FACULDADE FECAP

CURSO: Análise e Desenvolvimento de Sistemas

ANÁLISE DE RISCOS E PLANO DE MITIGAÇÃO – PROJETO INTEGRADOR CANNOLI INTELLIGENCE

Integrantes:
Alexandra Christine Silva Raimundo - 24026156

Carlos Augusto - 20010535

Hebert Esteves - 24026079

José Bento Almeida Gama - 24026127

São Paulo – 2025

Sumário

1. INTRODUÇÃO

O presente relatório apresenta a análise de riscos e o plano de mitigação aplicados ao Projeto Integrador Cannoli Intelligence, desenvolvido no âmbito do curso de Análise e Desenvolvimento de Sistemas da Faculdade FECAP. O projeto tem como objetivo principal a criação de uma plataforma de Business Intelligence (BI) e Inteligência Artificial (IA) capaz de transformar dados brutos em indicadores estratégicos, relatórios interativos e sugestões inteligentes voltadas à otimização da performance empresarial no setor alimentício.

A proposta da Cannoli Intelligence surgiu a partir da necessidade de centralizar informações comerciais, operacionais e de marketing de empresas parceiras em um único ambiente de análise. O sistema integra módulos de banco de dados, backend em Node.js, frontend em React e uma camada de inteligência artificial desenvolvida em Python, responsável por gerar insights automáticos e recomendações de campanhas baseadas em aprendizado de máquina.

Diante do volume e sensibilidade dos dados tratados, torna-se essencial aplicar princípios de Cibersegurança desde as fases iniciais do desenvolvimento. Nesse contexto, esta análise adota como referência o NIST Cybersecurity Framework (CSF), que fornece uma estrutura padronizada para identificar, proteger, detectar, responder e recuperar-se de ameaças cibernéticas. O estudo busca alinhar o projeto às melhores práticas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade (CIA) dos dados e serviços prestados.

Além disso, foi utilizada a Matriz GUT (Gravidade, Urgência e Tendência) como ferramenta para a priorização dos riscos identificados durante a fase de mapeamento. Essa metodologia permite classificar e quantificar os impactos potenciais sobre os ativos do sistema, direcionando as ações de mitigação de forma estratégica e proporcional à criticidade dos riscos.

A integração entre os princípios do NIST CSF e a análise GUT proporciona uma abordagem completa e estruturada para a segurança no contexto acadêmico e profissional, demonstrando como o projeto Cannoli Intelligence pode servir de modelo para o desenvolvimento seguro de soluções tecnológicas aplicadas ao mercado real. Dessa forma, este documento visa não apenas relatar vulnerabilidades e soluções técnicas, mas também reforçar a importância da cultura de segurança digital dentro do ciclo de vida do desenvolvimento de software.

2. METODOLOGIA

Para a priorização e tratamento dos riscos, foi aplicada a Matriz GUT (Gravidade, Urgência e Tendência), associando-a às funções do NIST CSF: Identify, Protect, Detect, Respond e Recover. A metodologia permite determinar quais riscos exigem resposta imediata e quais podem ser acompanhados a longo prazo, direcionando os esforços de mitigação de forma estratégica.

Risco Identificado	Função NIST	Gravidade (G)	Urgência (U)	Tendência (T)	Cálculo GxUxT	Criticidade	Ação/Mitigação Recomendada
Vazamento de dados sensíveis	Protect	5	5	5	125	**Crítico**	Criptografia AES-256 + TLS 1.3 + IAM/MFA
Ataques de força bruta em login	Detect / Protect	4	4	5	80	**Alto**	Rate limiting, Captcha e bloqueio após tentativas
SQL Injection	Protect	4	4	4	64	**Alto**	ORM, prepared statements e sanitização de inputs
Indisponibilidade por DDoS	Detect / Respond	4	3	4	48	**Alto**	WAF, rate limiting e monitoramento de tráfego
Usuário interno mal-intencionado	Identify / Protect	3	2	4	24	**Médio**	RBAC, auditoria de logs e segregação de funções
Falha em backup/restauração	Recover	4	3	3	36	**Baixo**	Testes periódicos de backup e redundância
Lacunas de preenchimento em dados crítico	Identify	3	4	4	48	**Médio**	Regras de validação e auditoria de dados no backend
Falhas de integração com APIs externas	Protect	3	3	4	36	**Médio**	Autenticação segura (tokens), logs e testes automatizados

