



GT-LFI - *Learn from Incidents* - Sistema de Ensino- Aprendizagem, Gamificação e Classificação a partir de Incidentes

Apresentação final - RNP - 14/07/2025

Coordenador - Prof. Dr. Rodrigo Sanches Miani - FACOM/UFU

Incidentes de Segurança



O que é um incidente?

Evento que compromete a **confidencialidade**, **integridade** e/ou **disponibilidade**.



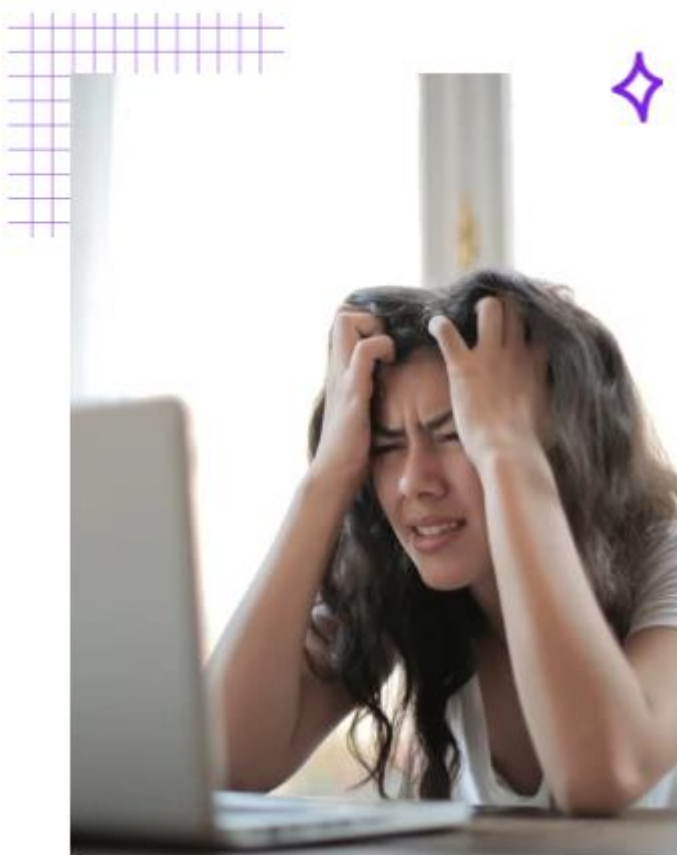
Cenário Atual

700M de ataques no Brasil em 2024 (2º país mais atacado da América Latina).



Impacto

Sobrecarga em CSIRTs, PoPs e empresas. Demanda por profissionais qualificados!



A resposta a incidentes é **lenta, manual e não escalável!**



Faltam profissionais qualificados!

4,8 milhões de vagas! 90% dos entrevistados apontam falta de habilidades (especialmente em resposta a incidentes).



Treinamento ineficiente

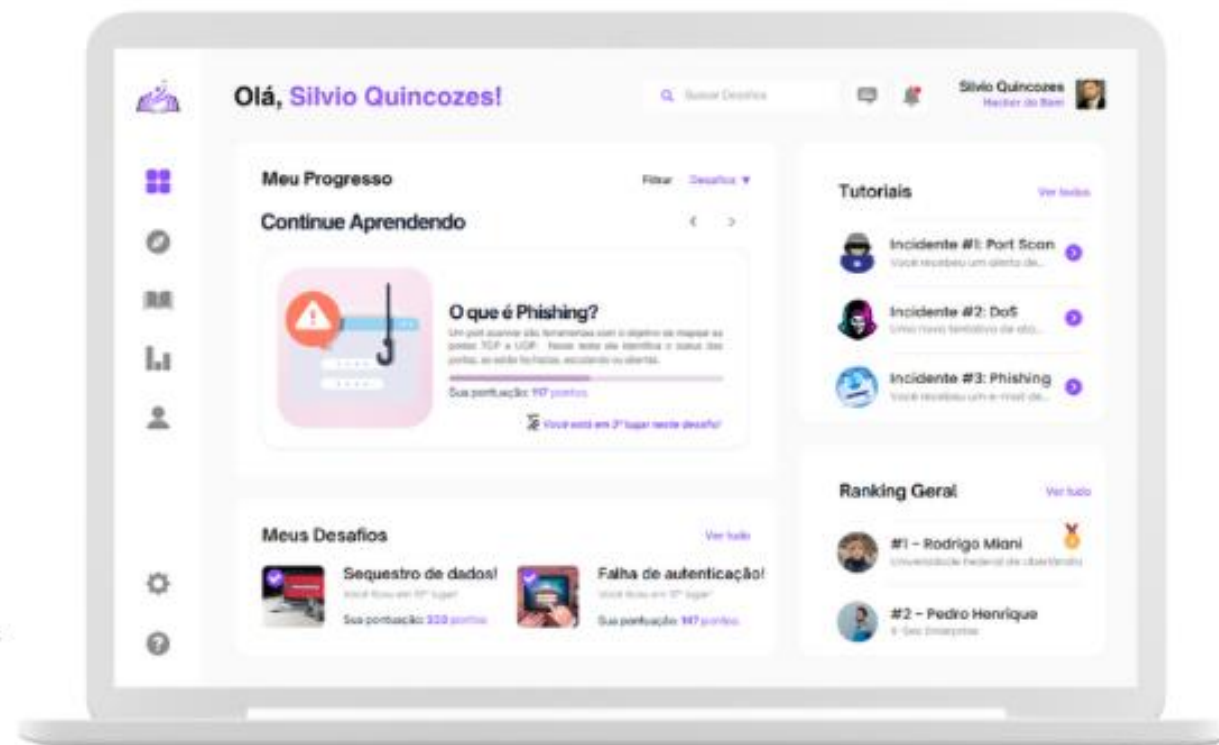
Cursos com foco teórico, **desconectados da prática** e pouco efetivos para a realidade.

