



Curso <b>4NAADS_S</b>	Disciplina <b>Ciberseauranca e Defesa Cibernética</b>
Data <b>16/10/2025</b>	Alunos <b>ANDREIA SILVA, GUILHERME MENDES, LUAN MEIRELES, MATHEUS FRANCISCO</b>

## Sumário

Levantamento de Riscos, Vulnerabilidades e Ameaças.....	2
Introdução .....	2
1. Identify (ID) – Identificar .....	2
2. Protect (PR) – Proteger .....	2
3. Detect (DE) – Detectar .....	2
4. Respond (RS) – Responder.....	3
5. Recover (RC) – Recuperar .....	3
6. Matriz GUT .....	4
7. Conclusão .....	4

## **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

### **Introdução**

O presente documento tem como objetivo apresentar o levantamento de riscos, vulnerabilidades e ameaças do projeto Cannoli, seguindo como referência o NIST Cybersecurity Framework, amplamente utilizado para estruturar a gestão de segurança da informação.

O NIST divide as práticas de cibersegurança em cinco funções principais: Identify (Identificar), Protect (Proteger), Detect (Detectar), Respond (Responder) e Recover (Recuperar). A partir dessas etapas, é possível entender o ambiente, aplicar controles, detectar falhas, agir diante de incidentes e restaurar o sistema quando necessário.

### **1. Identify (ID) – Identificar**

Objetivo: entender os ativos, riscos, processos e dados do projeto.

ID.AM – Gerenciamento de Ativos:

- Falta de mapeamento de todos os sistemas e usuários com acesso ao sistema Cannoli.
- Risco de vazamento de dados sensíveis de clientes e administradores.

ID.BE – Ambiente de Negócios:

- Falta de definição clara sobre quem administra as permissões de acesso.
- Dependência de servidores externos (cloud).

ID.GV – Governança:

- Ausência de políticas formais de segurança e controle de acesso.
- Falta de plano de continuidade em caso de incidentes.

ID.RA – Avaliação de Risco:

- Falta de análise de impacto em caso de ataque cibernético.
- Ameaça de perda de dados ou exposição indevida.

ID.RM – Estratégia de Gerenciamento de Risco:

- Falta de registro de procedimentos formais para resposta e mitigação.

### **2. Protect (PR) – Proteger**

Objetivo: implementar medidas para evitar ou reduzir danos em caso de incidentes.

PR.AC – Controle de Acesso:

- Falhas na autenticação de usuários e ausência de autenticação multifator.
- Risco de acesso não autorizado ao painel administrativo.

PR.AT – Conscientização e Treinamento:

- Falta de orientação sobre senhas seguras e boas práticas de segurança.

PR.DS – Segurança de Dados:

- Ausência de criptografia (sem HTTPS/SSL).
- Risco de exposição de informações durante comunicações.

PR.IP – Processos de Proteção:

- Falta de revisão periódica de permissões e registros de acesso.

PR.MA – Manutenção:

- Ausência de auditorias e atualizações regulares de segurança.

PR.PT – Tecnologia de Proteção:

- Falta de firewall e antivírus corporativo configurados.

### **3. Detect (DE) – Detectar**

Objetivo: monitorar o sistema e identificar incidentes rapidamente.

DE.CM – Monitoramento Contínuo:

- Falta de ferramentas de monitoramento de acessos e falhas.

- Ausência de alertas automáticos para atividades suspeitas.

DE.DP – Processos de Detecção:

- Incidentes podem não ser detectados a tempo devido a logs desatualizados.
- Ameaça: ataque não identificado pode causar vazamento de dados.

#### 4. Respond (RS) – Responder

Objetivo: agir de forma rápida e eficaz quando um incidente é detectado.

RS.RP – Planejamento de Resposta:

- Falta de plano formal de resposta a incidentes.

RS.CO – Comunicação:

- Ausência de canal de comunicação definido para relatar incidentes.

RS.AN – Análise:

- Falta de procedimento para análise de causa e impacto de ataques.

RS.MI – Mitigação:

- Falta de medidas imediatas para conter ataques e reduzir impacto.

RS.IM – Melhorias:

- Falta de registro histórico para aprendizado e prevenção futura.

#### 5. Recover (RC) – Recuperar

Objetivo: restaurar dados e operações após um incidente.

RC.RP – Planejamento de Recuperação:

- Falta de política de backup automático e testes de restauração.

RC.IM – Melhorias:

- Ausência de plano documentado de recuperação pós-incidente.

RC.CO – Comunicação:

- Falta de comunicação transparente com usuários após falhas.
- Risco: perda de confiança e danos à reputação.

## 6. Matriz GUT

Interpretação da Matriz:

- Vermelho | Crítico (100–125): risco que exige ação imediata.
- Laranja | Alto (70–99): precisa de plano de mitigação a curto prazo.
- Amarelo | Médio (40–69): monitoramento contínuo e prevenção.
- Verde | Baixo (até 39): riscos menores, podem ser aceitos temporariamente.

Nº	Risco Identificado	Gravidade (G)	Urgência (U)	Tendência (T)	Índice GUT (G×U×T)
1	Vazamento de dados sensíveis	5	5	5	125
2	Acesso não autorizado ao painel	5	5	4	100
3	Ausência de criptografia HTTPS	5	4	4	80
4	Falta de backup e plano de recuperação	4	4	4	64
5	Falta de monitoramento e logs automáticos	4	3	4	48
6	Códigos desatualizados e sem auditoria	3	3	3	27
7	Falta de treinamento e políticas de senha fraca	3	3	4	36
8	Indisponibilidade da plataforma (DDoS ou falha técnica)	4	3	3	36
9	Demora na resposta a incidentes	4	4	3	48
10	Danos à imagem e reputação	5	3	3	45

## 7. Conclusão

Com base na análise realizada, foram identificados os principais riscos, vulnerabilidades e ameaças relacionados ao projeto Cannoli. O uso do NIST Cybersecurity Framework possibilitou organizar o levantamento de forma estruturada, dividindo as ações em cinco etapas: Identify, Protect, Detect, Respond e Recover.

A Matriz GUT foi utilizada para priorizar os riscos, indicando os pontos mais críticos que exigem atenção imediata, como a proteção de dados sensíveis, autenticação de acesso e falta de backups. Essa integração entre o NIST e a GUT oferece uma visão ampla e prática da segurança cibernética, contribuindo para um ambiente digital mais estável e confiável.