



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



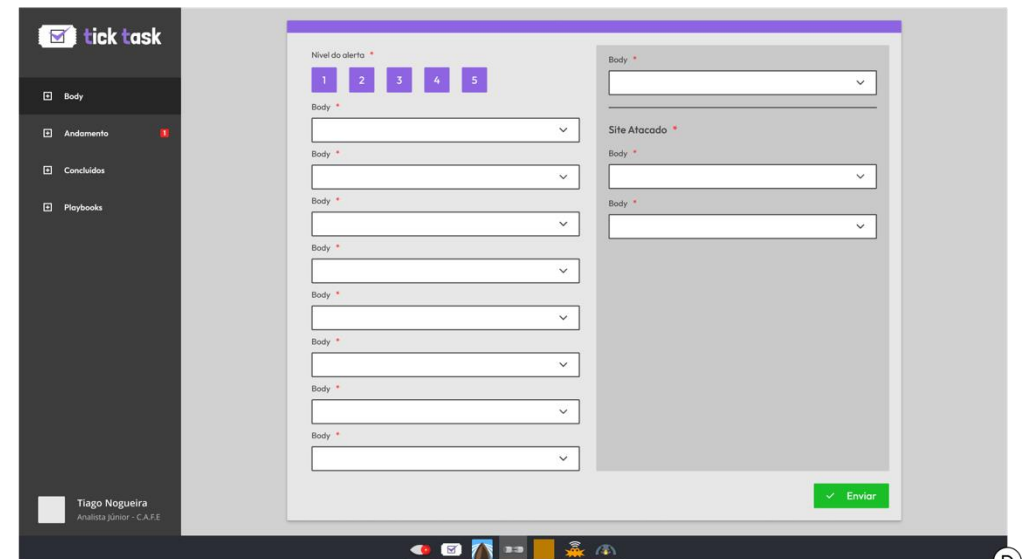
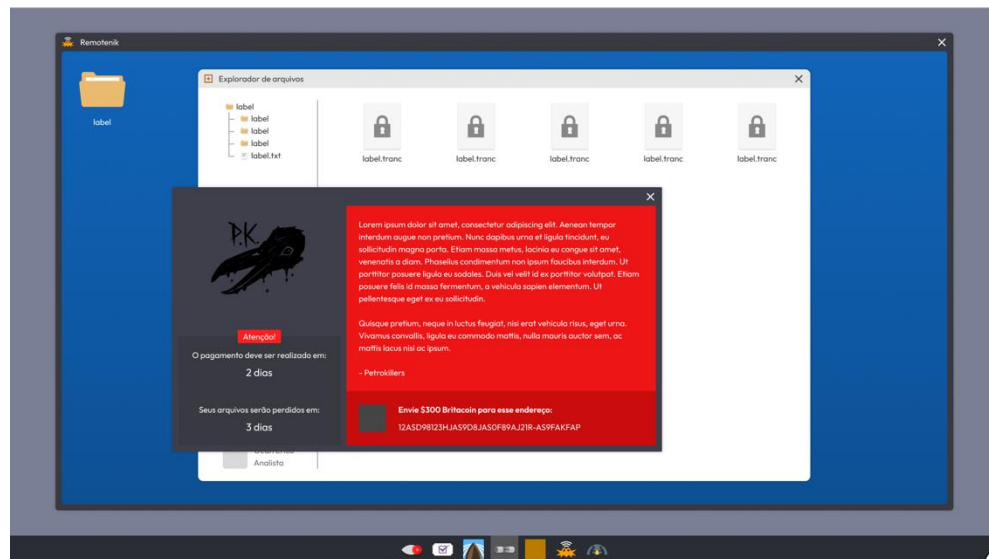