Como resolver o problema? - Parte 1



Plataforma de Aprendizagem

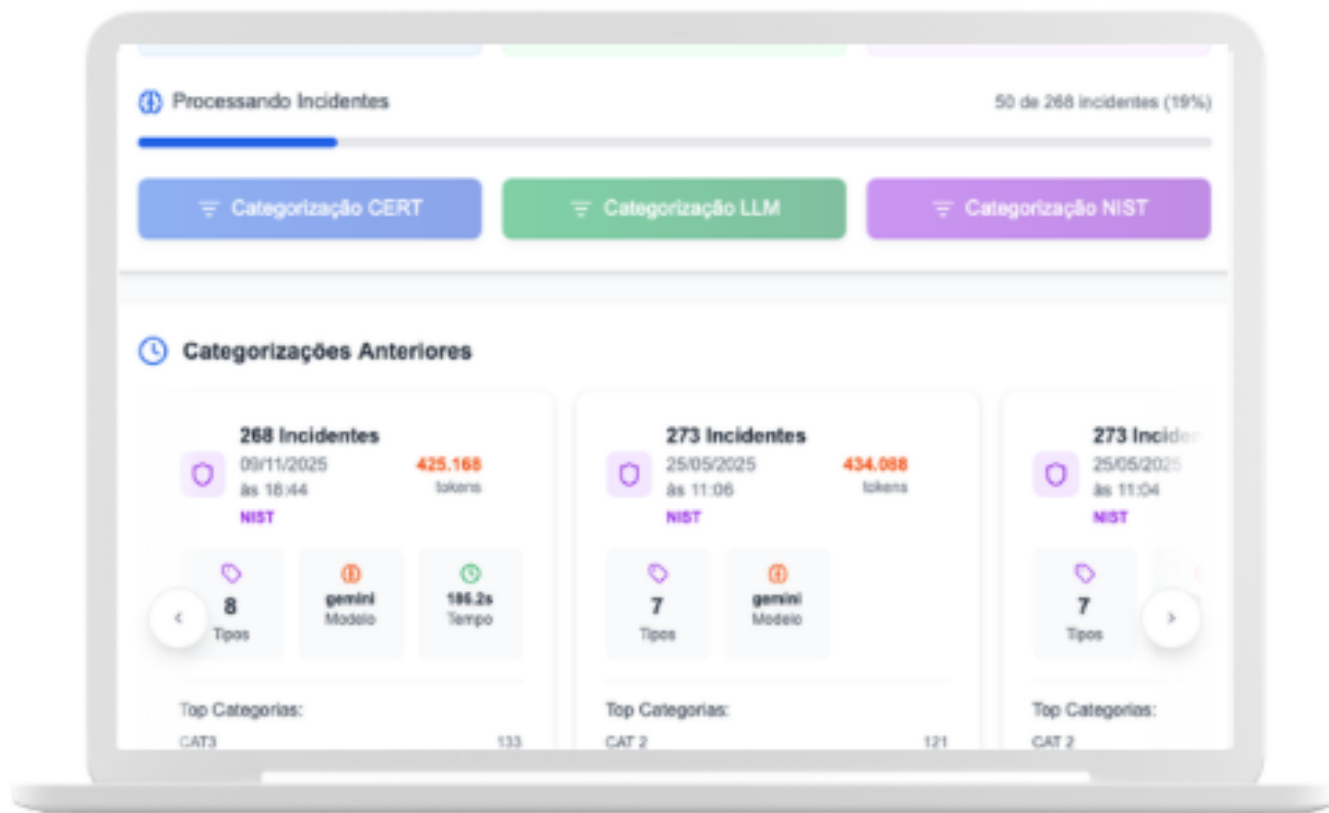
- Experiência **prática** e **envolvente** no aprendizado de resposta a incidentes.
- Aprendizado contínuo e **gamificado** com **ranking**, **missões** e **trilhas** de aprendizagem.
- Simulação de incidentes com **inteligência artificial** a partir de **dados reais e atualizados**.



Como resolver o problema? - Parte 2

Classificação e geração automática de playbooks

- **Tickets** de incidentes são basicamente formados por **textos**.
- IAs, em particular **LLMs**, podem ser usadas para auxiliar em **tarefas** que demandam **tempo dos analistas**: classificação de incidentes e geração de playbooks
- Considerando a sensibilidade dos dados, é importante inserir o analista no processo (**human-in-the-loop**).



