FUNDAÇÃO ESCOLA DE COMÉRCIO ÁLVARES PENTEADO
FECAP

Análise de Riscos e Priorização GUT – Projeto Cannoli

Adriano Xu Ming Hui
Cauã William Barbieri Brandão
Gabriel Orlandi Portes
Karoline Lemos Avelar
Matheus Santoro Carriço Veiga

Nov/2025

Introdução

Após o levantamento de riscos, vulnerabilidades e ameaças realizado na etapa anterior, foi elaborada a presente Tabela de Priorização GUT, com o objetivo de classificar os riscos de segurança identificados no projeto Dashboard Interativo Cannoli conforme seu grau de criticidade.

O método GUT (Gravidade, Urgência e Tendência) permite avaliar cada risco de forma quantitativa, priorizando aqueles que exigem tratamento imediato e ações preventivas estratégicas.
Nesta etapa, a análise também foi alinhada ao Framework NIST, referência internacional em gestão de riscos de cibersegurança.

Tabela de Riscos x GUT – Cibersegurança Cannoli

Nº	Risco Identificado	Gravidade (G)	Urgência (U)	Tendência (T)	Pontuação (GxUxT)	Classificação	Impacto Potencial / Observação
1	Vazamento de dados de clientes e parceiros	5	5	5	125	Crítico	Viola a LGPD, compromete a reputação e pode gerar penalidades legais.
2	Falhas de autenticação e senhas fracas	5	4	5	100	Crítico	Permite acesso indevido ao painel administrativo. Necessário uso de hashing (bcrypt) e MFA.
3	Exposição de chaves API e tokens no repositório	5	5	4	100	Crítico	Abre acesso à infraestrutura e banco de dados. Mitigação via variáveis de ambiente (.env).
4	Comunicação sem HTTPS	4	5	4	80	Alto	Dados podem ser interceptados. Requer certificação SSL/TLS.
5	Falta de backup automático e redundância de dados	4	4	4	64	Alto	Perda de dados e histórico de pedidos em caso de falha. Necessário backup diário na nuvem.
6	Ataques de injeção SQL no backend	4	4	4	64	Alto	Possibilidade de manipulação do banco de dados. Mitigação com ORM seguro (Prisma) e sanitização de entradas.
7	Acesso indevido por usuários internos (admins)	3	4	4	48	Médio	Falta de controle de privilégios pode gerar vazamento interno. Aplicar RBAC.
8	Dependências desatualizadas (Node.js/React)	3	3	4	36	Médio	Vulnerabilidades conhecidas podem ser exploradas. Atualizações e npm audit são essenciais.
9	Ataques de força bruta em logins	4	3	3	36	Médio	Tentativas automatizadas comprometem credenciais. Implementar bloqueio e limite de tentativas.
10	Falta de logs e auditoria de segurança	3	3	3	27	Baixo	Dificulta rastreio de incidentes. Necessário sistema de monitoramento e alertas.

Critérios de Avaliação GUT

Valor	Gravidade (G)	Urgência (U)	Tendência (T)
5	Impacto extremo (paralisa o sistema ou viola a LGPD)	Exige ação imediata	Piora rapidamente
4	Impacto alto, mas controlável	Deve ser tratado em até 1 semana	Piora em curto prazo
3	Impacto moderado	Pode aguardar o próximo ciclo de manutenção	Piora lentamente
2	Baixo impacto	Correção pode ser planejada	Estável
1	Impacto mínimo	Pode ser ignorado	Não tende a piorar

Análise e Recomendações

Os riscos de maior criticidade (≥ 100) estão ligados à proteção de dados e infraestrutura, exigindo ação imediata.
Esses riscos devem ser tratados conforme as boas práticas da OWASP Top 10 e a Lei Geral de Proteção de Dados (LGPD), incluindo:

- ➢ Implementação de criptografia TLS/HTTPS e hashing de senhas;
- ➢ Armazenamento seguro de chaves de API e tokens em variáveis de ambiente;
- ➢ Backups automatizados e redundantes em nuvem;
- ➢ Autenticação multifator (MFA) e controle de acesso por função (RBAC);
- ➢ Monitoramento de segurança contínuo e testes de penetração regulares.

Alinhamento com o Framework NIST

A priorização dos riscos apresentada na Matriz GUT foi estruturada com base no Framework de Cibersegurança do NIST (National Institute of Standards and Technology), assegurando conformidade com padrões internacionais de segurança da informação.

Função NIST	Aplicação no Projeto Cannoli
Identify (Identificar)	Mapeamento dos riscos e vulnerabilidades da aplicação.
Protect (Proteger)	Implementação de criptografia, backups e autenticação segura.
Detect (Detectar)	Criação de logs, alertas e monitoramento de anomalias.
Respond (Responder)	Ações imediatas frente a incidentes de segurança e falhas críticas.
Recover (Recuperar)	Estratégias de backup, restauração e continuidade operacional.

A integração do método GUT ao Framework NIST fortalece a gestão de riscos da Cannoli, promovendo resiliência cibernética, prevenção de incidentes e conformidade com a LGPD.

Conclusão

Com base na Matriz GUT, observa-se que o projeto Cannoli apresenta três riscos críticos de segurança, que demandam mitigação imediata para garantir confidencialidade, integridade e disponibilidade dos dados (CIA Triad).
A aplicação das medidas corretivas propostas permitirá que o Dashboard Interativo Cannoli opere de forma segura, escalável e em conformidade com a LGPD, reforçando a confiança dos usuários e parceiros da plataforma.

A gestão de riscos contínua é fundamental para a maturidade em segurança digital da startup Cannoli.