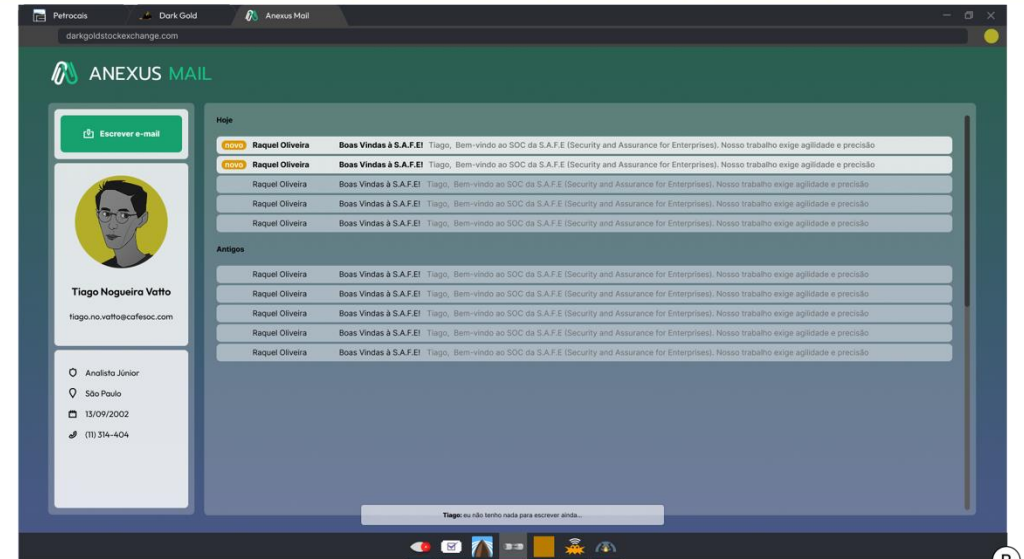
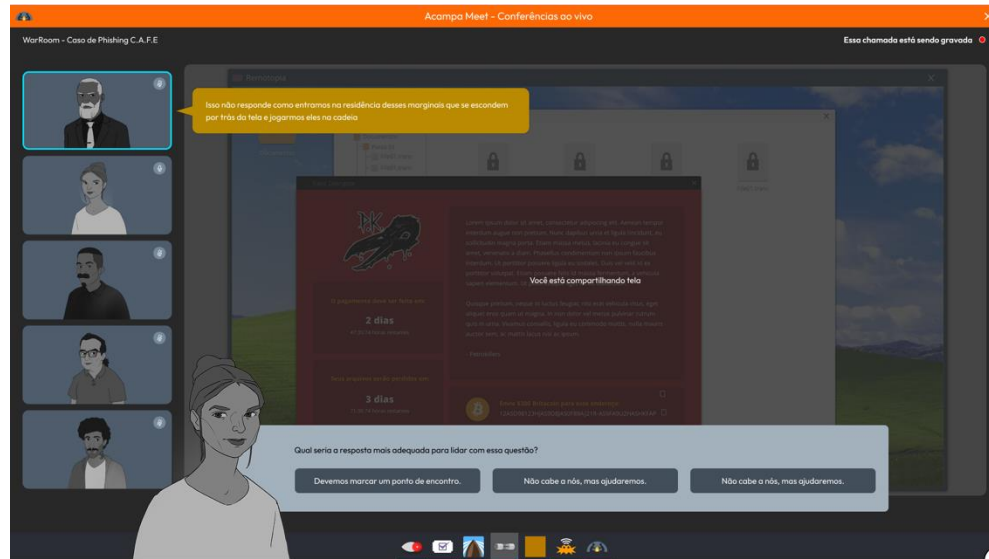
Eduardo Pontes Rodrigues