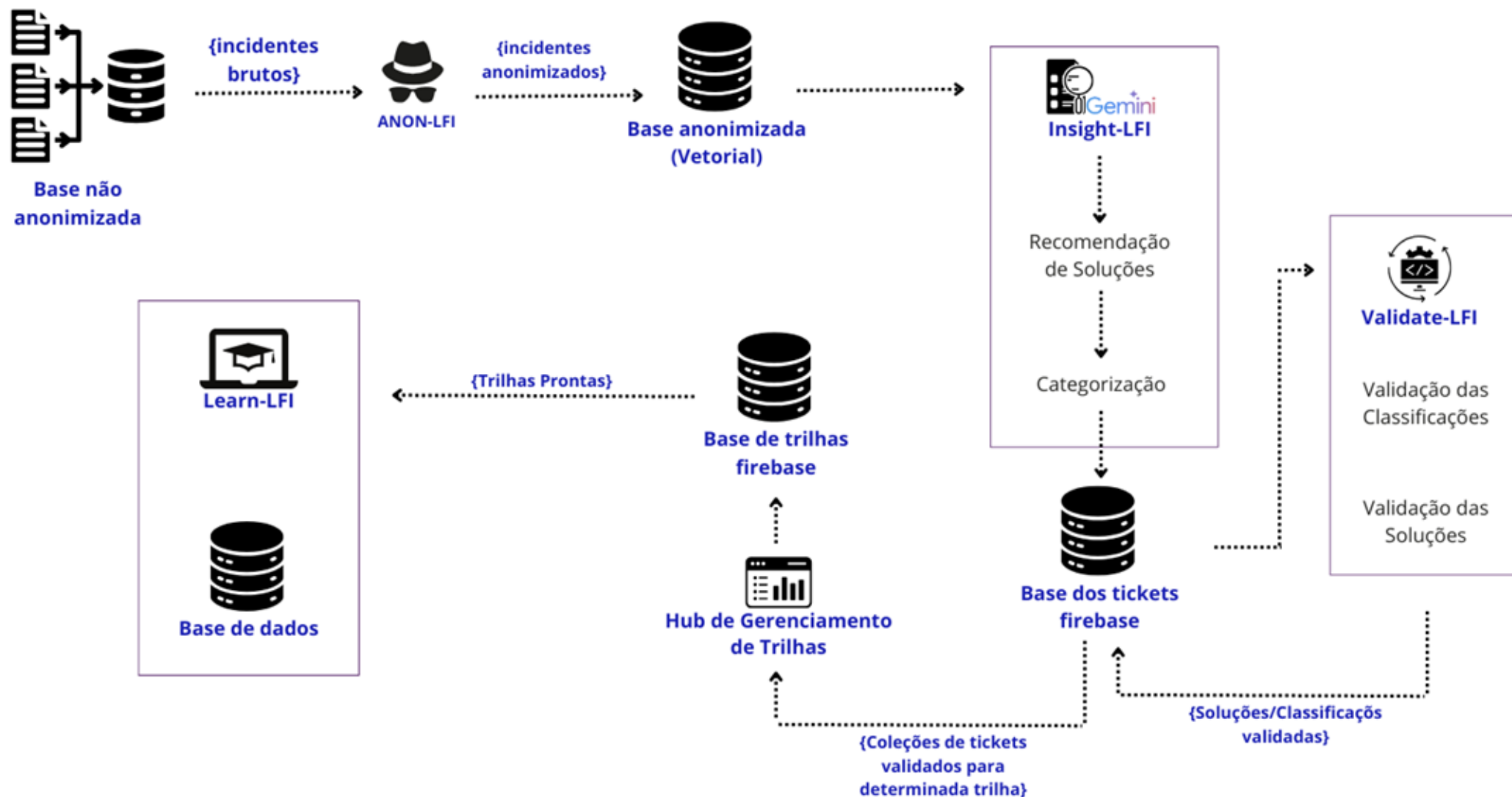
Proposta

Integrar anonimização, classificação, validação humana e gamificação em um fluxo único de aprendizagem a partir de incidentes reais

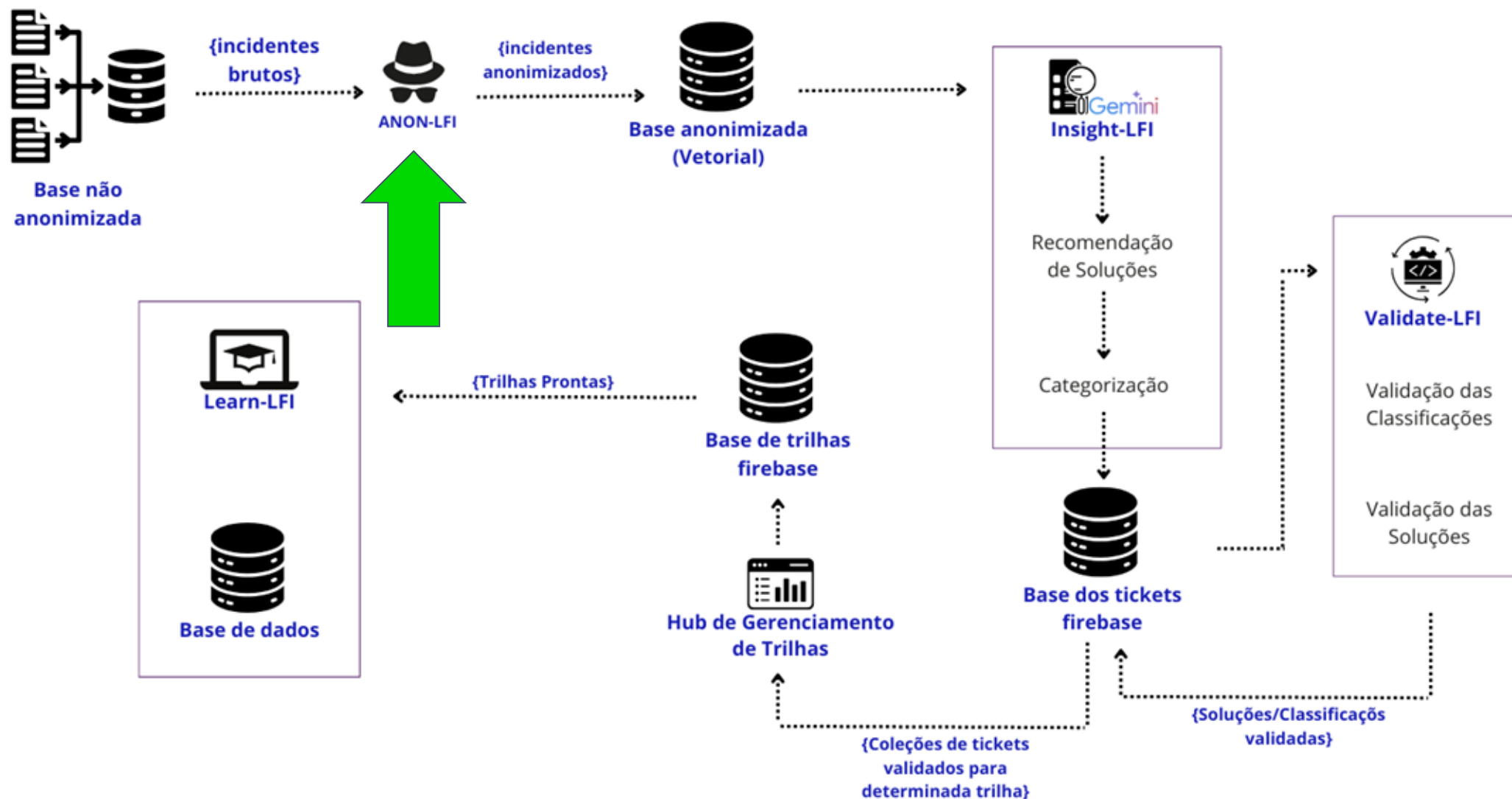
- **Anonimização** de incidentes reais com possibilidade de reidentificação controlada
- **Classificação** automática de incidentes com apoio de IA
- **Validação** humana e apoio à construção de playbooks
- Ambiente **gamificado** para **formação** prática em resposta a incidentes



Arquitetura



Arquitetura



Arquitetura



Anon-LFI **Home** [Checar API](#) [Checar Modelos NLP](#) [Perfil](#)

Processamento de Texto

Análise rápida de entidades e anonimização em um fluxo unificado.

