# Cibersegurança e Defesa Cibernética

# Entrega 1 – Projeto Interdisciplinar

**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: 24026568**

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

Objetivo: Compreender riscos, ativos, pessoas, dados e processos.

* **ID.AM (Gerenciamento de Ativos):** Dependência de infraestrutura de terceiros (cloud, restaurantes).
* **ID.BE (Ambiente de Negócios):** Escopo mal definido → retrabalho e aumento de custos.
* **ID.GV (Governança):** Falta de plano de segurança e LGPD; ausência de plano de continuidade de negócio.
* **ID.RA (Avaliação de Risco):** Protótipos não validados; feedback ignorado; mudanças frequentes nos requisitos.
* **ID.RM (Estratégia de Gerenciamento de Risco):** Stakeholders não identificados corretamente; rotatividade da equipe.

### **2. Protect (PR) – Proteger**

Objetivo: Implementar salvaguardas para limitar ou conter impactos de eventos cibernéticos.

* **PR.AC (Controle de Acesso):** Implementação falha de autenticação e perfis de acesso; APIs mal protegidas.
* **PR.AT (Conscientização e Treinamento):** Treinamento insuficiente dos stakeholders.
* **PR.DS (Segurança de Dados):** Exposição de dados sensíveis pelo chatbot; falhas de configuração da nuvem (storage, permissões).
* **PR.IP (Processos e Procedimentos de Proteção da Informação):** Controle de versão inadequado no repositório; documentação incompleta/desatualizada.
* **PR.MA (Manutenção):** Código mal estruturado → difícil manutenção.
* **PR.PT (Tecnologia de Proteção):** Cobertura de testes insuficiente.

### **3. Detect (DE) – Detectar**

Objetivo: Desenvolver atividades para identificar a ocorrência de eventos de segurança.

* **DE.CM (Monitoramento Contínuo de Segurança):** Falhas não detectadas em testes.
* **DE.DM (Processos de Detecção):** Chatbot treinado com dados incorretos → decisões erradas.

### **4. Respond (RS) – Responder**

Objetivo: Desenvolver planos para agir diante de incidentes detectados.

* **RS.RP (Planejamento de Resposta):** Como a organização vai se preparar, garantindo que existam planos claros de resposta.
* **RS.CO (Comunicação):** Feedback ignorado → insatisfação do cliente.
* **RS.AN (Análise):** Avaliação de ataques cibernéticos (injeção SQL, brute force, XSS).
* **RS.MI (Mitigação):** Vazamento de dados pessoais (sanções LGPD).
* **RS.IM (Melhorias):** Após o sistema completo, realizar os devidos ajustes para mantê-lo sempre funcionando.

### **5. Recover (RC) – Recuperar**

Objetivo: Restaurar serviços após incidentes e melhorar resiliência.

* **RC.RP (Planejamento de Recuperação):** Falhas de energia ou infraestrutura durante testes/implantação.
* **RC.IM (Melhorias):** Ajustes após indisponibilidade em nuvem ou concorrência tecnológica.
* **RC.CO (Comunicação):** Engajamento com stakeholders após falhas e resistências.

| **Nº** | **Item (Risco / Vulnerabilidade / Ameaça)** | **G** | **U** | **T** | **Prioridade (G×U×T)** |
| --- | --- | --- | --- | --- | --- |
| 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 | 27 |
| 13 | Mudanças frequentes nos requisitos | 3 | 3 | 4 | 36 |
| 14 | Protótipos não validados → retrabalho | 3 | 3 | 3 | 27 |
| 15 | Cobertura de testes insuficiente → falhas não detectadas | 4 | 2 | 3 | 24 |
| 16 | Problemas no deploy em nuvem → indisponibilidade | 4 | 3 | 3 | 36 |
| 17 | Treinamento insuficiente dos stakeholders | 3 | 3 | 3 | 27 |
| 18 | Feedback ignorado → insatisfação do cliente | 2 | 2 | 3 | 12 |
| 19 | Dependência de infraestrutura de terceiros (cloud, restaurantes) | 4 | 3 | 3 | 36 |
| 20 | Controle de versão inadequado no repositório | 3 | 3 | 3 | 27 |
| 21 | Código mal estruturado → difícil manutenção | 3 | 3 | 3 | 27 |
| 22 | Chatbot treinado com dados incorretos ou incompletos | 3 | 3 | 4 | 36 |
| 23 | Documentação incompleta ou desatualizada | 2 | 2 | 3 | 12 |
| 24 | Resistência dos stakeholders/usuários à mudança | 3 | 3 | 3 | 27 |
| 25 | Concorrência tecnológica (soluções já existentes) | 3 | 2 | 3 | 18 |
| 26 | Falhas de energia ou infraestrutura local | 4 | 3 | 3 | 36 |
| 27 | Viés em modelos de Inteligência Artificial | 3 | 3 | 4 | 36 |
| 28 | Mudanças legais/regulatórias (LGPD, segurança de dados) | 4 | 4 | 4 | 64 |
| 29 | Falta de engajamento dos parceiros (restaurantes) | 3 | 3 | 3 | 27 |