Analista Sênior

1. We Got Hacked! – APT 171 - Petrokillers



1. We Got Hacked! – Ferramentas



2. Extensão do Projeto

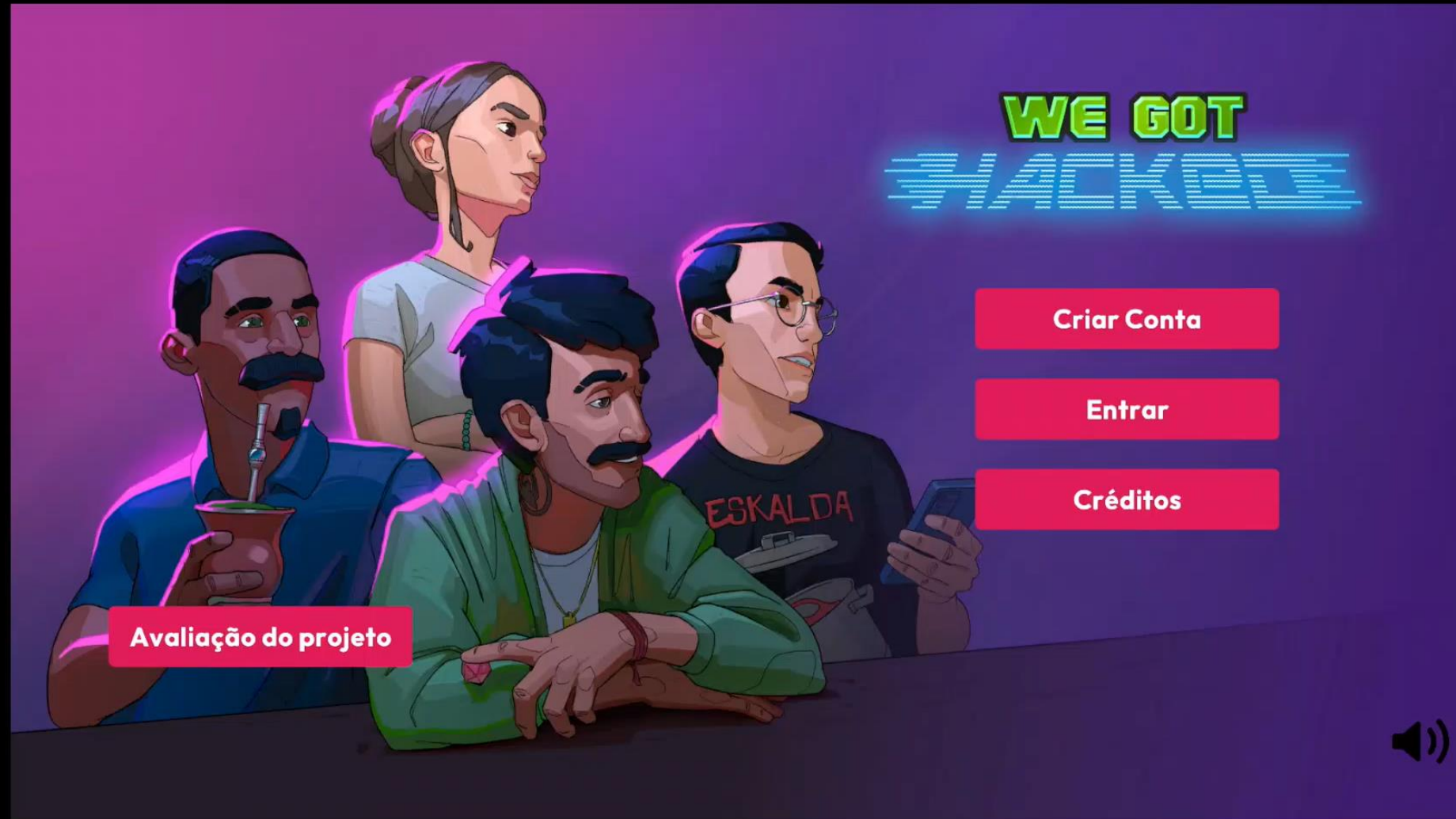


- Melhorias implementadas com base no projeto de extensão proposto pelo GT-IR e no feedback obtido com os residentes do Programa Hackers do Bem;
- Os aprimoramentos no jogo contemplam:
 - Melhorias na estrutura do jogo;
 - Avanços no game design e na arte;
 - Inserção de novos elementos educacionais.

