GT-IR: We Got Hacked!
Simulador de treinamento para aprendizado de resposta a incidentes

Coordenador: Prof. Dr. Luciano Ignaczak

Tópicos Abordados

1. We Got Hacked!
2. Projeto de Extensão
3. Resultados

1. We Got Hacked!

- Jogo de simulação no formato *single-player* disponível como aplicação *web;*
- Inspirado em uma rotina de um SOC;
- 3 fases / incidentes:
  - (1) pichação de site;
  - (2) ransomware;
  - (3) vazamento de dados.

1. We Got Hacked! – Equipe do SOC

Raquel Garcia Hent

Gerente

Tiago Nogueira Vatto

Analista Júnior

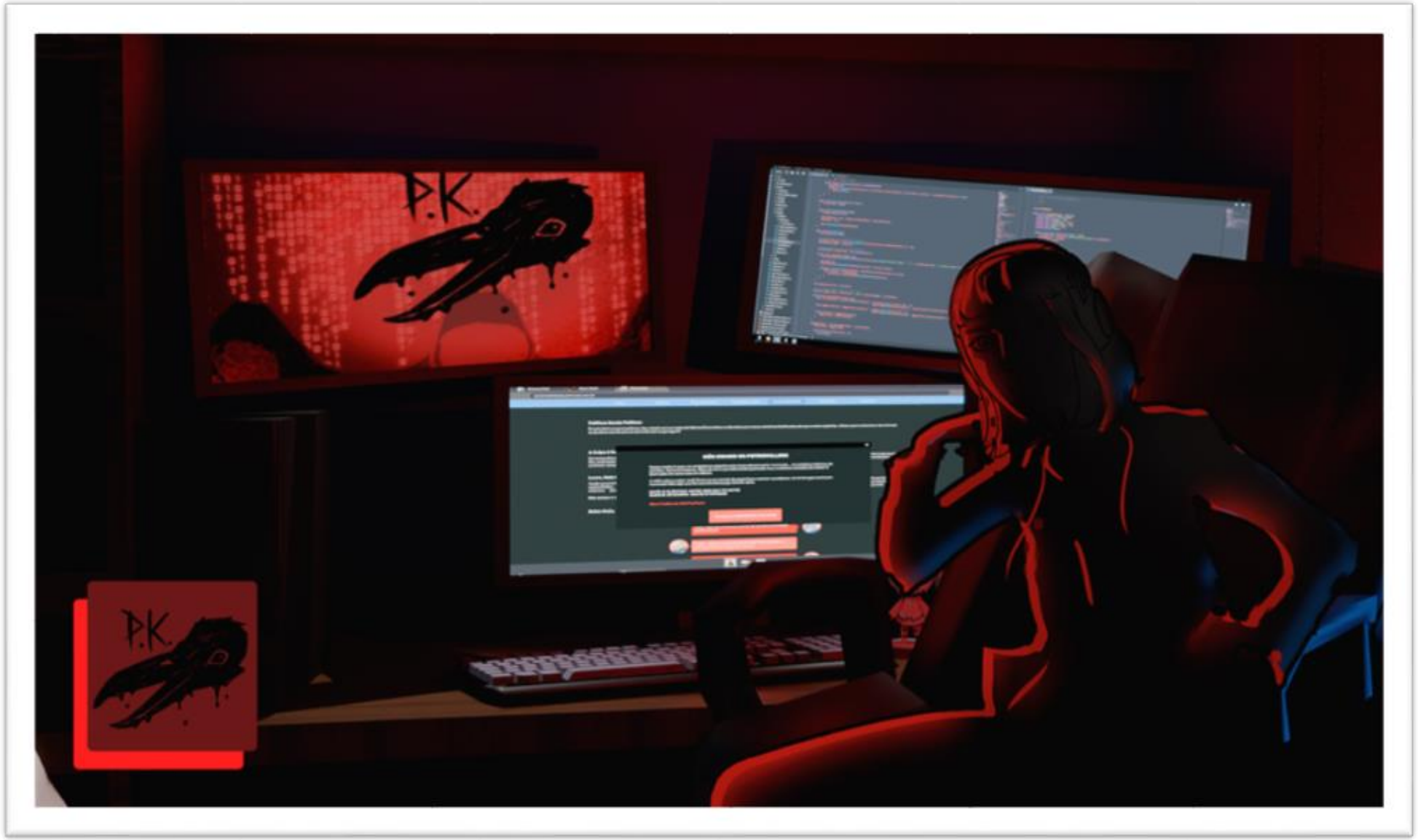
Rafael Medina Oliveira

Analista Pleno

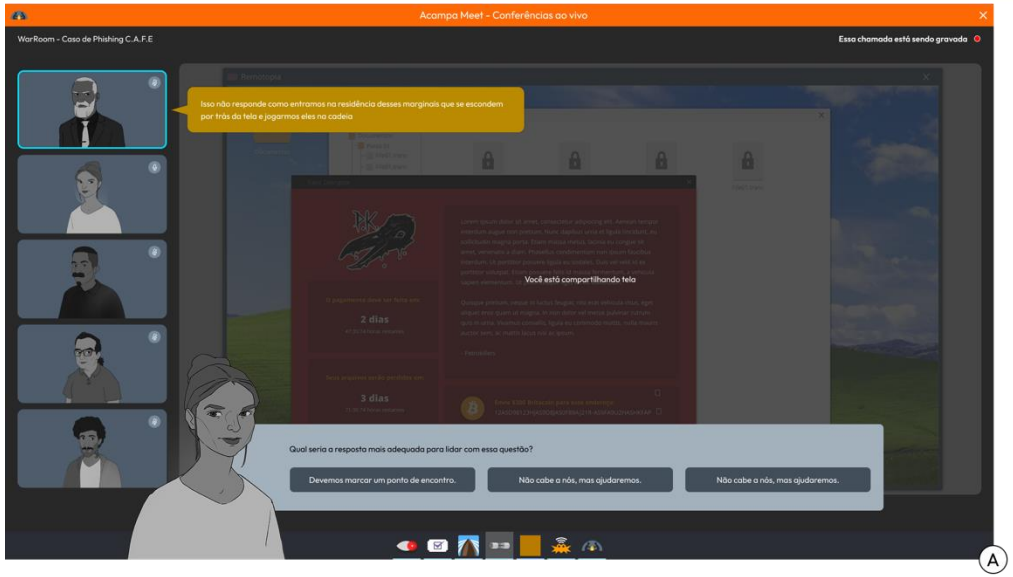
Eduardo Pontes Rodrigues

Analista Sênior

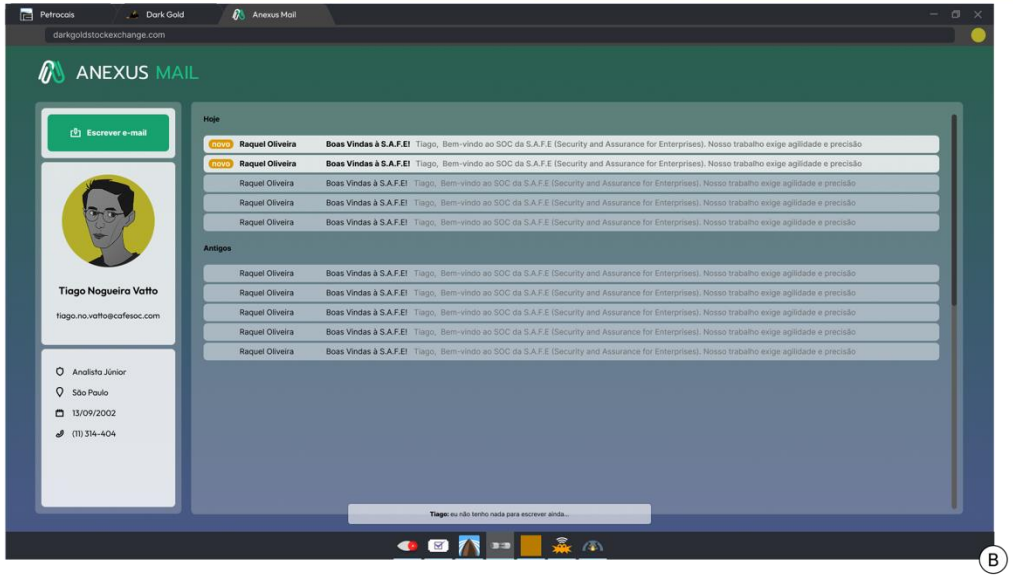
1. We Got Hacked! – APT 171 - Petrokillers



