



DESAFIOS EM CIBERSEGURANÇA E TECNOLOGIAS AVANÇADAS

Resultados da Pesquisa Perspectivas para o futuro

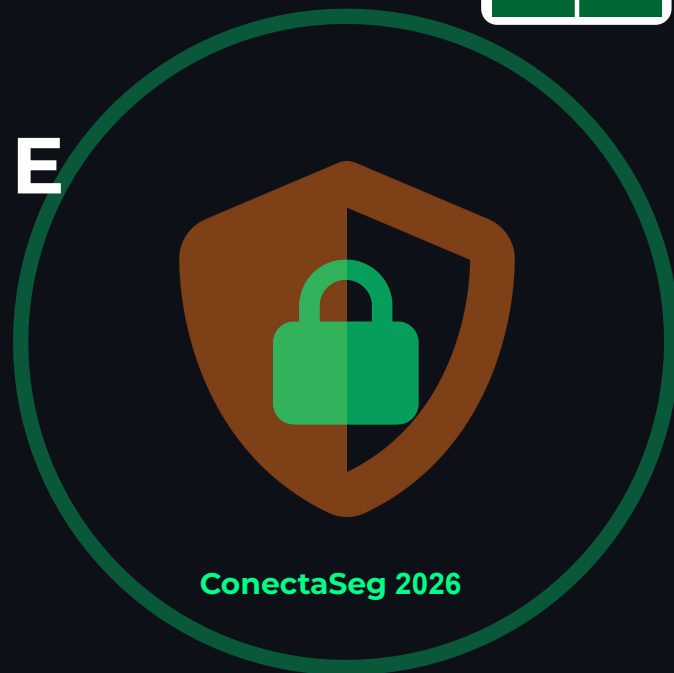
Professores

Dra. Edna Dias Canedo e Dr. Laerte Peotta de Melo

Programa

PPCA — Pós-Graduação em Computação Aplicada

```
> initializing_scan...  
> loading_modules: [AI_SEC, CLOUD_DEFENSE, API_GUARD]  
> status: SECURE
```



ConectaSeg 2026



Segurança Ofensiva



Inteligência Artificial



Proteção de Dados

O Perfil dos Respondentes

> Coletamos dados de especialistas atuantes

PESQUISA 2026
N = 88 PROFISSIONAIS

Nível de Atuação



● Técnico (40%) ● Gestores (37%) ● Executivos (17%)

Setores em Destaque



Órgãos Governamentais

Principal base da pesquisa

26%



Empresas Públicas

Forte presença estatal

19%



Empresas Privadas

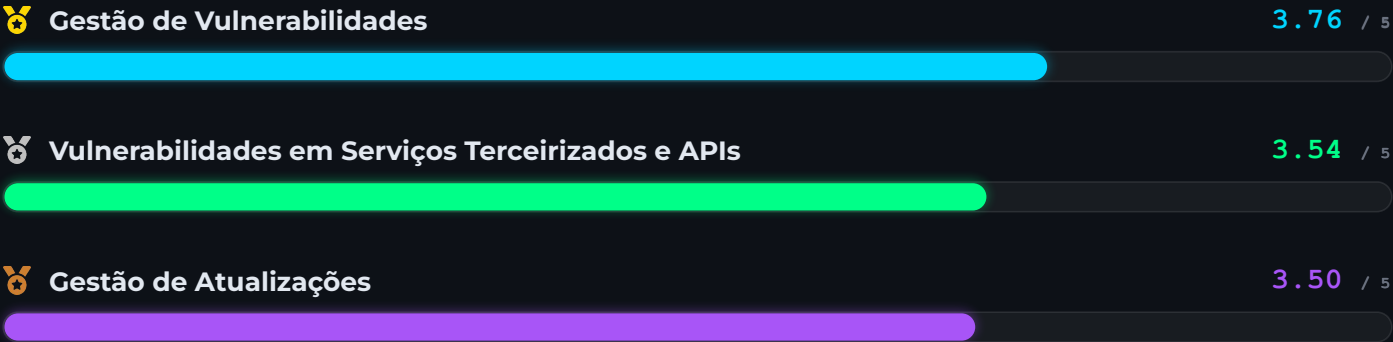
Setor corporativo

17%

Fatores de Maior Impacto na Cibersegurança

⚠️ A gestão contínua do ambiente atual é a maior dor

ESCALA DE IMPACTO (1-5)



Insight do Especialista

"Apesar de falarmos muito sobre inovações, o **fundamental bem feito** (gestão de falhas e atualizações) é o que mais preocupa os profissionais hoje, especialmente ao lidar com **APIs e serviços de terceiros**."

