FUNDAÇÃO ESCOLA DE COMÉRCIO ÁLVARES PENTEADO
FECAP

Análise e Desenvolvimento de Sistemas

Adeilson Nunes - 23025670

Bruna Cristina Lira - 24025837

Daniela Pauzer - 24025749

Enzo Sangiacomo - 24025841

Rafaela Coelho - 24026076

São Paulo

2025

Adeilson Nunes - 23025670

Bruna Cristina Lira - 24025837

Daniela Pauzer - 24025749

Enzo Sangiacomo - 24025841

Rafaela Coelho - 24026076

Levantamento de Riscos, Vulnerabilidades e Ameaças

Trabalho de Cibersegurança e Defesa Cibernética: Levantamento de Riscos, Vulnerabilidades e Ameaças.
Projeto Integrado 2025-2
Apresentado à Fundação Escola de Comércio
Álvares Penteado - FECAP
Orientador: Prof. Ronaldo Araújo

São Paulo

2025

Índice

Introdução

O presente documento tem como objetivo apresentar o levantamento de riscos, vulnerabilidades e ameaças do projeto Dashboard Interativo Cannoli, seguindo como referência o NIST Cybersecurity Framework, amplamente utilizado para estruturar a gestão de segurança da informação.

O NIST divide as práticas de cibersegurança em cinco funções principais: Identify (Identificar), Protect (Proteger), Detect (Detectar), Respond (Responder) e Recover (Recuperar).
A partir dessas etapas, é possível entender o ambiente, aplicar controles, detectar falhas, agir diante de incidentes e restaurar o sistema quando necessário.

1. Identify (ID) – Identificar

- **Objetivo:** entender os ativos, riscos, processos e dados do projeto.

ID.AM – Gerenciamento de Ativos:

- Falta de mapeamento de todos os sistemas e usuários com acesso ao dashboard.
- Risco de **vazamento de dados sensíveis** de clientes e administradores.

ID.BE – Ambiente de Negócios:

- Falta de definição clara sobre quem administra as permissões de acesso.
- Dependência de servidores externos (cloud).

ID.GV – Governança:

- Ausência de políticas formais de segurança e controle de acesso.
- Falta de plano de continuidade em caso de incidentes.

ID.RA – Avaliação de Risco:

- Falta de análise de impacto caso ocorra um ataque cibernético.
- Ameaça de perda de dados ou exposição indevida.

ID.RM – Estratégia de Gerenciamento de Risco:

- Falta de registro de procedimentos para resposta e mitigação.

2. Protect (PR) – Proteger

- **Objetivo:** implementar medidas para evitar ou reduzir danos em caso de incidentes.

PR.AC – Controle de Acesso:

- Falha na autenticação de usuários.
- Risco de **acesso não autorizado ao dashboard**.

PR.AT – Conscientização e Treinamento:

- Falta de orientação aos usuários sobre senhas fortes e boas práticas.

PR.DS – Segurança de Dados:

- **Vulnerabilidade:** ausência de criptografia nas comunicações (sem HTTPS/SSL).
- **Risco:** exposição de informações sensíveis durante o uso do sistema.

PR.IP – Processos de Proteção:

- Falta de verificação e atualização das permissões de acesso.
- Inexistência de logs automáticos de alteração de dados.

PR.MA – Manutenção:

- Códigos sem auditoria de segurança e sem rotina de atualização.

PR.PT – Tecnologia de Proteção:

- Falta de uso de firewall e antivírus corporativo.

3. Detect (DE) – Detectar

- **Objetivo:** monitorar o sistema e identificar incidentes rapidamente.

DE.CM – Monitoramento Contínuo:

- Falta de ferramentas que monitorem tentativas de acesso e falhas de login.
- Ausência de alertas automáticos para atividades suspeitas.

DE.DP – Processos de Detecção:

- **Risco:** incidentes não detectados a tempo.
- **Vulnerabilidade:** logs desatualizados e não revisados.
- **Ameaça:** ataque não identificado resultando em vazamento de informações.

