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

1. Introdução

O presente documento apresenta o levantamento de riscos, vulnerabilidades e ameaças relacionados ao desenvolvimento e uso do **Dashboard Interativo Cannoli**, conforme diretrizes do Projeto Interdisciplinar do 4º semestre de ADS – FECAP.
O objetivo é identificar os principais pontos de atenção em termos de segurança da informação, alinhados às normas ISO/IEC e ao NIST Cybersecurity Framework, garantindo a confidencialidade, integridade e disponibilidade (CIA) dos dados da plataforma.

2. Riscos Identificados

- **R1** – Vazamento de dados sensíveis de clientes, administradores e parceiros.

- **R2** – Acesso não autorizado ao dashboard, por roubo de credenciais ou falha de autenticação.

- **R3** – Indisponibilidade da plataforma por falhas técnicas ou ataques cibernéticos (ex.: DDoS).

- **R4** – Perda de dados devido à ausência de backup ou falha em rotinas de recuperação.

- **R5** – Manipulação indevida de relatórios/exportações, comprometendo a confiabilidade das análises.

- **R6** – Uso indevido de dispositivos móveis com sessão ativa sem logout adequado.

3. Vulnerabilidades

- **V1** – Políticas de senha fracas (reutilização, ausência de complexidade mínima).
- **V2** – Ausência de criptografia nas comunicações (não utilização de SSL/TLS/HTTPS).
- **V3** – Banco de dados sem camadas adicionais de proteção, suscetível a ataques de injeção SQL.
- **V4** – Armazenamento de informações sensíveis sem criptografia em repouso.
- **V5** – Falta de monitoramento contínuo de logs e alertas.
- **V6** – Falhas de desenvolvimento que podem permitir vulnerabilidades como XSS e CSRF.

4. Ameaças

❖ **Humanas Intencionais**

- Ataques de hackers com objetivo de roubar dados ou derrubar a plataforma.
- Usuários maliciosos internos (insiders) explorando acessos privilegiados.

❖ **Humanas Não Intencionais**

- Erros operacionais de usuários (ex.: exclusão acidental de registros, uploads incorretos).
- Compartilhamento indevido de credenciais por descuido.

❖ **Não Humanas**

- Interrupções de energia, falhas de hardware e indisponibilidade da rede.
- Desastres naturais que comprometam os servidores físicos (se hospedados on-premises).

5. Conclusão

O levantamento evidencia que o Dashboard Interativo Cannoli está sujeito a riscos inerentes ao ambiente digital, que podem impactar diretamente a continuidade do negócio e a confiabilidade dos dados.
Para mitigar esses riscos, recomenda-se a implementação de controles de segurança da informação, como:

- Autenticação multifator (MFA).
- Criptografia de dados em trânsito e em repouso.
- Políticas de backup e recuperação de desastres.
- Monitoramento contínuo e análise de logs.
- Treinamento de usuários para prevenção de falhas humanas.