# 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. Riscos (eventos que podem impactar negativamente o projeto)**

* Escopo mal definido → gera retrabalho e aumento de custos.
* Cronograma irrealista → atraso na entrega.
* Stakeholders não identificados corretamente → requisitos incompletos ou conflitantes.
* Rotatividade da equipe → perda de conhecimento crítico.
* Mudanças frequentes nos requisitos.
* Protótipos não validados → retrabalho na fase de desenvolvimento.
* Cobertura de testes insuficiente → falhas não detectadas.
* Problemas no deploy em nuvem → indisponibilidade temporária.
* Treinamento insuficiente dos stakeholders → baixa adoção da solução.
* Feedback ignorado → insatisfação do cliente.
* Dependência de infraestrutura de terceiros (cloud, restaurantes) → risco de indisponibilidade.

**2. Vulnerabilidades (fragilidades internas do projeto/sistema que podem ser exploradas)**

* Falta de plano de segurança e LGPD.
* Falhas de configuração da nuvem (storage, permissões).
* Controle de versão inadequado no repositório.
* APIs mal protegidas (sem autenticação/autorização adequadas).
* Implementação falha de autenticação e perfis de acesso.
* Código mal estruturado → difícil manutenção e suscetível a erros.
* Chatbot treinado com base em dados incorretos ou incompletos.
* Exposição de dados sensíveis pelo chatbot.
* Documentação incompleta ou desatualizada.
* Ausência de plano de continuidade de negócio.

**3. Ameaças (fatores externos que podem explorar vulnerabilidades ou impactar o projeto)**

* Ataques cibernéticos (injeção SQL, XSS, brute force em login).
* Vazamento de dados pessoais → sanções por LGPD.
* Indisponibilidade de serviços de nuvem (falha da AWS, Azure etc.).
* Resistência dos stakeholders/usuários à mudança → baixa adesão.
* Concorrência tecnológica (soluções já existentes no mercado).
* Falhas de energia ou infraestrutura local durante testes/implantação.
* Viés em modelos de Inteligência Artificial → decisões incorretas.
* Interrupções por mudanças legais/regulatórias (LGPD, segurança de dados).
* Falta de engajamento dos parceiros (restaurantes) → impacto na validação.

Assim temos:

* **Riscos** = cenários possíveis que podem acontecer.
* **Vulnerabilidades** = pontos fracos internos.
* **Ameaças** = fatores externos que podem explorar essas vulnerabilidades.