2. Extensão do Projeto – Estrutura do Jogo

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

2. Extensão do Projeto – Estrutura do Jogo



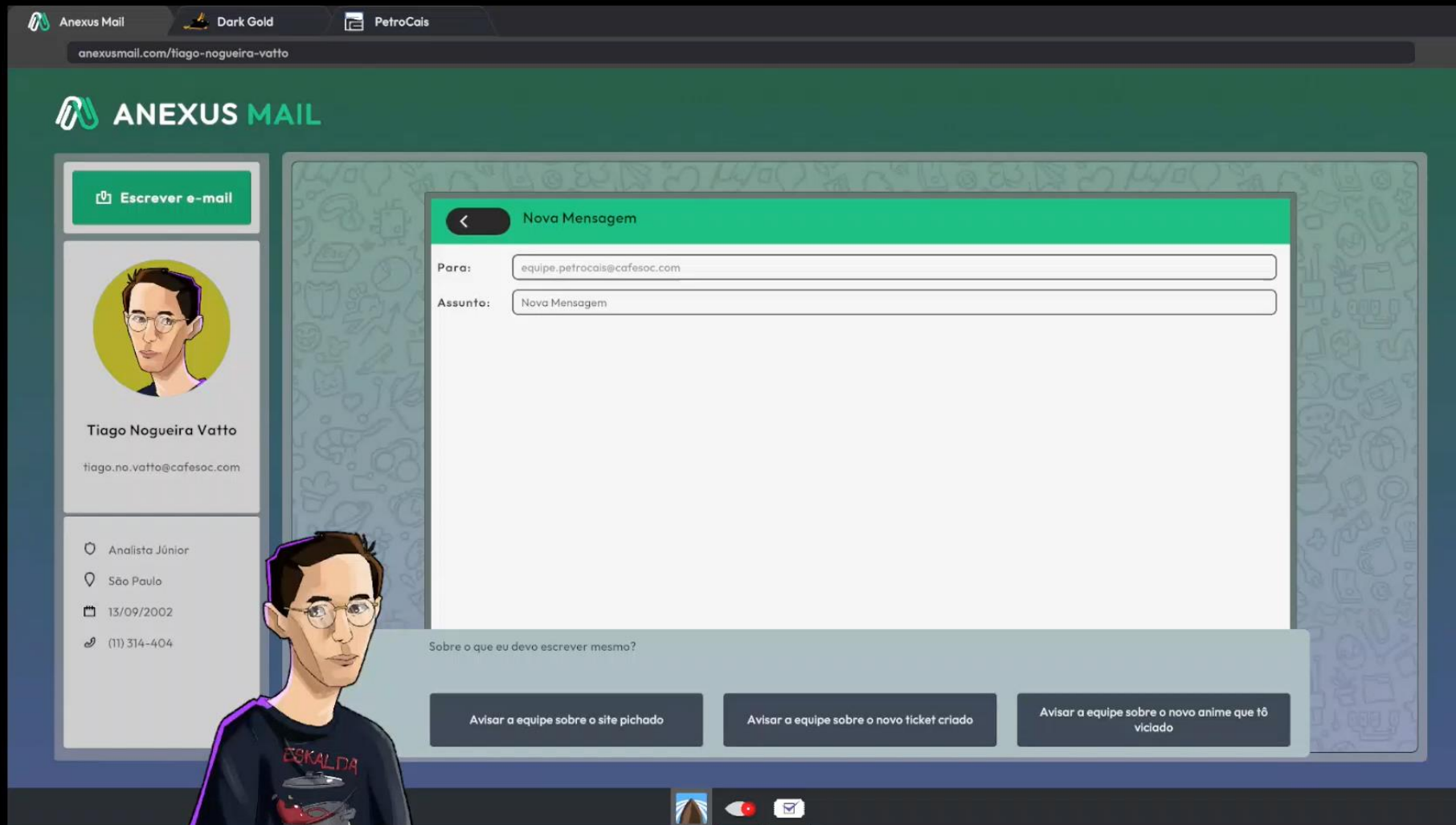
2. Extensão do Projeto – Game Design e Arte

Melhoria	Origem	Situação
Melhoria da cutscene inicial	<i>Feedback</i> 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	<i>Feedback</i> dos Residentes	Concluída
Adicionar sons em alertas e ações	<i>Feedback</i> dos Residentes e Projeto de Extensão (1º objetivo)	Concluída
Adicionar trilha sonora ambiente	<i>Feedback</i> dos Residentes e Projeto de Extensão (1º objetivo)	Concluída
Aumentar tamanho das fontes	<i>Feedback</i> dos Residentes	Concluída
Correção de erros nos textos	<i>Feedback</i> dos Residentes	Concluída
Melhorias de contexto nos textos	Projeto de Extensão (2º objetivo)	Concluída
Rota alternativa	Projeto de Extensão (2º objetivo)	Concluída