Principais Desafios de Segurança Digital

! A raiz dos problemas: falhas humanas e de desenvolvimento

RANKING DE VOTOS



OPINIÃO DOS EXPERTS

01



Exposição de dados sensíveis

Vazamentos não intencionais e credenciais fracas

42 VOTOS

02



Falta de treinamento ou cultura de segurança

Gap de conhecimento entre desenvolvedores

36 VOTOS

03



Vulnerabilidades em código-fonte

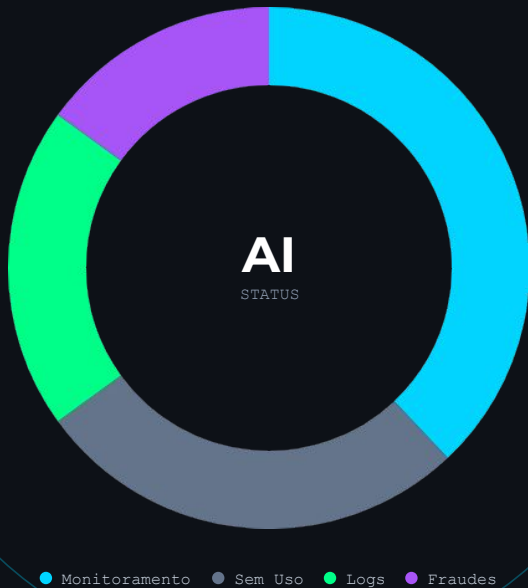
Bibliotecas externas e falhas de lógica

25 VOTOS

IA na Cibersegurança

🤖 Expectativa vs. Realidade: Onde a IA está realmente operando?

DISTRIBUIÇÃO DE USO



Monitoramento e Detecção 38%

A aplicação mais madura da IA. O foco principal das organizações é automatizar a identificação de anomalias em tempo real.



Nenhum uso atual 34%

Apesar do hype, muitas organizações ainda não implementaram IA, refletindo baixa maturidade, especialmente na academia e justiça.



Nichos Específicos FIN & PUB 32%

Forte uso de análise de logs no setor **Financeiro** e prevenção de fraudes em **Órgãos Públicos**.

Temas Emergentes

O Futuro da Pesquisa Aplicada: Garantir a operação e preparar para IA

PRIORIDADE MÉDIA (1-5)



0

1

2

3

4

5



Cadeia de Suprimentos



Ausência de Due Diligence de terceiros com avaliação efetiva — não apenas questionários auto respondidos pelos fornecedores.



Órgão Governamental



Existe baixa visibilidade das dependências existentes e vulnerabilidades. Grande parte dos códigos é reaproveitada.



Infraestrutura Crítica



Existe a preocupação constante de apagão aéreo por invasão de hacker, comprometendo o controle de tráfego.



Segurança Aérea



Preocupações com IA



Preocupações: exposição de dados sensíveis em prompts, Shadow AI fora da governança, prompt injection, envenenamento de dados e deepfakes em spear phishing.



Setor Financeiro/Público



O uso de IA requer atenção especial à proteção dos dados estratégicos. É essencial garantir supervisão humana.



Defesa



Muitas soluções, muitos dashboards... Falta governança de IA frente à urgência das áreas de negócio.



