clientes e Administrador), autenticação JWT com expiração e refresh token, armazenamento de senhas com bcrypt + salt.
- **Proteção de Dados:** Criptografia em trânsito (TLS 1.2/1.3), criptografia em repouso para dados sensíveis (AES-256), políticas de backup e versionamento seguro.
- **Segurança no Desenvolvimento:** Uso de prepared statements/ORM, sanitização de inputs, pipeline CI/CD com scanner de vulnerabilidades.
- **Controle de Dependências:** Monitoramento de CVEs e atualizações periódicas.
- **Treinamento e Conscientização:** clientes e colaboradores orientados contra phishing e engenharia social.

Categorias:

- PR.AC (Access Control): Controle de acessos (MFA, privilégios mínimos).
- PR.AT (Awareness & Training): Conscientização e treinamento em segurança.
- PR.DS (Data Security): Proteção de dados sensíveis (criptografia, DLP).
- PR.IP (Information Protection Processes & Procedures): Processos de proteção da informação.
- PR.MA (Maintenance): Manutenção segura de sistemas e softwares.
- PR.PT (Protective Technology): Tecnologias de proteção (firewall, EDR, WAF).

Exemplo de possivel implementação de melhoria: Implementar MFA em todos os acessos e treinar clientes e colaboradores da Cannoli contra phishing.

4. Capacidades de Detecção

Monitoramento e Logging: Registro centralizado de logs de autenticação, detecção de múltiplas tentativas de login, alertas automáticos.
Ferramentas de Detecção: Rate limiting, análise de padrões de tráfego, integração futura com SIEM.

Objetivo: Identificar rapidamente atividades anômalas e possíveis incidentes de segurança.

Categorias:

- DE.CM (Security Continuous Monitoring): Monitoramento contínuo de logs, tráfego e comportamento.
- DE.DP (Detection Processes): Definição de processos de detecção claros e acionáveis.

Exemplo de possivel implementação de melhoria: Implantação de um SIEM (ex: Splunk, QRadar, ELK) para correlação de eventos e alertas de ameaças.

5. Planos de Resposta

Procedimento de Resposta a Incidentes: Identificação da origem, contenção, erradicação e recuperação.
Comunicação: Registro do incidente, escalonamento ao responsável, comunicação
Lições Aprendidas: documentação de incidentes e melhorias

Objetivo: Minimizar o impacto dos incidentes por meio de uma resposta coordenada, eficiente e documentada.

Categorias:

- RS.RP (Response Planning): Planejamento de resposta a incidentes.
- RS.CO (Communications): Comunicação interna e externa durante incidentes.
- RS.AN (Analysis): Análise detalhada do incidente.
- RS.MI (Mitigation): Mitigação de ataques em andamento.
- RS.IM (Improvements): Melhorias contínuas no plano de resposta.

Exemplo de possivel implementação de melhoria: Playbook de resposta a ransomware com isolamento da máquina e acionamento de stakeholders da Cannoli.

6. Planos de Recuperação

- Backup & Restore: Políticas de backup diário/semanal, testes periódicos.
- Plano de Continuidade: Definição de RTO (Recovery Time Objective) e RPO (Recovery Point Objective).
- Lições Aprendidas: Registro de incidentes e melhorias contínuas.

Objetivo: Restaurar serviços e capacidades após um incidente, garantindo resiliência organizacional.

Categorias:

- RC.RP (Recovery Planning): Planejamento de recuperação.
- RC.IM (Improvements): Ajustes pós-incidente para fortalecer o ambiente.
- RC.CO (Communications): Comunicação com clientes, parceiros e órgãos reguladores.

Exemplo de possivel implementação de melhoria: Criação de uma documentação de Disaster Recovery.

7. Matriz de Riscos (NIST)

Risco	Função NIST	Probabilidade	Impacto	Criticidade	Mitigação
Vazamento de dados	Protect	Alta	Alta	Crítico	Criptografia + IAM
Força bruta em login	Detect/Protect	Alta	Média	Alto	Rate limiting + Captcha
SQL Injection	Protect	Média	Alta	Alto	ORM + validação de inputs
Indisponibilidade por DDoS	Detect/Respond	Média	Alta	Alto	WAF + rate limiting
Usuário interno mal-intencionado	Identify/Protect	Baixa	Alta	Médio	RBAC + auditoria
Falha em backup/restauração	Recover	Média	Alta	Alto	Testes periódicos de backup

8. Conclusão

O estudo evidenciou que, ao alinhar o projeto ao NIST Cybersecurity Framework (CSF), é possível estruturar um plano robusto de cibersegurança que contempla prevenção, detecção e resposta a incidentes. A análise revelou riscos críticos, como vazamento de dados e ataques de força bruta, e propôs controles adequados, incluindo criptografia, autenticação JWT e monitoramento de logs, essenciais para garantir a confidencialidade, integridade e disponibilidade (CIA) dos dados e serviços.

A aplicação prática deste framework no contexto acadêmico contribui não apenas para a qualidade do Projeto Integrador, mas também para a formação de profissionais capacitados a atuar em cenários reais de cibersegurança. As recomendações apresentadas fortalecem a resiliência do sistema e estabelecem um plano de melhoria contínua, alinhando o projeto às melhores práticas internacionais de segurança da informação.