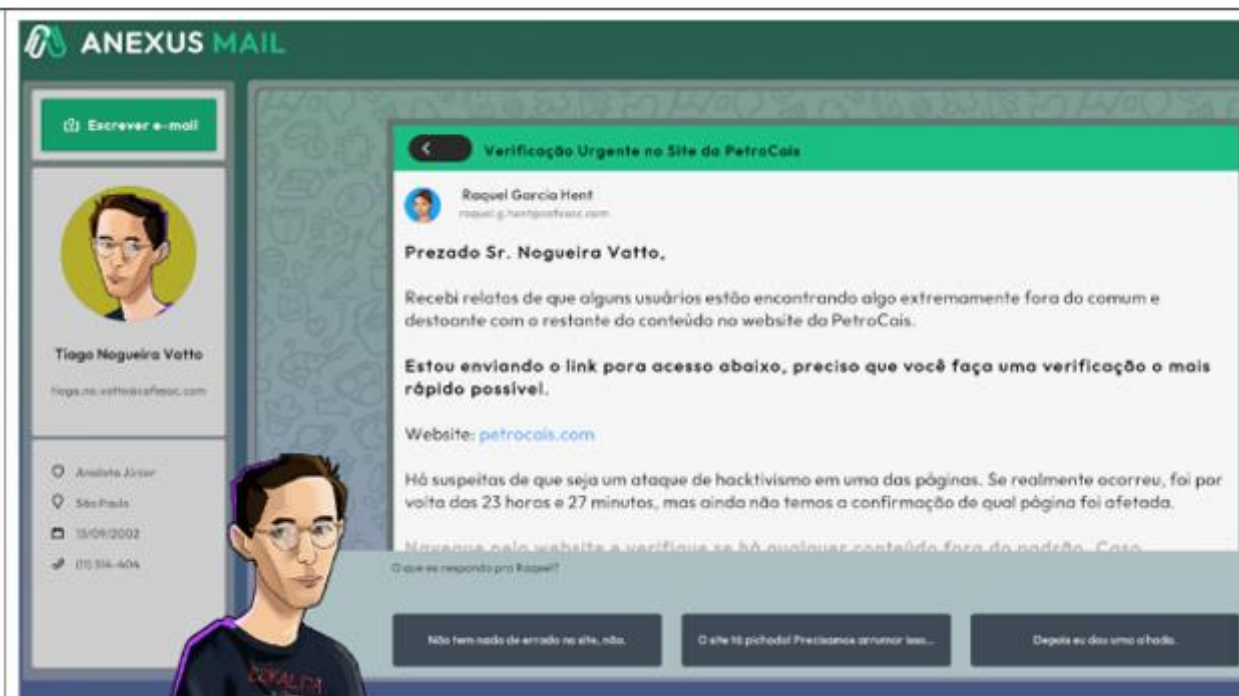
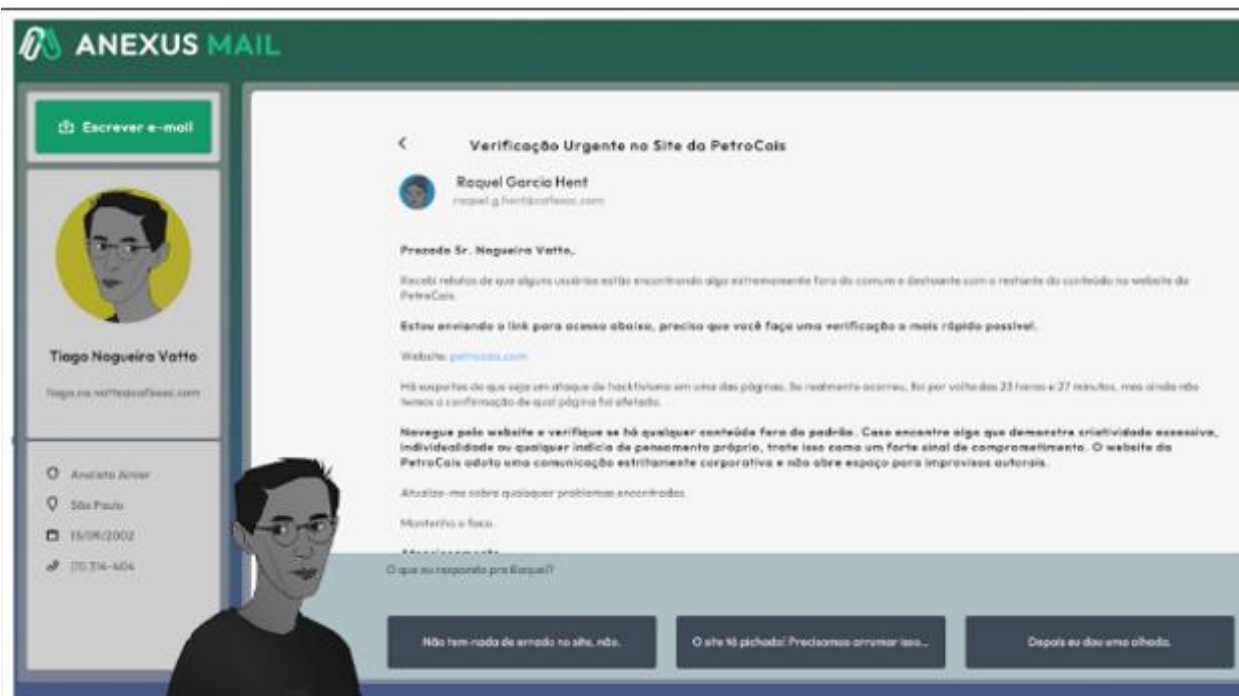
2. Extensão do Projeto – Game Design e Arte