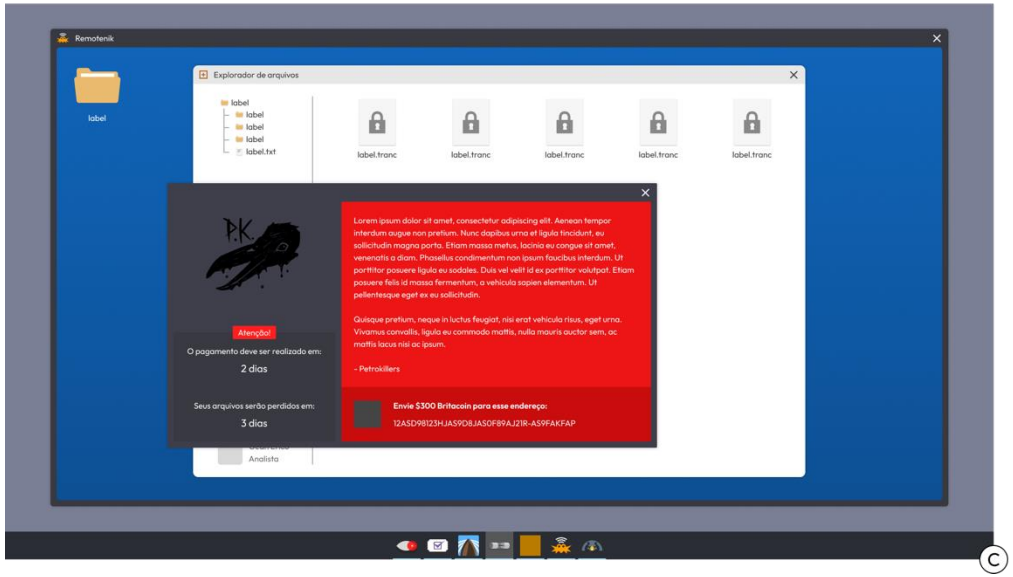
1. We Got Hacked! – Ferramentas



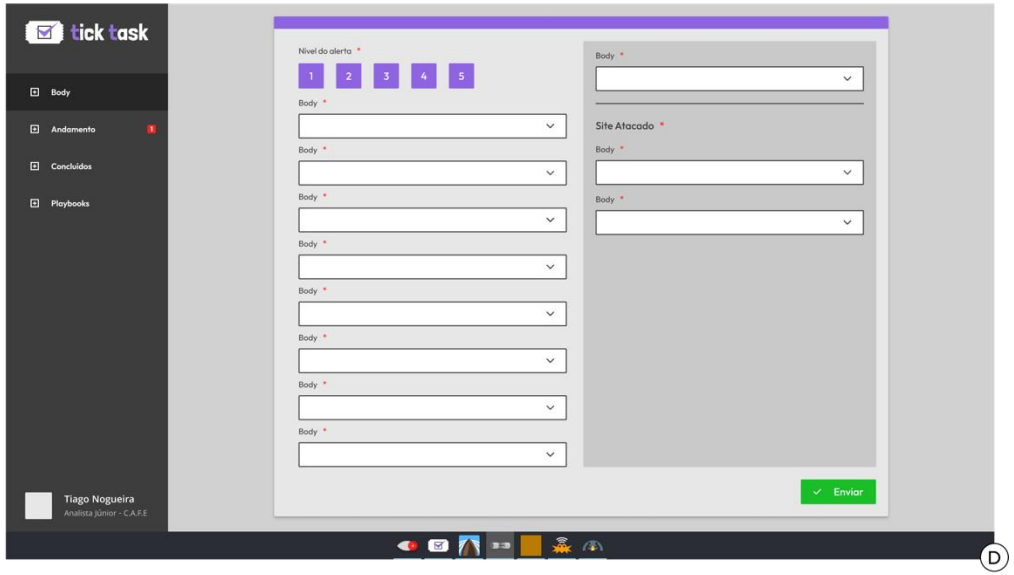
A



B



C



D

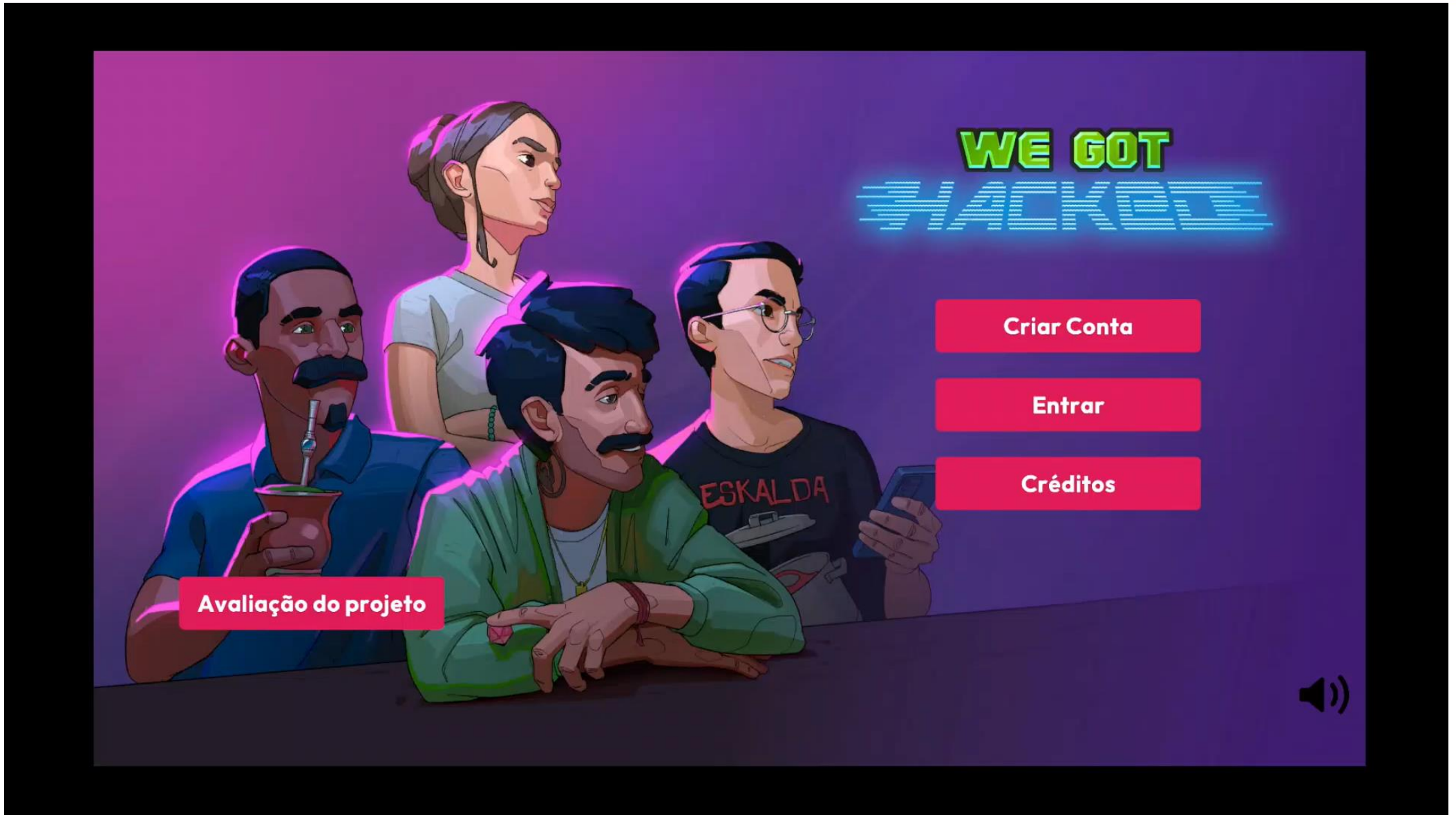
2. Extensão do Projeto

- Melhorias implementadas com base no projeto de extensão proposto pelo GT-IR e no feedback obtido com os residentes do Programa Hackers do Bem;
- Os aprimoramentos no jogo contemplam:
  - Melhorias na estrutura do jogo;
  - Avanços no game design e na arte;
  - Inserção de novos elementos educacionais.

2. Extensão do Projeto – Estrutura do Jogo

Melhoria	Origem	Situação
Cadastro com confirmação por e-mail	*Feedback* dos Residentes	Concluída
Ferramenta para reset de senha	*Feedback* dos Residentes	Concluída
Salvamento do progresso	*Feedback* dos Residentes	Concluída
Documentação técnica das melhorias	Projeto Extensão (4º objetivo)	Concluída