Texto

ID: TCK-2026-0605-006
Organização afetada: Atlântica Pagamentos S.A.
Domínio institucional: atlanticapay.com.br
Tipo de incidente: Consultas DNS para domínios suspeitos
IP de origem: 200.19.145.206
Hostname: FIN-ANALISTA-023.atlanticapay.com.br
Usuário associado: marina.costa@atlanticapay.com.br
Data de notificação: 05/06/2026 às 16:25:33 UTC
Status: Aberto
Descrição do incidente:
Foi identificado que o host FIN-ANALISTA-023.atlanticapay.com.br, pertencente à Atlântica Pagamentos S.A., realizou múltiplas consultas

[Extrair Entidades](#) [Anonimizar Texto](#)

Texto anonimizado

ID: TCK-2026-0605-006
Organização afetada: [ORGANIZATION_f45c2974d5] S.A.
Domínio institucional: atlanticapay.com.br
Tipo de incidente: Consultas DNS para domínios suspeitos
IP de origem: [IP_ADDRESS_78a85bf824]
Hostname: FIN-ANALISTA-023.atlanticapay.com.br
Usuário associado: [EMAIL_ADDRESS_d82fbfdcee]
Data de notificação: 05/06/2026 às 16:25:33 UTC

Usuário:

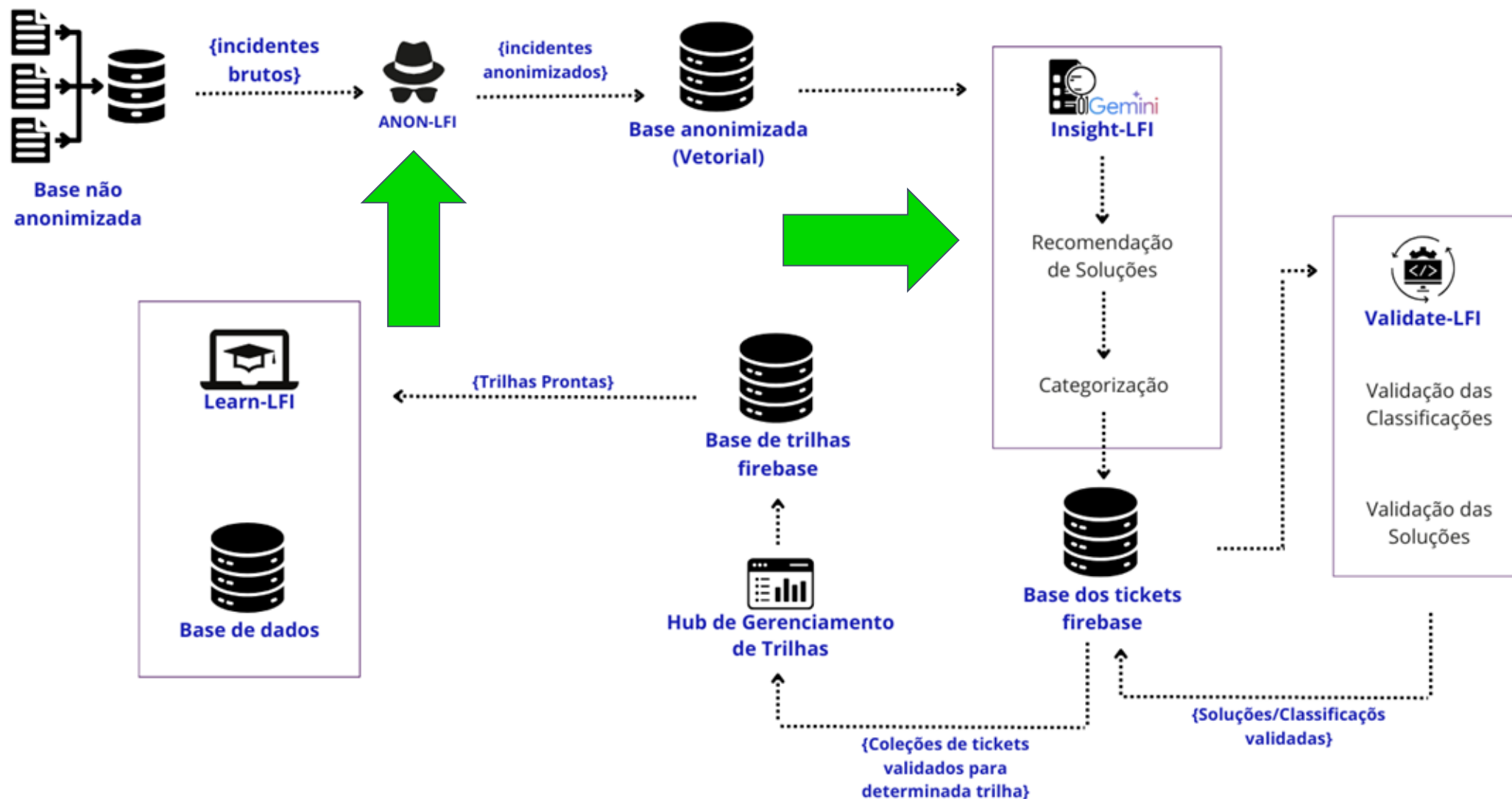
teste1@gtlfi.com.br

Senha:

GT_LFI!@34



Arquitetura



Arquitetura



LFI AutoClass

Home

Upload de Incidentes

Chat Contextual

Categorização

Tickets

Resultados

Ambiente: Residentes

Sair

Categorização CERT

Concluído

teste1@gtlfi.com.br

gemini-3.1-flash-lite

1 incidentes

3.4s

Salvar Resultado

Recarregar

Processando Incidentes

1 de 1 incidentes (100%)

Incidentes	Categorias	Tokens	Tempo
1	1	1.353	3.4s

Entendendo os Tokens

- Tokens de Entrada:** Quantidade de "palavras" ou frações de palavras enviadas à IA para processamento (ex: descrições de incidentes, instruções).
- Tokens de Saída:** Quantidade de "palavras" geradas pela IA como resposta (ex: categorias, motivos da classificação).
- Tokens Totais:** Soma dos tokens de entrada e saída, geralmente usada para cálculo de custo.

Estimativa de Custo (Modelo: gemini-3.1-flash-lite)

Valores baseados em US\$ 0,25/milhão (entrada) e US\$ 1,50/milhão (saída) para o modelo selecionado. Conversão para Real (BRL) considera 1 USD = R\$ 5,60. Estes são valores de exemplo e podem variar.