2. Extensão do Projeto – Game Design e Arte



2. Extensão do Projeto – Game Design e Arte



2. Extensão do Projeto – Conteúdo Educacional

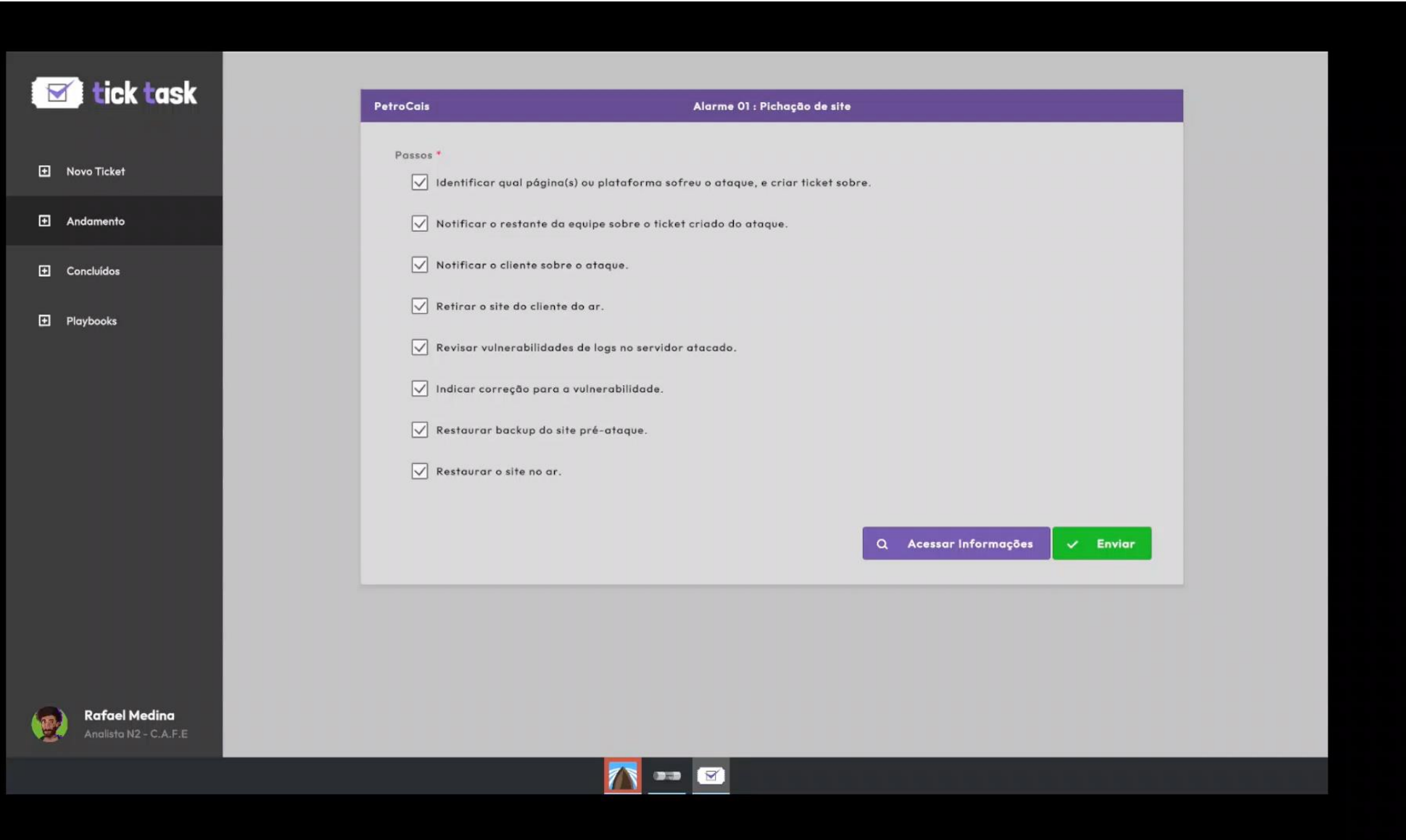


Fase	Incidente	Tópicos das aulas
1	Pichação de sites	SOC
		SIEM
		Agentes de ameaça e grupos hacktivistas
		Pichação de sites
2	<i>Ransomware</i>	Códigos maliciosos
		Indicadores de comprometimento (IoCs)
		<i>Ransomware</i>
3	Vazamento de dados	Comunicação de incidentes
		Ferramenta de inspeção de pacotes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

2. Extensão do Projeto – Conteúdo Educacional



2. Extensão do Projeto – Conteúdo Educacional



The screenshot displays the 'tick task' application interface. On the left is a dark sidebar with the 'tick task' logo and navigation links: 'Novo Ticket', 'Andamento', 'Concluídos', and 'Playbooks'. The main area shows a task titled 'Alarme 01: Pichação de site' under the 'PetroCals' category. It contains a checklist of steps, all of which are checked. At the bottom right of the task area are two buttons: 'Acessar Informações' and 'Enviar'. The bottom of the screen features a task bar with a user profile for 'Rafael Medina, Analista N2 - C.A.F.E.' and system icons.