Gestor



Focos de Pesquisa

Temas mais citados



IA Adversarial / Seg. LLMs

5



Criptografia Pós-Quântica

4



Riscos na Cadeia de Suprimentos

4



Resposta a Incidentes / SOAR

4



Seg. Nuvem / Infra Crítica

3



Threat Hunting

2

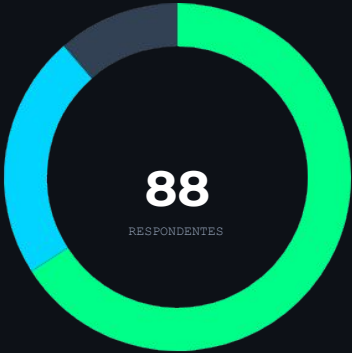


Base de dados: 88 respostas processadas

Potencial de Colaboração

📌 Interesse em Parceria com a UnB/PPCA

ENGAJAMENTO
ALTA RECEPTIVIDADE



Sim (58) Talvez (20) Não (10)

89%

dos profissionais estão abertos à colaboração e pesquisa aplicada com a UnB/PPCA.

✓ 58 Sim (66%) + 20 Talvez (23%) = Oportunidade Clara de Parceria

SGD/MGI - Governo Federal



"Avançar pesquisas em segurança ofensiva/defensiva com IA, privacidade diferencial e resistência a ransomware nas instituições públicas."

FAB - Força Aérea



"Frameworks de governança e resiliência digital para aviação, alinhados à ISO 31000, ISO 27005 e diretrizes da OACI."

Pesquisador / Doutorado



"Third-Party Risk Management: proteção da cadeia de suprimentos - o elo mais fraco define o nível de segurança de toda a cadeia."

Conclusões e Recomendações

 Síntese Estratégica & Próximos Passos

STATUS: FINALIZADO
2026 OUTLOOK



Fator Humano & Cultura



A cibersegurança necessita urgentemente de processos de conscientização e treinamento **'Shift-Left'** entre desenvolvedores para mitigar vulnerabilidades na fonte.



Vulnerabilidade na Cadeia



O ecossistema de **APIs de terceiros** e serviços integrados foi identificado como um dos elos mais fracos e críticos da atual cadeia de segurança.



Oportunidades de Pesquisa



Existe um espaço claro e demandado para consultoria especializada em **Continuidade de Negócios** e protocolos de Segurança Aplicada à **Inteligência Artificial**.



DESAFIOS EM CIBERSEGURANÇA E TECNOLOGIAS AVANÇADAS

Resultados da Pesquisa Perspectivas para o futuro

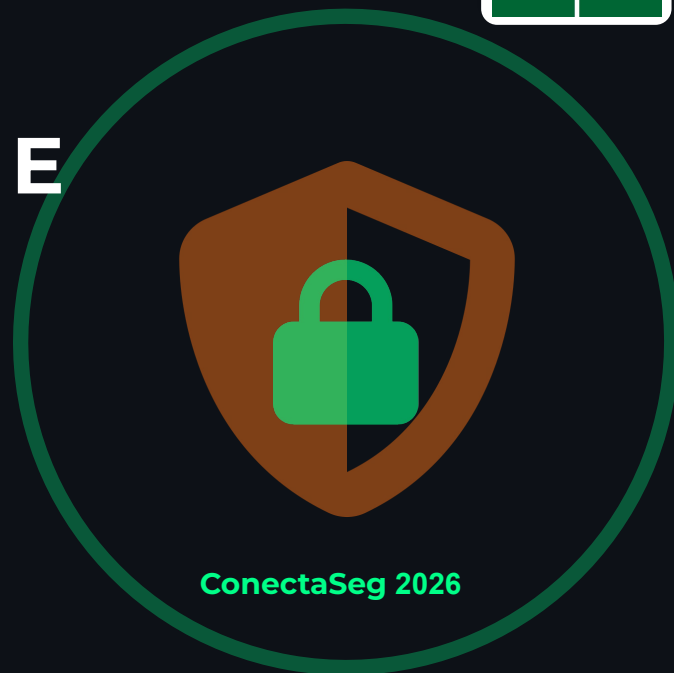
Professores

Dra. Edna Dias Canedo e Dr. Laerte Peotta de Melo

Programa

PPCA — Pós-Graduação em Computação Aplicada

```
> initializing_scan...  
> loading_modules: [AI_SEC, CLOUD_DEFENSE, API_GUARD]  
> status: SECURE
```



ConectaSeg 2026



Segurança Ofensiva



Inteligência Artificial



Proteção de Dados