Custo de Entrada: 1.136 tokens × (US\$ 0,25 / 1M) = US\$ 0,000284

Custo de Saída: 217 tokens × (US\$ 1,50 / 1M) = US\$ 0,000326

Custo Total Estimado (USD): US\$ 0,00061

Custo Total Estimado (BRL): R\$ 0,00

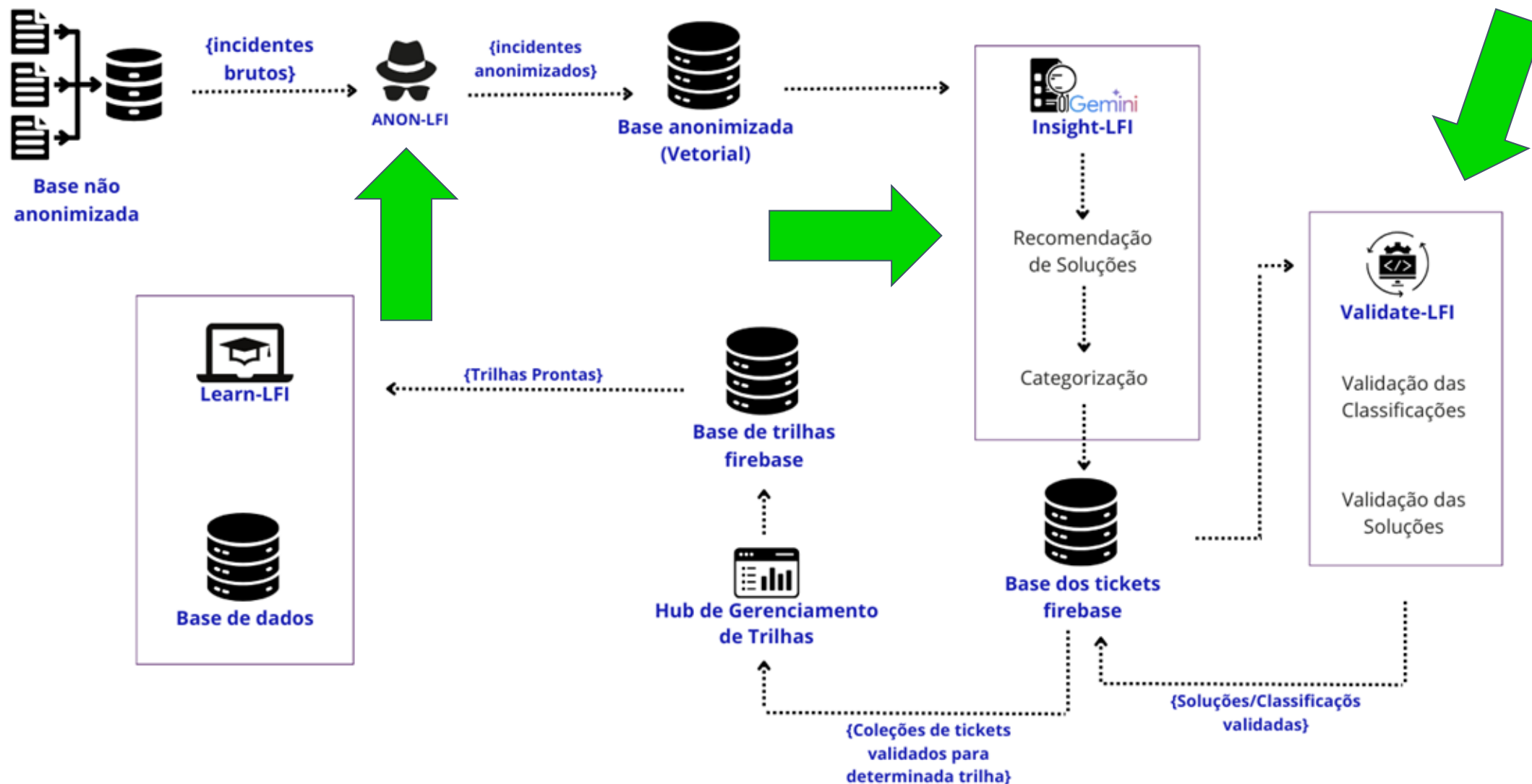
Distribuição

Invasão 1

Usuário:
teste1@gtlfi.com.br
Senha:
GT_LFI!@34



Arquitetura



TICKET EM ANDAMENTO

INC-20260524-97ZFV3

Etapa 1 de 2



Conteúdo Original (RAW)

Dados brutos do incidente

5962152,Host com o serviço SMB vulnerável,[IP_ADDRESS_63f2ec5bb5],[DATE_TIME_4ca32ffef1] 03:25:27+00:00,Resolvido,Acesso Indevido-Vazamento/SMB

Expandir conteúdo



Classificações Originais

Geradas automaticamente pelo sistema

CERT

Invasão

O incidente relata acesso indevido e vazamento de dados através de um serviço SMB vulnerável, caracterizando uma invasão bem-sucedida.

LLM

Vulnerabilidade de Serviço

O incidente refere-se a um serviço SMB vulnerável exposto, o que representa uma falha de configuração ou falta de atualização que permite acesso indevido.

NIST

CAT5

The incident involves a vulnerable SMB service being exploited, which falls under the exploitation of technical flaws.



Suas Classificações

Edite e valide as categorias identificadas

CERT

Invasão

LLM

Vulnerabilidade de Serviço

NIST

CAT5

Comentários sobre a classificação

Adicione observações sobre as categorias identificadas...

Usuário:

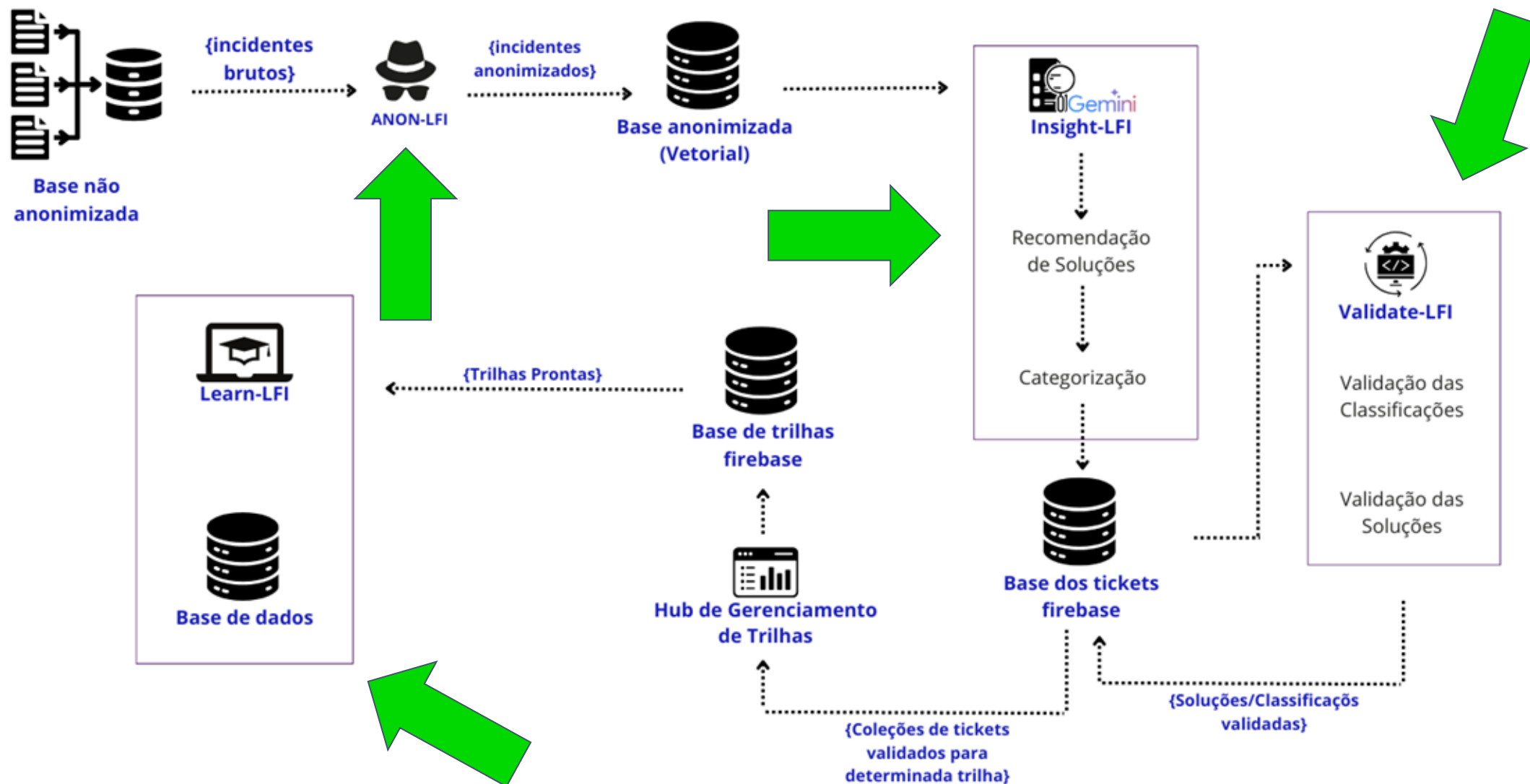
teste1@gtlfi.com.br

Senha:

GT_LFI!@34



Arquitetura



Arquitetura



1

Novato

5 / 100 XP - próximo nível 2

5%

Buscar Desafios

Rodrigo Sanches Miani

Nível 1 - Hacker do Bem

R

Meu Progresso

Meus Cursos

Ver tudo

Você ainda não se inscreveu em nenhuma trilha

Explore as sugestões abaixo para começar sua jornada de aprendizado.

Sugestões Para Você



Trilha 2 – Nível Básico - Classificar Incidentes de Segurança

A Trilha 2 – Nível Básico: Como Classificar Incidentes de Segurança capacita o aluno a compreender e aplicar os princípios...

● Principiante

🕒 2h 📁 2 módulos 🏆 150 XP

👤 0



Trilha 1 – Nível Básico - O que são Incidentes de Segurança

Objetivo: Compreender o conceito de incidente de segurança da informação, sua importância dentro de um contexto...

● Principiante

🕒 1h 📁 2 módulos 🏆 140 XP

👤 0



Trilha 4 – Nível Intermediário - Playbooks para Classificação de Incidentes de Segurança – Caso Prático: Ataque DDoS...



Trilha 3 – Nível Básico - Atividades sobre Incidentes de Segurança

Atividades sobre ataques DDoS, incidentes de segurança, exemplificados em python e algumas outras atividades de baixa ...

Ranking Geral

		Izys Machado	Sem organização	485 XP	Nv. 3
#2		Lorenzo Ponsi Ficher	Sem organização	470 XP	Nv. 3
#3		Ana Sales	Sem organização	465 XP	Nv. 3
#4		Lucas Martins	Sem organização	450 XP	Nv. 3
#5		Erick	Sem organização	440 XP	Nv. 3

Pontos = XP acumulado ao completar ações nas trilhas.