tick task

- Novo Ticket
- Andamento
- Concluídos
- Playbooks

PetroCals **Alarme 01: Pichação de site**

Passos *

- ☒ Identificar qual página(s) ou plataforma sofreu o ataque, e criar ticket sobre.
- ☒ Notificar o restante da equipe sobre o ticket criado do ataque.
- ☒ Notificar o cliente sobre o ataque.
- ☒ Retirar o site do cliente do ar.
- ☒ Revisar vulnerabilidades de logs no servidor atacado.
- ☒ Indicar correção para a vulnerabilidade.
- ☒ Restaurar backup do site pré-ataque.
- ☒ Restaurar o site no ar.

[Acessar Informações](#) [Enviar](#)

Rafael Medina
Analista N2 - C.A.F.E.

2. Extensão do Projeto – Não implementados

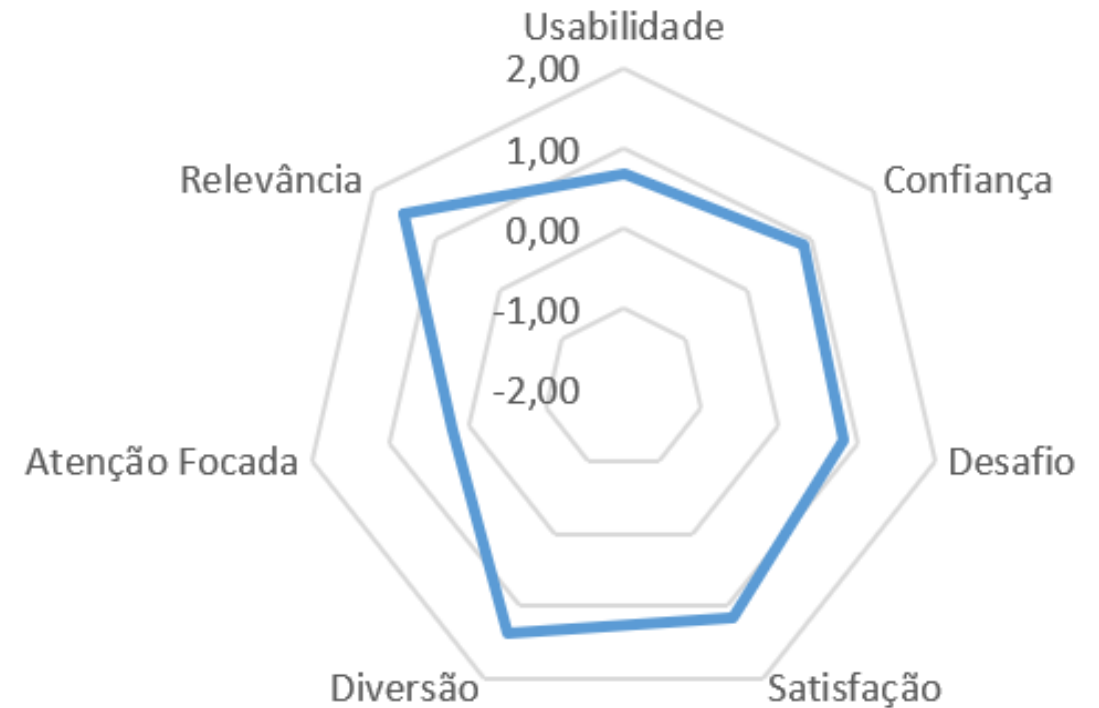
Objetivo	Melhoria	Origem	Situação
Melhorias de <i>game design</i> e arte	Melhorar o feedback após cada fase ou quando se comete um erro	Feedback dos Residentes	Não foram implementados
	Possibilidade de rever diálogos na <i>cutscene</i> de abertura		
	Melhorar o scroll e a navegação de telas		
	Criação 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

