Curso **4NAADS_S**	Disciplina **CIBERSEGURANÇA E DEFESA CIBERNÉTICA**
Data **29/09/2025**	Professor **RONALDO ARAUJO**

INTEGRANTES

Anderson Yavi Fernandez – RA:24025678
Gabriel Gonçalves Pires – RA: 24026518
Isabela Nunes Zeferino – RA:24026460
Kaique Neres de Oliveira – RA:24026134
Luiz Felipe Galdino de Carvalho – RA: 2402656

INTRODUÇÃO

A matriz GUT (Gravidade, Urgência e Tendência) é uma metodologia amplamente utilizada na gestão de riscos para apoiar a priorização de ações corretivas e preventivas. Por meio da atribuição de pontuações a cada um desses critérios, é possível mensurar o impacto potencial de cada risco sobre o projeto e, assim, direcionar os esforços de mitigação de forma mais eficiente.

Nesta etapa, foi elaborada uma **tabela de Riscos x GUT** a partir dos riscos identificados na fase anterior do projeto. Cada risco foi avaliado quanto à sua **Gravidade (G)**, representando o impacto caso o evento ocorra; **Urgência (U)**, que indica o tempo disponível para agir antes que o risco se concretize; e **Tendência (T)**, que mede a probabilidade de crescimento ou agravamento do risco ao longo do tempo.

O produto da multiplicação desses três fatores (G x U x T) resultou na **pontuação de prioridade**, utilizada para classificar os riscos em ordem decrescente de criticidade. Essa análise permite identificar os pontos mais sensíveis do projeto e orientar a tomada de decisão quanto às ações de controle, mitigação e monitoramento necessárias.

Nº	Item	G	U	T	Prioridade

1	Vazamento de dados pessoais (sanções LGPD)	5	5	5	125
2	Implementação falha de autenticação e perfis de acesso	5	5	4	100
3	Falta de plano de segurança e LGPD	5	5	5	125
4	APIs mal protegidas (sem autenticação/autorização)	5	4	4	80
5	Exposição de dados sensíveis pelo chatbot	5	4	4	80
6	Falhas de configuração da nuvem (storage, permissões)	4	4	4	64
7	Indisponibilidade de serviços de nuvem (AWS/Azure)	4	3	4	48
8	Ataques cibernéticos (SQL Injection, XSS, brute force)	5	3	3	45
9	Ausência de plano de continuidade de negócio	4	4	4	64
10	Escopo mal definido → retrabalho e custos	4	3	3	36
11	Stakeholders não identificados corretamente	4	3	3	36
12	Rotatividade da equipe → perda de conhecimento crítico	3	3	3	
13	Mudanças frequentes nos requisitos	3	3	4	
14	Protótipos não validados → retrabalho	3	3	3	
15	Cobertura de testes insuficiente → falhas não detectadas	4	2	3	16
	Problemas no deploy em nuvem → indisponibilidade	4	3	3	
17	Treinamento insuficiente dos stakeholders	3	3	3	
18	Feedback ignorado → insatisfação do cliente	2	2	3	
19	Dependência de infraestrutura de terceiros (cloud, restaurantes)	4	3	3	
20	Controle de versão inadequado no repositório	3	3	3	
21	Código mal estruturado → difícil manutenção	3	3	3	
22	Chatbot treinado com dados incorretos ou incompletos	3	3	4	
23	Documentação incompleta ou desatualizada	2	2	3	
24	Resistência dos stakeholders/usuários à mudança	3	3	3	
25	Concorrência tecnológica (soluções já existentes)	3	2	3	
26	Falhas de energia ou infraestrutura local 4 3 3 27 Viés em modelos de Inteligência Artificial 3 3 4				
28	Mudanças legais/regulatórias (LGPD, segurança de dados)	4	4	4	
29	Falta de engajamento dos parceiros (restaurantes)	3	3	3	

CONCLUSÃO

A aplicação da matriz GUT possibilitou uma visão estruturada e objetiva dos principais riscos associados ao projeto. A análise evidenciou que os riscos com maior prioridade estão relacionados à segurança da informação e à conformidade com a LGPD, como o vazamento de dados pessoais, a falha na implementação de autenticação e perfis de acesso e a ausência de plano de segurança e conformidade legal. Esses riscos representam ameaças significativas tanto do ponto de vista técnico quanto regulatório, demandando ações imediatas de mitigação e monitoramento contínuo.

Outros riscos de prioridade intermediária, como falhas de configuração em ambientes de nuvem, indisponibilidade de serviços críticos, mudanças legais e regulatórias e ausência de plano de continuidade de negócio, também requerem atenção, sendo recomendável o estabelecimento de planos de contingência e estratégias de resposta rápida.

Por fim, riscos de menor prioridade, ainda que com impacto reduzido, devem ser acompanhados e revisados periodicamente, de modo a prevenir sua evolução para níveis críticos. Com essa priorização, o projeto passa a dispor de uma base sólida para o gerenciamento proativo de riscos, contribuindo para a redução de vulnerabilidades, aumento da confiabilidade operacional e alinhamento às exigências legais e de segurança da informação.

27
36
27
24
36
27
12
36
27
27
36
12
27
18
36
36
64
27