Suas Estatísticas

5

XP Total

1

Nv. 1

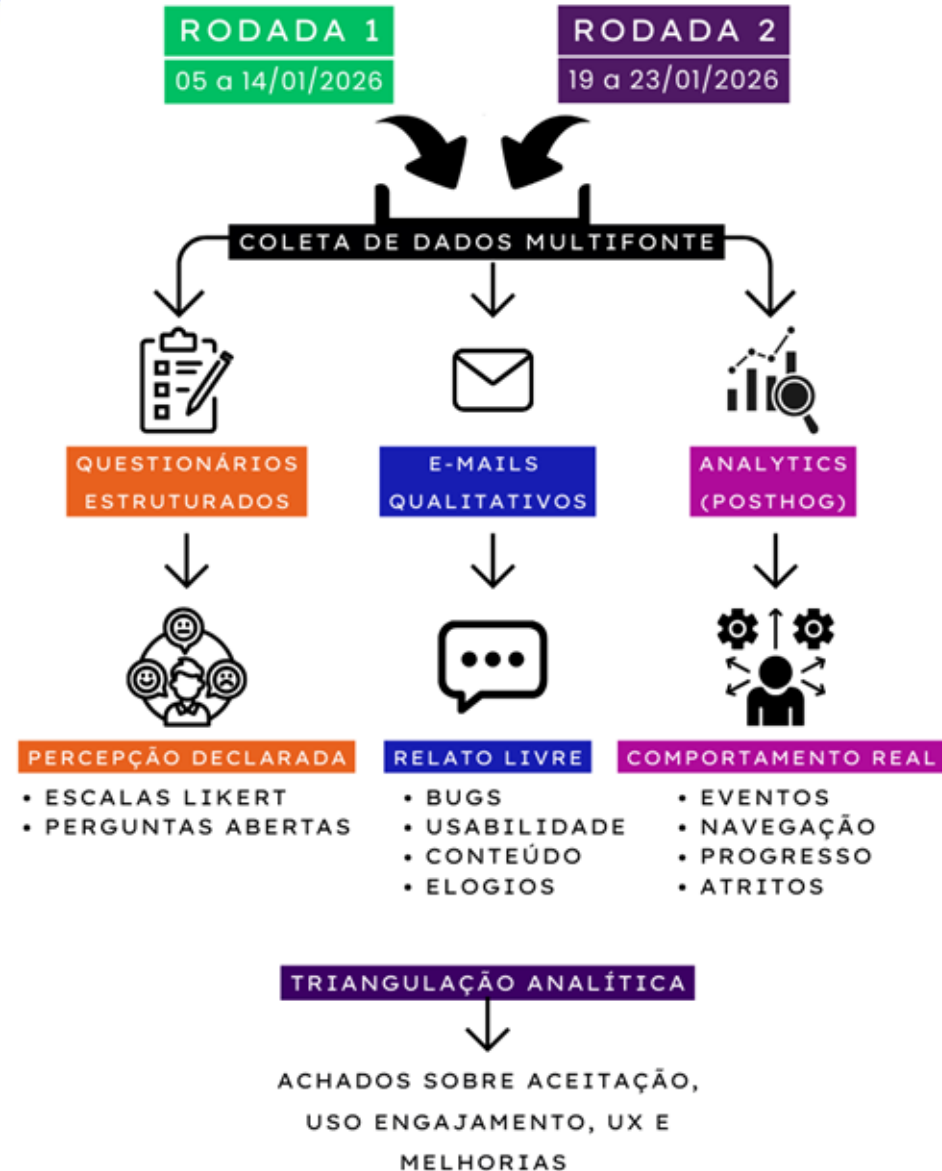
Nível

0

Conta
Google



Avaliação - Primeira onda



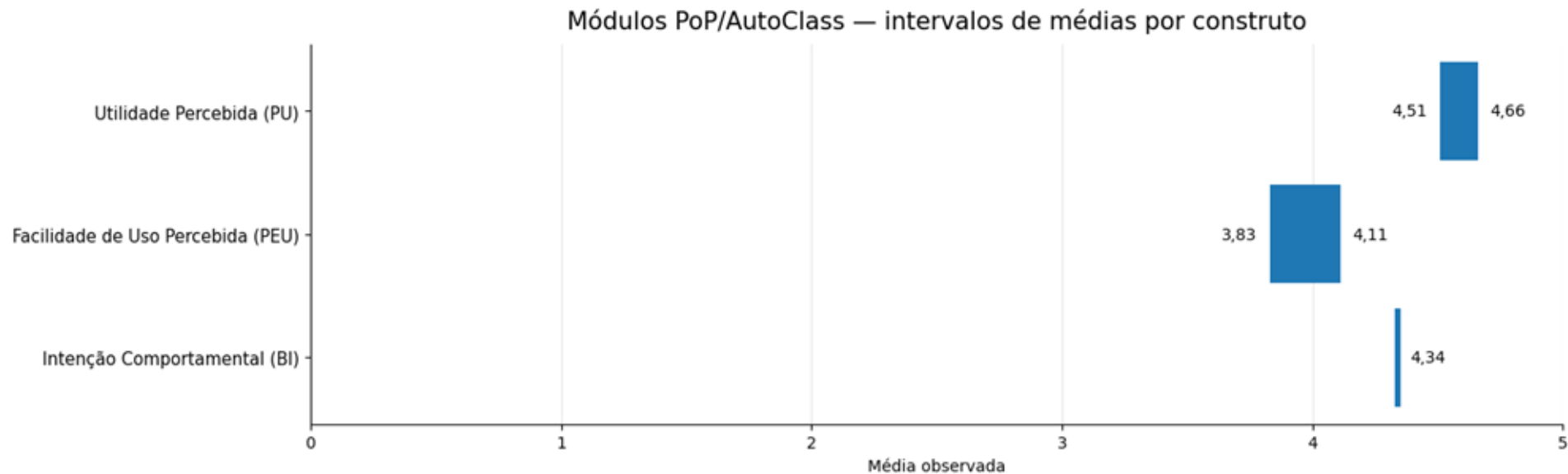
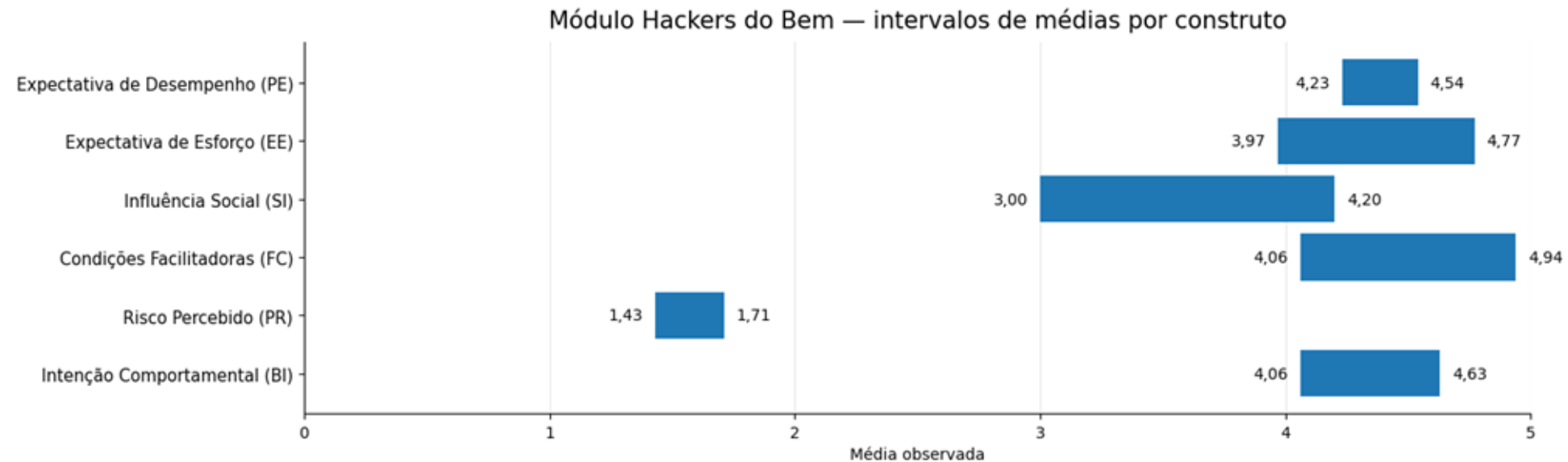
Sumário da avaliação - Principais resultados

Trilha	Tentativas	Score médio	Taxa de aprovação
Trilha 1 – O que são Incidentes	36	77,50	80,56%
Trilha 2 – Classificar Incidentes	94	65,27	54,26%
Trilha 3 – Ataques DDoS com Python	70	93,11	84,29%
Trilha 4 – Playbooks DDoS	35	83,80	82,86%

Sumário da avaliação - Principais resultados

Ajustes e melhorias	Quantidade	Pontos positivos	Quantidade
Bugs	18	Material didático	15
Usabilidade	15	Estrutura de ensino	10
Material didático	8	Usabilidade	5
Estrutura de ensino	6	Funcionalidade	2