2. Extensão do Projeto – Estrutura do Jogo

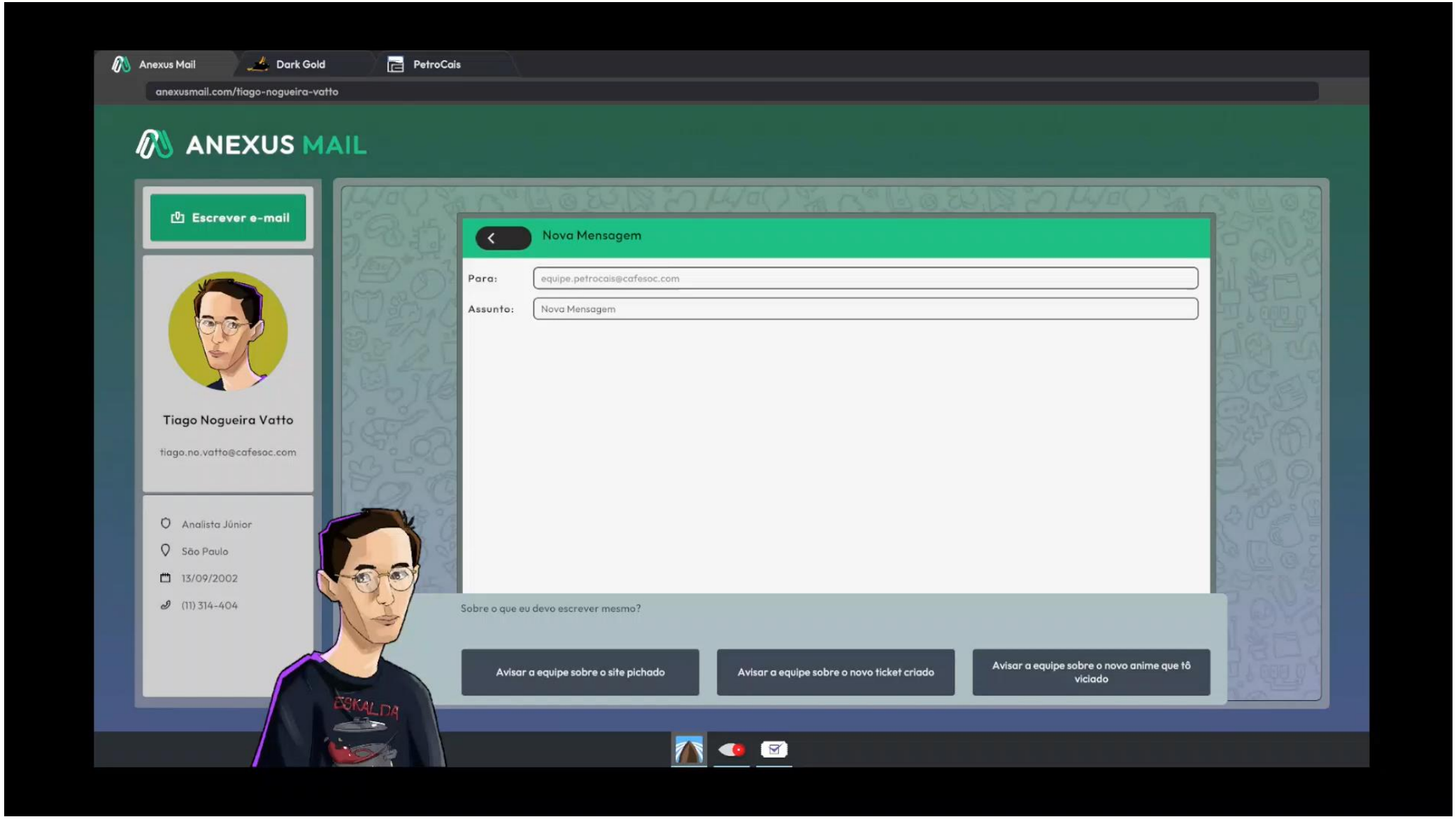


2. Extensão do Projeto – Game Design e Arte

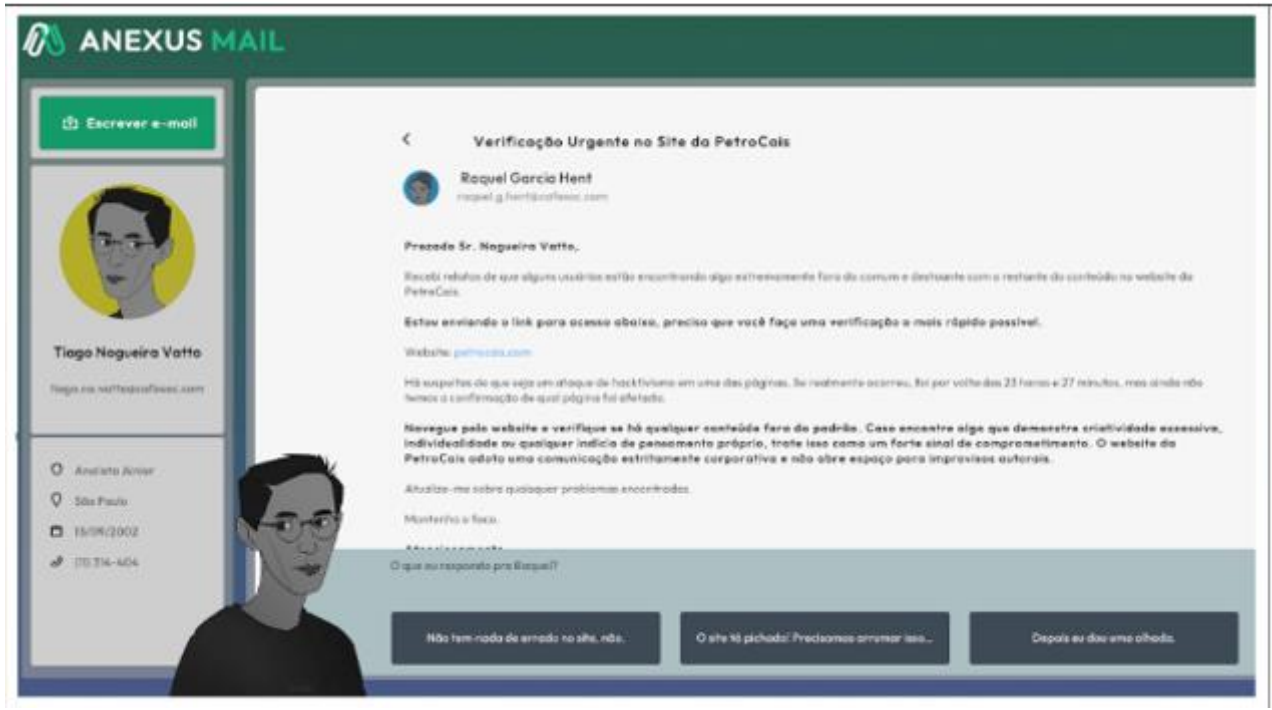
Melhoria	Origem	Situação
Melhoria da cutscene inicial	*Feedback* dos Residentes	Concluída
Melhoria nas cutscenes intermediárias e finais	Projeto de Extensão (1º e 2º objetivo)	Concluída
Refinamento estético das aplicações e dos personagens	Projeto de Extensão (1º objetivo)	Concluída
Alertar quando o preço da ação é modificado	*Feedback* dos Residentes	Concluída
Adicionar sons em alertas e ações	*Feedback* dos Residentes e Projeto de Extensão (1º objetivo)	Concluída
Adicionar trilha sonora ambiente	*Feedback* dos Residentes e Projeto de Extensão (1º objetivo)	Concluída
Aumentar tamanho das fontes	*Feedback* dos Residentes	Concluída
Correção de erros nos textos	*Feedback* dos Residentes	Concluída
Melhorias de contexto nos textos	Projeto de Extensão (2º objetivo)	Concluída
Rota alternativa	Projeto de Extensão (2º objetivo)	Concluída

