Curso	Disciplina
4NAADS_S	Cibersegurança e Defesa Cibernética
Data	Alunos
07/11/2025	ANDREIA SILVA, GUILHERME MENDES, LUAN MEIRELES, MATHEUS FRANCISCO

INTRODUÇÃO

A segurança da informação é um dos pilares fundamentais para a manutenção da integridade, confidencialidade e disponibilidade dos dados em qualquer sistema tecnológico. No contexto do projeto Cannoli, torna-se essencial compreender e priorizar os riscos que podem comprometer a operação da plataforma e a proteção das informações dos usuários e parceiros.

Nesta segunda entrega, é apresentada a Matriz de Riscos e GUT (Gravidade, Urgência e Tendência), desenvolvida a partir do levantamento realizado na entrega anterior. O objetivo é avaliar e classificar os riscos identificados, estabelecendo uma hierarquia de criticidade que permita direcionar os esforços de mitigação de forma estratégica e eficaz.
Dessa forma, o estudo proporciona uma visão clara sobre quais riscos exigem resposta imediata, quais devem ser monitorados e quais possuem impacto reduzido, contribuindo para o fortalecimento da cibersegurança no ambiente do projeto.

A Matriz GUT é uma ferramenta de priorização de riscos, que atribui valores de 1 a 5 para cada fator — Gravidade (G), Urgência (U) e Tendência (T).
O produto desses valores gera o Índice GUT, que determina a prioridade de mitigação conforme a criticidade de cada risco.

Cor	Classificação	Faixa	Ação Recomendada
🔴 Vermelho	**Crítico**	100–125	Exige ação imediata
🟠 Laranja	**Alto**	70–99	Plano de mitigação a curto prazo
🟡 Amarelo	**Médio**	40–69	Monitorar e prevenir
🟢 Verde	**Baixo**	até 39	Risco aceitável temporariamente

RISCOS X GUT								
Nº	**Risco Identificado**	**G**	**U**	**T**	**Índice GUT**	**Impacto**	**Probabilidade**	**Nível**
🔴 1	Vazamento de dados sensíveis	5	5	5	125	Alto	Alta	Crítico
🔴 2	Acesso não autorizado ao painel	5	5	4	100	Alto	Média/Alta	Crítico
🟠 3	Ausência de criptografia HTTPS	5	4	4	80	Alto	Média/Alta	Alto
🟡 4	Falta de backup e plano de recuperação	4	4	4	64	Alto	Média/Alta	Médio
🟡 5	Falta de monitoramento e logs automáticos	4	3	4	48	Alto	Média/Alta	Médio
🟢 6	Códigos desatualizados e sem auditoria	3	3	3	27	Médio	Média	Baixo
🟢 7	Falta de treinamento e políticas de senha fraca	3	3	4	36	Médio	Média/Alta	Baixo
🟢 8	Indisponibilidade da plataforma (DDoS ou falha técnica)	4	3	3	36	Alto	Média	Baixo
🟡 9	Demora na resposta a incidentes	4	4	3	48	Alto	Média	Médio
🟡 10	Danos à imagem e reputação	5	3	3	45	Alto	Média	Médio