Avaliação - Primeira onda



Avaliação - Segunda onda

Indicador	Resultado	Comparação com a primeira avaliação	Observação
Respondentes válidos	9 (UTAUT) 14 (pré-teste) 6 (pós-teste)	35 (UTAUT) 9 e-mails	Tivemos uma etapa adicional: pré-teste e pós-teste
Usuários ativos	15	33 (-54,5%)	Pico diário (PostHog)
Eventos totais	2.873	16.269 (-82,3%)	Redução proporcional à amostra reduzida
Lições concluídas	101	508 (-80,1%)	7 usuários únicos completaram lições (funil)
Quizzes submetidos	41	235 (-82,6%)	7 usuários únicos submeteram quizzes
Trilhas concluídas	18	79 (-77,2%)	6 usuários únicos concluíram trilhas
Dead clicks	826	2.448 (-66,3%)	Proporção dead_click/evento: 28,7% (2ª) vs 15,0% (1ª)
Rage clicks	11	145 (-92,4%)	Proporção rage/evento: 0,38% (2ª) vs 0,89% (1ª)

HACKERS
DO
BEM

ANÁLISE — PRÉ-TESTE N=14														
#	Participante	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Acertos	Erros	% Acerto
1	c*****@gmail.com	OK	OK	NOK	OK	OK	OK	OK	NOK	NOK	OK	7	3	70%
2	t*****@unipampa.edu.br	OK	OK	OK	OK	OK	OK	OK	OK	NOK	OK	9	1	90%
3	t*****@unipampa.edu.br	OK	OK	OK	OK	OK	NOK	NOK	NOK	NOK	OK	6	4	60%
4	p*****@unipampa.edu.br	OK	NOK	NOK	NOK	OK	OK	NOK	NOK	OK	NOK	4	6	40%
5	m*****@gmail.com	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	10	0	100%
6	b*****@gmail.com	OK	OK	OK	NOK	OK	OK	OK	OK	OK	OK	9	1	90%
7	c*****@gmail.com	OK	OK	NOK	NOK	NOK	OK	OK	NOK	OK	NOK	5	5	50%
8	l*****@unipampa.edu.br	OK	OK	NOK	NOK	NOK	OK	OK	NOK	NOK	NOK	4	6	40%
9	l*****@gmail.com	OK	OK	OK	NOK	OK	OK	OK	OK	OK	OK	9	1	90%
10	m*****@gmail.com	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	10	0	100%
11	g*****@gmail.com	OK	OK	OK	OK	NOK	OK	OK	NOK	NOK	NOK	6	4	60%
12	d*****@unipampa.edu.br	OK	OK	OK	NOK	OK	OK	OK	NOK	NOK	OK	7	3	70%
13	a*****@unipampa.edu.br	OK	NOK	OK	NOK	OK	NOK	NOK	NOK	NOK	NOK	3	7	30%
14	m*****@unipampa.edu.br	OK	OK	NOK	NOK	OK	OK	OK	NOK	OK	NOK	6	4	60%
Média												7	3	68%

HACKERS
DO
BEM

ANÁLISE — PÓS-TESTE														
#	Participante	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Acertos	Erros	% Acerto
1	e*****@gmail.com	OK	OK	NOK	NOK	OK	OK	OK	OK	OK	OK	8	2	80%
2	l*****@gmail.com	OK	OK	OK	OK	OK	OK	OK	OK	OK	NOK	9	1	90%
3	g*****@gmail.com	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	10	0	100%
4	l*****8@unipampa.edu.br	OK	OK	OK	NOK	OK	OK	OK	OK	OK	OK	9	1	90%
5	r*****@gmail.com	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	10	0	100%
6	m*****@unipampa.edu.br	OK	OK	OK	NOK	OK	OK	OK	OK	OK	OK	9	1	90%
Média												9	1	92%

O GT-LFI entregou um ecossistema funcional para aprendizagem e apoio à resposta a incidentes, validado com residentes do Hackers do Bem.

- **Produtos:** plataforma gamificada de ensino e plataforma de gerenciamento para PoPs, CSIRTs e SOCs.
- **Ferramentas:** Anon para anonimização de tickets e Insight para categorização, geração de playbooks e análise com IA.
- **Avaliação:** 44 avaliações completas (UTAUT), pré-teste, pós-teste e 31 pontos de melhoria implementados entre as duas avaliações.
- **Produção:** 3 artigos publicados, 1 submetido e 1 em preparação com prêmio de Artefato Destaque no SBSeg 2025 para o Anon-LFI.

- **Registro do software** - processo iniciado. Primeira reunião marcada para o fim de julho com a equipe responsável da RNP;
- **Redação de artigos** - o artigo que compreende todo o trabalho desenvolvido está em fase de revisão antes de submissão, outras submissões estão previstas (avaliações e salão de ferramentas);
- **Trabalhos acadêmicos associados ao projeto:** 2 dissertações de mestrado (UNIPAMPA e UFU) e 1 tese de doutorado (UFU);
- **Aproximação com a RNP/PoP e outras empresas - difusão e uso dos produtos:** Validate/PoP - Leandro Bertholdo, Anon - Diego Kreutz.

Coordenação



Dr. Rodrigo
Sanches Miani

Coordenador Geral



Dr. Silvio Ereno
Quincozes

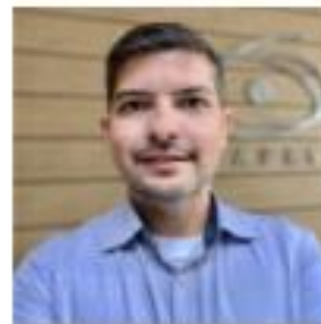


Dr. Diego Luis
Kreutz

Coordenadores Locais

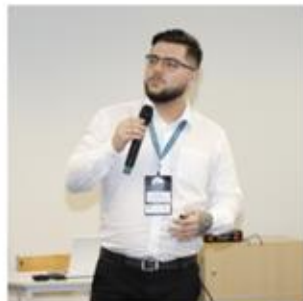


Dr. Leandro
Bertholdo



Dr. Rafael
Dias Araújo

Bolsistas e colaboradores



Felipe Scherer



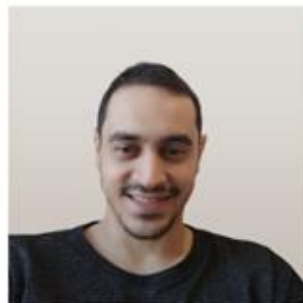
Felipe Nestor Dresch



Sebastião de Jesus



Carolina Bandel



Alvaro Santana



João Pedro Esteves



Beatriz Machado

Agradecimentos



Demonstração



<https://tinyurl.com/GTLFI-DEMO>