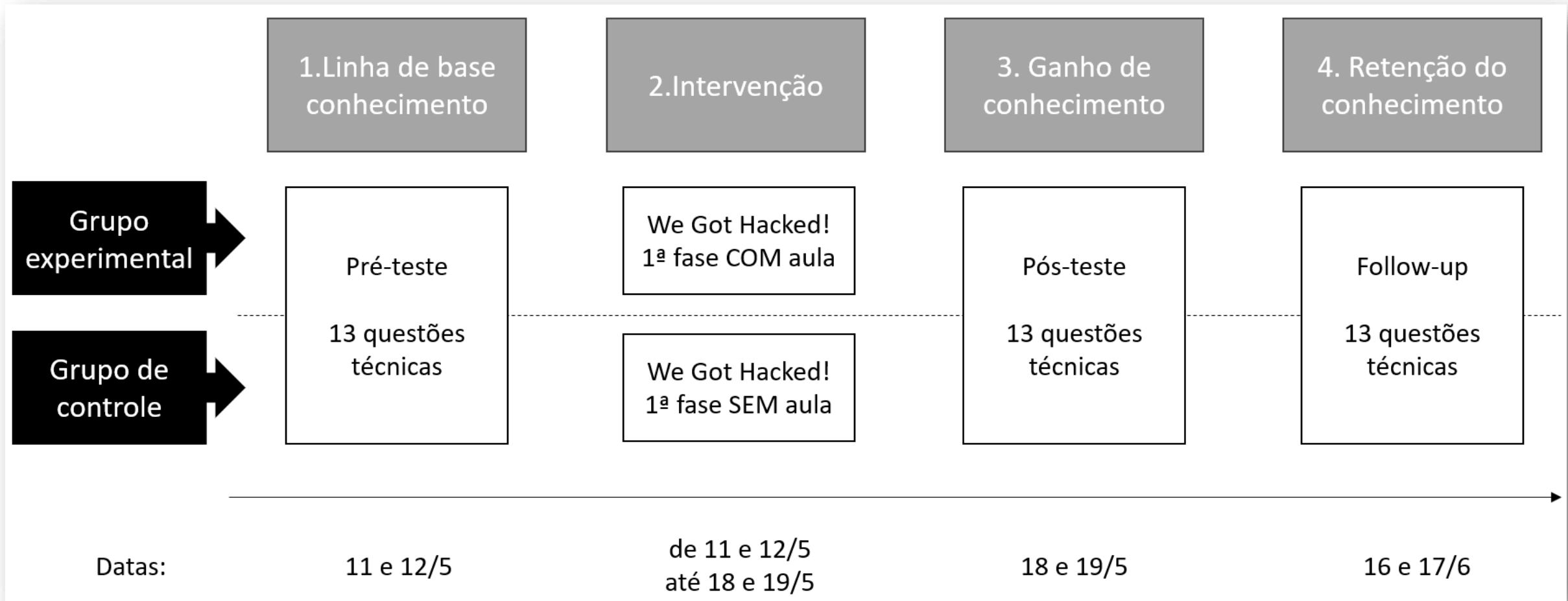
Etapa	Residentes
Residentes convidados	29
Entraram no grupo	28
Jogaram o We Got Hacked!	27
Responderam sobre a experiência (MEEGA+)	25

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%





Conheça o ..
We Got Hacked!