Letra	Significado	Descrição
G	Gravidade	Impacto no negócio/segurança
U	Urgência	Quão rápido precisa agir
T	Tendência	Chance de piorar/ocorrer
GxUxT	Prioridade	Define a criticidade final

3. RESULTADOS – MATRIZ GUT DE RISCOS

3.1 Tabela GUT – Riscos x Ações de Mitigação

A seguir, apresenta-se a tabela GUT consolidada, com a classificação de riscos segundo os critérios de Gravidade, Urgência e Tendência, bem como o cálculo de criticidade e as ações recomendadas para mitigação.

4. ANÁLISE DAS AÇÕES DE MITIGAÇÃO

4.1 Criptografia AES-256 + TLS 1.3 + IAM/MFA

Risco tratado: Vazamento de dados sensíveis. Aplicação: uso de criptografia forte em trânsito e repouso, autenticação multifator e controle de identidade. Benefício: garante a confidencialidade e integridade das informações.

4.2 Rate Limiting e Firewall de Aplicação

Risco tratado: ataques de negação de serviço. Aplicação: limitação de requisições no Node.js e uso de firewall para bloqueio de acessos suspeitos. Benefício: protege a disponibilidade do sistema.

4.3 Backup Automatizado e Redundância de Dados

Risco tratado: perda de dados. Aplicação: agendamento de backups automáticos e replicação da pasta IA_output. Benefício: assegura recuperação rápida em incidentes.

4.4 Logs e Auditoria de Eventos

Risco tratado: falta de rastreabilidade. Aplicação: registro detalhado de operações críticas e acessos administrativos. Benefício: melhora a detecção de incidentes e conformidade.

4.5 Validação de Inputs e Sanitização de Dados

Risco tratado: injeção de código. Aplicação: verificação de entradas e uso de express-validator no backend. Benefício: impede exploração de falhas de segurança.

4.6 Controle de Perfis e Acesso JWT (RBAC)

Risco tratado: acesso indevido. Aplicação: autenticação JWT e controle por papéis (admin, professor, aluno). Benefício: garante segregação de privilégios.

4.7 Monitoramento e Detecção de Ameaças

Risco tratado: ataques em tempo real. Aplicação: integração com logs e alertas de anomalias. Benefício: reduz o tempo de resposta a incidentes.

4.8 Autenticação Segura e Senhas Criptografadas

Risco tratado: roubo de credenciais. Aplicação: uso de bcrypt e políticas de senha forte. Benefício: reforça a segurança de contas de usuários.

5. APLICAÇÃO DAS SOLUÇÕES NO CANNOLI INTELLIGENCE

As soluções de mitigação serão incorporadas diretamente na arquitetura do projeto. O backend, desenvolvido em Node.js, implementará rate limiting, JWT e logs de auditoria. A comunicação entre backend e o módulo de IA em Python será protegida com TLS e tokens de acesso. Backups automáticos garantirão a integridade dos dados gerados, e as validações de input reforçarão a segurança contra ataques comuns.

6. CONCLUSÃO

As ações propostas fortalecem o sistema Cannoli Intelligence, assegurando conformidade com o NIST CSF e boas práticas de segurança. A adoção dessas medidas desde o início do desenvolvimento promove maior resiliência, confiabilidade e responsabilidade acadêmica no tratamento de dados sensíveis.

7. REFERÊNCIAS

NIST – Cybersecurity Framework (CSF), 2023.

OWASP Foundation. Top 10 Web Application Security Risks, 2023.

Microsoft Azure Documentation. Security and Compliance, 2024.

Ferreira, C. (2021). Segurança da Informação e Gestão de Riscos. São Paulo: Atlas.