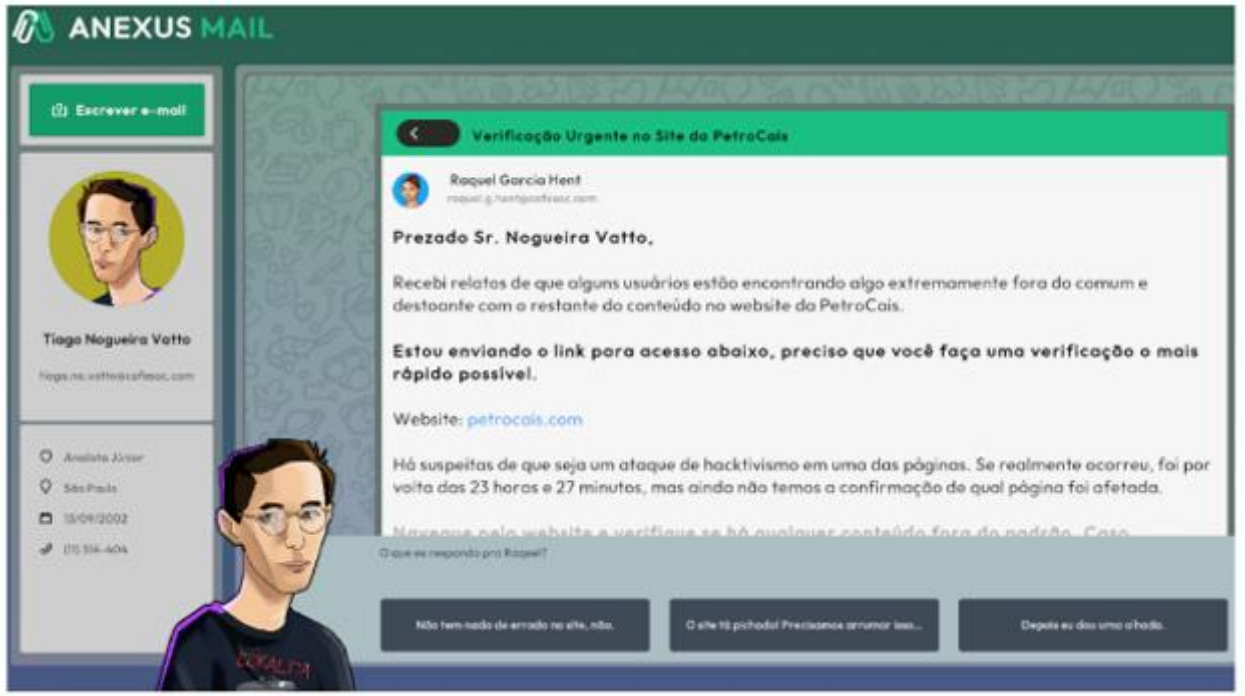
2. Extensão do Projeto – Game Design e Arte

