

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

Tabela de riscos x GUT

Trabalho de Cibersegurança e Defesa Cibernética: Tabela de riscos x GUT

Projeto Integrado 2025-2

Apresentado à Fundação Escola de Comércio

Álvares Penteado - FECAP

Orientador: Prof. Ronaldo Araújo

São Paulo

2025

Índice

Introdução	4
1. Matriz de Análise de Riscos x GUT.....	5
2. Conclusão.....	6

Introdução

Este documento apresenta a Matriz de Análise de Riscos do projeto Dashboard Interativo para a empresa Cannoli, desenvolvido no âmbito do Projeto Integrador chamado InovaTech.

O estudo tem como objetivo identificar, avaliar e classificar os riscos relacionados à segurança da informação do sistema, garantindo maior confiabilidade, disponibilidade e integridade dos dados.

A análise foi elaborada a partir dos riscos, vulnerabilidades e ameaças levantados na primeira etapa do trabalho, seguindo as diretrizes do NIST Cybersecurity Framework e utilizando o método GUT (Gravidade, Urgência e Tendência) para priorização.

Com base nessas informações, foram atribuídas pontuações de probabilidade e impacto para cada risco, resultando na definição de níveis de criticidade distribuídos em quatro zonas de decisão — Tolerável, Significativo, Sério e Intolerável — conforme o modelo proposto pelo professor.

Essa metodologia permite compreender de forma estruturada a postura de segurança cibernética do projeto, orientando ações preventivas e decisões estratégicas para mitigar falhas e fortalecer o ambiente do sistema.

1. Matriz de Análise de Riscos x GUT

I	Categor	Risco	Prob	Impacto	Nível	Zona	Grav	Urg.	Tendêñ	G x U x	Priorida
1	INTERNA	Pedido de Demissão Voluntário	1	4	4	Tolerável	2	2	2	8	8
2	INTERNA	Falta de mapeamento de sistemas e usuários com acesso	3	4	12	Sério	4	3	3	36	36
3	INTERNA	Risco de vazamento de dados sensíveis de clientes e administradores	4	5	20	Intolerável	5	5	5	125	125
4	INTERNA	Falta de definição sobre quem administra permissões de acesso	3	3	9	Sério	3	3	2	18	18
5	EXTERNA	Dependência de servidores externos (cloud)	2	4	8	Significativo	4	2	3	24	24
6	INTERNA	Ausência de políticas formais de segurança e controle de acesso	4	4	16	Intolerável	4	4	4	64	64
7	INTERNA	Falta de análise de impacto em ataques cibernéticos	3	5	15	Sério	5	4	4	80	80
8	INTERNA	Falta de registro de procedimentos para resposta e mitigação	3	4	12	Sério	4	3	3	36	36
9	INTERNA	Falha na autenticação de usuários	4	4	16	Intolerável	4	5	4	80	80
10	INTERNA	Ausência de criptografia nas comunicações (sem HTTPS/SSL)	4	5	20	Intolerável	5	5	5	125	125
11	INTERNA	Códigos sem auditoria de segurança	3	3	9	Sério	3	3	3	27	27
12	INTERNA	Falta de firewall e antivírus corporativo	5	5	25	Intolerável	5	5	5	125	125
13	INTERNA	Falta de ferramentas de monitoramento	4	4	16	Intolerável	4	4	4	64	64
14	INTERNA	Logs desatualizados e não revisados	3	3	9	Sério	3	3	3	27	27
15	INTERNA	Falta de plano formal de resposta a incidentes	4	4	16	Intolerável	4	5	4	80	80
16	INTERNA	Ausência de medidas de mitigação (bloqueio de IPs, etc.)	3	4	12	Sério	4	4	3	48	48
17	INTERNA	Falta de política de backup automático e testes de restauração	4	5	20	Intolerável	5	5	5	125	125
18	EXTERNA	Falta de comunicação com usuários em caso de falhas	3	3	9	Sério	3	3	2	18	18

2. Conclusão

Com base na matriz apresentada, foi possível identificar e avaliar os principais riscos que podem impactar a operação e a segurança do Dashboard Interativo desenvolvido pelo projeto InovaTech. A aplicação da metodologia GUT, aliada à análise de probabilidade e impacto, proporcionou uma visão clara das prioridades de mitigação e controle.

Os resultados indicam que parte dos riscos classificados como sérios ou intoleráveis exigem a implementação de novos controles, como firewall, criptografia, políticas de backup e auditorias de código. Já os riscos de menor criticidade pode ser mantidos sob monitoramento contínuo e revisão periódica dos controles existentes.

Dessa forma, o estudo reforça a importância de uma gestão proativa de segurança da informação, assegurando que o projeto InovaTech mantenha sua plataforma robusta, confiável e alinhada às boas práticas de cibersegurança, fortalecendo a confiança dos usuários e parceiros da solução.