4. Respond (RS) – Responder

- **Objetivo:** agir de forma rápida e eficaz quando um incidente é detectado.

RS.RP – Planejamento de Resposta:

- Falta de plano formal de resposta a incidentes.
- **Risco:** demora na tomada de decisão durante ataques.

RS.CO – Comunicação:

- Falta de canal definido para comunicar falhas aos administradores.

RS.AN – Análise:

- Ausência de procedimento para investigar incidentes e suas causas.

RS.MI – Mitigação:

- Falta de medidas para reduzir o impacto de ataques, como bloqueio de IPs.

RS.IM – Melhorias:

- Não há registro de incidentes anteriores para evitar repetições.

5. Recover (RC) – Recuperar

- **Objetivo:** restaurar dados e operações após um incidente.

RC.RP – Planejamento de Recuperação:

- Falta de política de **backup automático** e testes de restauração.
- **Risco:** perda permanente de dados do dashboard.

RC.IM – Melhorias:

- Não há plano documentado de recuperação pós-incidente.

RC.CO – Comunicação:

- Falta de comunicação com usuários em caso de falhas ou indisponibilidade.
- **Ameaça:** danos à imagem e confiança dos parceiros da Cannoli.

6. Matriz GUT

Nº	Risco Identificado	Gravidade (G	Urgência (U	Tendência	Índice GUT (G×U×	Priorida
1	Vazamento de dados sensíveis de clientes e administradores	5	5	5	125	Crítico
2	Acesso não autorizado ao dashboard (falha na autenticação)	5	5	4	100	Crítico
3	Falta de criptografia nas comunicações (sem HTTPS/SSL)	5	4	4	80	Alto
4	Falta de backup e plano de recuperação de dados	4	4	4	64	Médio
5	Falha no monitoramento e ausência de logs automáticos	4	3	4	48	Médio
6	Códigos desatualizados e sem auditoria de segurança	3	3	3	27	Baixo
7	Falta de treinamento dos usuários e políticas de senha fraca	3	3	4	36	Baixo
8	Indisponibilidade temporária da plataforma (ataque DDoS ou falha técnica)	4	3	3	36	Baixo
9	Demora na resposta a incidentes detectados	4	4	3	48	Médio
10	Danos à imagem e reputação da empresa após falhas	5	3	3	45	Médio

➢ Interpretação da Matriz

- Vermelho | Crítico (100–125): risco que exige ação imediata.
- Laranja | Alto (70–99): precisa de plano de mitigação a curto prazo.
- Amarelo | Médio (40–69): monitoramento contínuo e prevenção.
- Verde | Baixo (até 39): riscos menores, podem ser aceitos temporariamente.

7. Conclusão

Com base na análise realizada, foi possível identificar os principais **riscos, vulnerabilidades e ameaças** relacionados ao projeto **Dashboard Interativo Cannoli**, considerando as possíveis falhas que podem comprometer a segurança, a disponibilidade e a confiabilidade das informações.

A aplicação do **NIST Cybersecurity Framework** permitiu organizar o levantamento de forma estruturada e técnica, dividindo as ações em cinco etapas: **Identify, Protect, Detect, Respond e Recover**. Essa metodologia ajudou a entender melhor cada fase do processo de segurança, desde a identificação dos riscos até a recuperação em caso de incidentes, garantindo uma visão completa sobre o ambiente do sistema.

Além disso, a **Matriz GUT (Gravidade, Urgência e Tendência)** foi utilizada para avaliar e priorizar os riscos identificados, destacando quais exigem maior atenção e resposta imediata. Os resultados mostraram que os pontos mais críticos estão relacionados à **proteção dos dados**, **autenticação de acesso**, **ausência de backup** e **falhas no monitoramento de segurança**.

De modo geral, o estudo demonstra que a segurança da informação é um processo contínuo, que exige atenção constante e boas práticas em todas as etapas do desenvolvimento. A integração entre o **NIST Framework** e a **Matriz GUT** trouxe uma visão mais completa e prática para o projeto, contribuindo para a criação de uma solução mais **segura, estável e confiável** para a plataforma Cannoli.