2. Extensão do Projeto – Game Design e Arte



2. Extensão do Projeto – Game Design e Arte



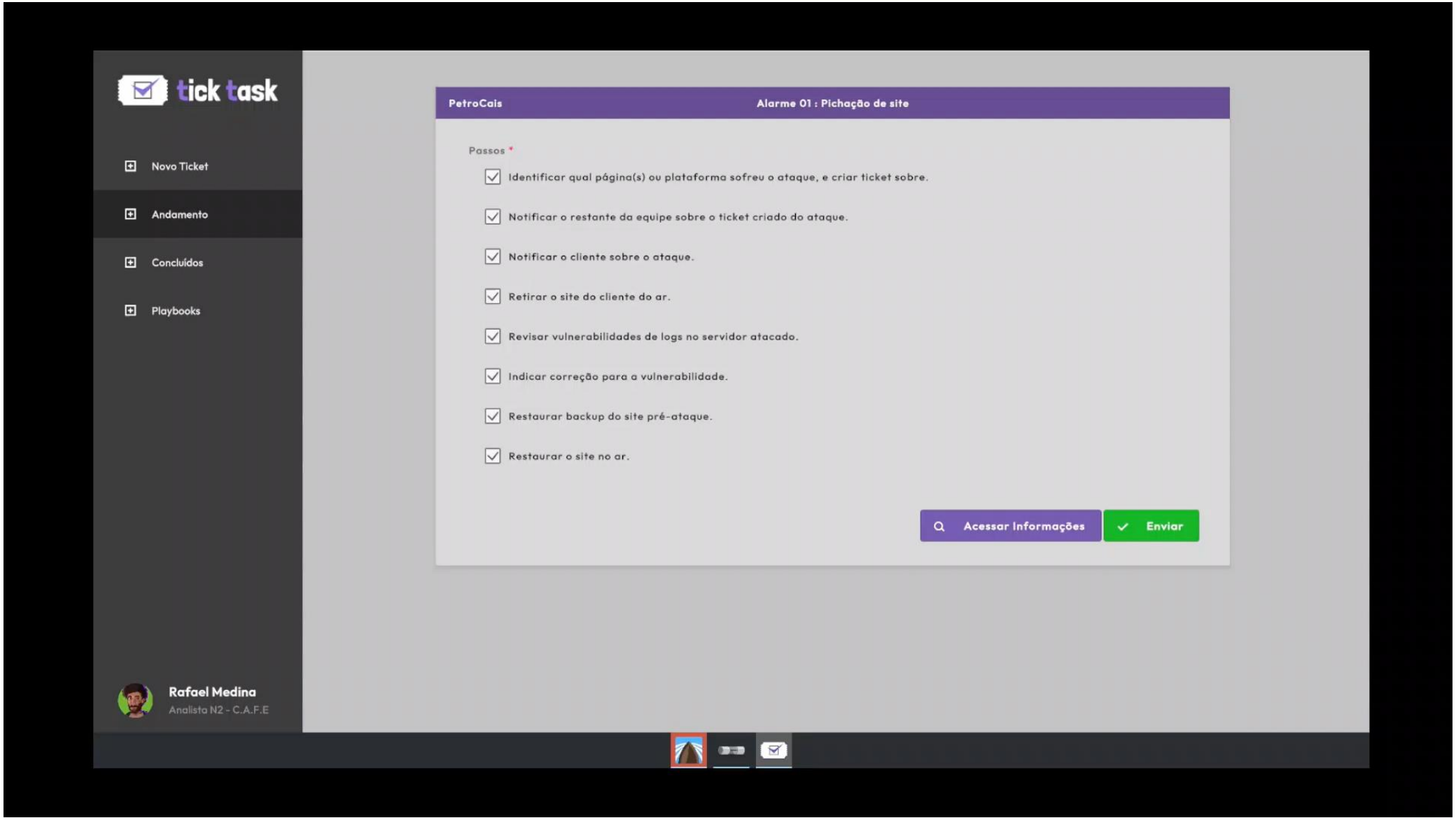


2. Extensão do Projeto – Conteúdo Educacional

Fase	Incidente	Tópicos das aulas
1	Pichação de sites	SOC
		SIEM
		Agentes de ameaça e grupos hacktivistas
		Pichação de sites
2	*Ransomware*	Códigos maliciosos
		Indicadores de comprometimento (IoCs)
		Ransomware
3	Vazamento de dados	Comunicação de incidentes
		Ferramenta de inspeção de pacotes
		Vazamento de dados

2. Extensão do Projeto – Conteúdo Educacional

2. Extensão do Projeto – Conteúdo Educacional



2. Extensão do Projeto – Não implementados

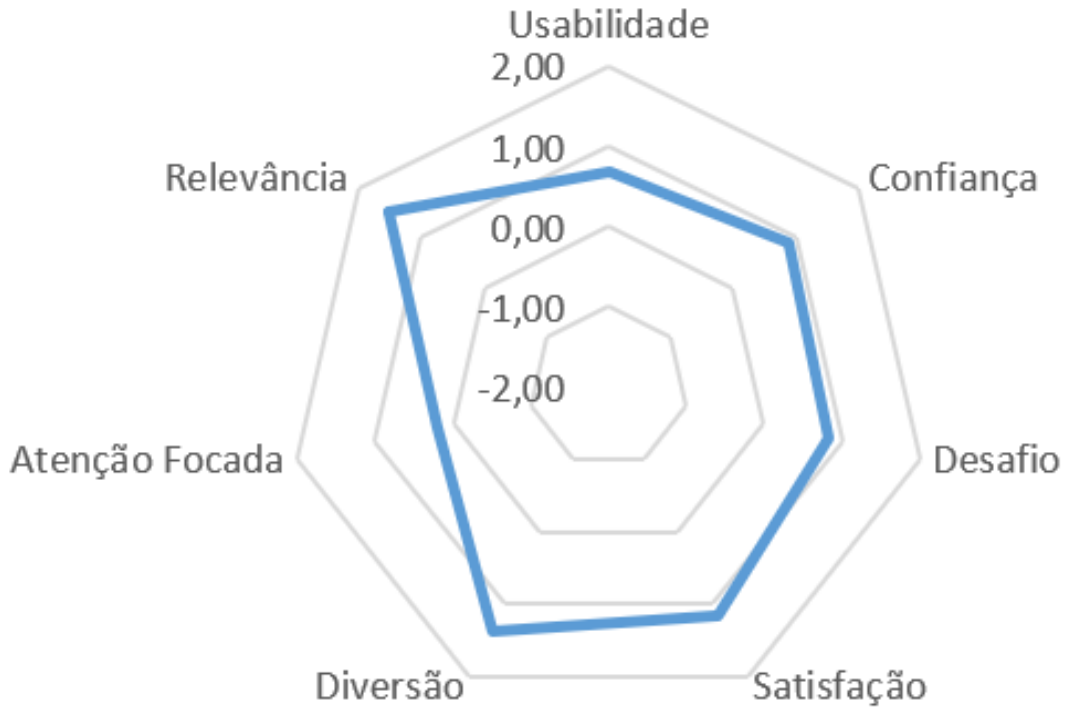
Objetivo	Melhoria	Origem	Situação
Melhorias de *game design* e arte	Melhorar o feedback após cada fase ou quando se comete um erro	*Feedback* dos Residentes	Não foram implementados
	Possibilidade de rever diálogos na *cutscene* de abertura		
	Melhorar o scroll e a navegação de telas		
	Criação de trilhas de aprendizagem customizadas,		
	Seleção de níveis de dificuldade		
Melhorias estruturais	Portabilidade para dispositivos móveis		
	Modos colaborativos e competitivos		

3. Resultados – Avaliação com os residentes

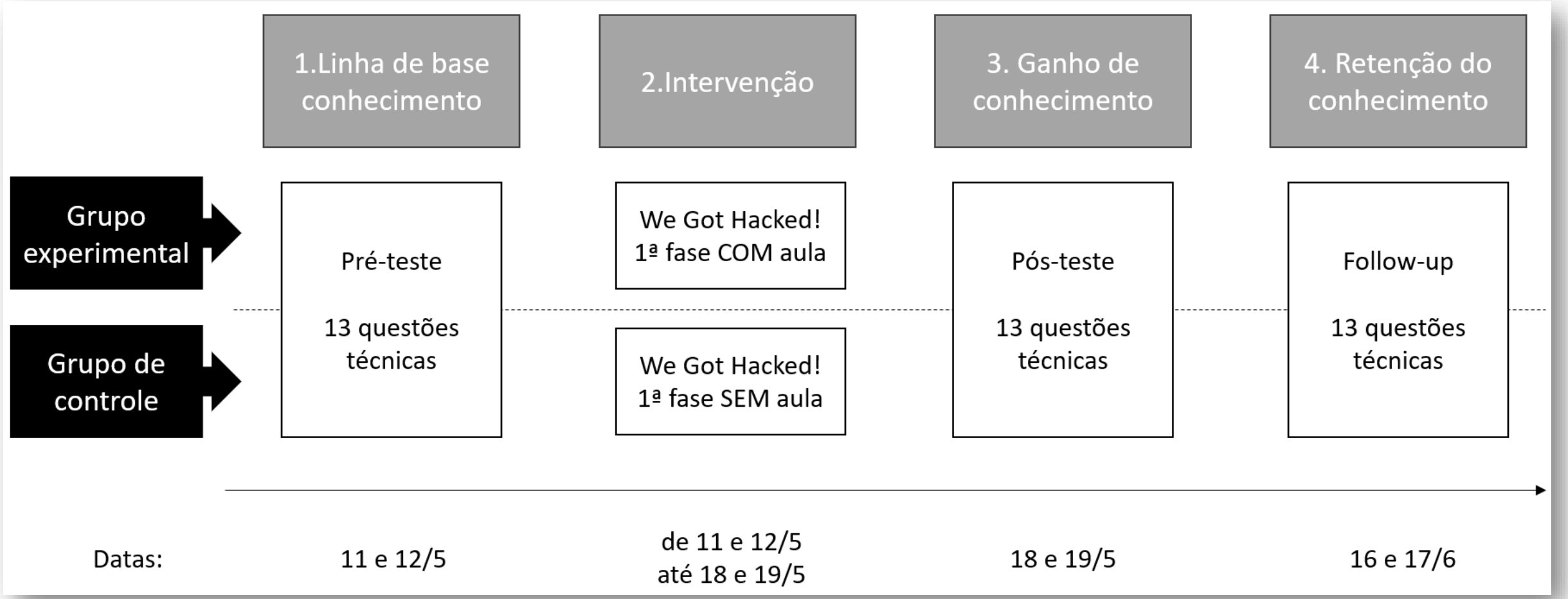
Etapa	Residentes
Residentes convidados	29
Entraram no grupo	28
Jogaram o We Got Hacked!	27
Responderam sobre a experiência (MEEGA+)	25

3. Resultados – Avaliação com os residentes

Médias da avaliação por dimensão	
Dimensão	Média
Usabilidade	0,68
Confiança	0,88
Desafio	0,84
Satisfação	1,18
Diversão	1,38
Atenção Focada	0,21
Relevância	1,53



3. Resultados – Avaliação com alunos UNISINOS



3. Resultados – Avaliação com alunos UNISINOS

Comparativo de acertos: Grupo de Controle e Grupo Experimental					
Grupo	Alunos	Pré-teste		Pós-teste	
		Acertos	%	Acertos	%
Controle	8	76	73,1%	89	85,6%
Experimental	10	105	80,8%	116	89,2%
Total	**18**	**181**	**77,4%**	**205**	**87,6%**


保安

Conheça o ..
We Got Hacked!