



RiNP

Educação, Pesquisa
e Inovação em Rede

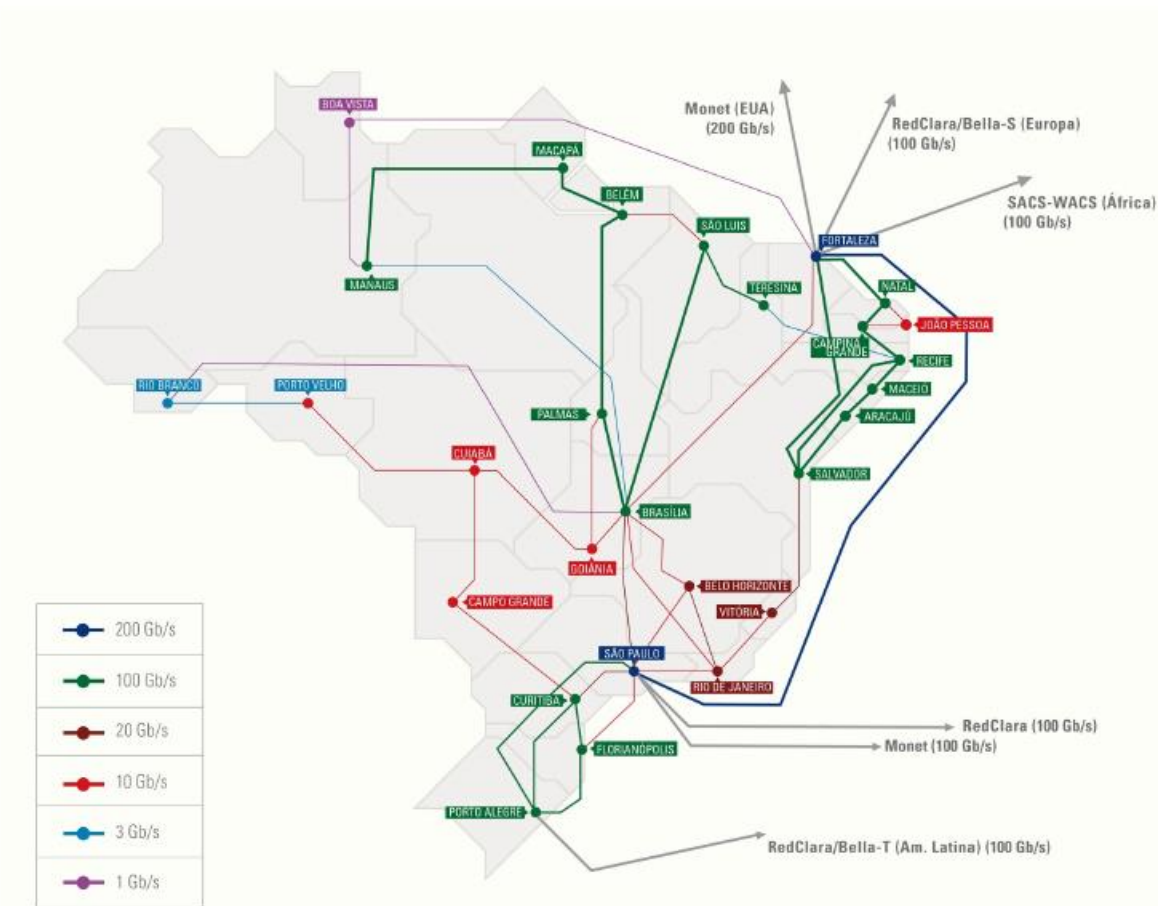
SEGURANÇA COMPROMETIDA

Como executamos pentests
e encontramos uma falha em
um software de uma
multinacional brasileira

Matheus Camargo · CAIS/RNP

RNP – Rede Nacional de Ensino e Pesquisa

- Internet de alta capacidade, serviços personalizados e promoção de projetos de inovação.
- Pioneiros, ao trazer a internet para o Brasil e a primeira rede de fibra ótica na América Latina em 2005.
- **4 milhões de alunos, professores e pesquisadores brasileiros.**
- **1500 universidades, institutos educacionais e culturais, agências de pesquisa, hospitais de ensino, parques e polos tecnológicos.**



CAIS – Inteligência em Cibersegurança



O que um pentest precisa entregar

- Entendimento do risco no contexto da aplicação

- Evidência reproduzível do que foi observado

- Informação útil para corrigir e revalidar

Reunião de Alinhamento

O teste começa no alinhamento

01 **Escopo**

Ativos, perfis, funções e exclusões

02 **Regras**

Janelas, limites de exploração e ações proibidas

03 **Contatos**

TI, desenvolvimento, SOC e resposta a incidentes

Testes de segurança: Reconhecimento

Primeiro, mapeamos a aplicação

Casos de uso e perfis de acesso

Hosts, serviços, endpoints e tecnologias

Fluxos de autenticação e autorização

Ler requisições, respostas, código e logs

Reconheciment
o é trabalho
paciente

Às vezes passamos dias construindo o mapa antes de encontrar um desvio relevante.

Testes de Segurança: Verificações Ativas e Validação

Teste ativo orientado por hipótese

- 01 Esperado** Qual controle deveria impedir a ação?
- 02 Variação** O que muda ao alterar entrada, ordem ou canal?
- 03 Evidência** O resultado confirma o desvio?

Este é um dos diferenciais do pentest:
Validação de vulnerabilidades

Testes
baseados em
frameworks e
guias:
OWASP WSTG,
API SECURITY,
CLOUD

Exploração & PoC

A PoC responde a uma pergunta:

O controle de segurança foi contornado com impacto verificável?

A exploração das vulnerabilidades pode permitir novos acessos e gerar a necessidade de novo reconhecimento

Elaboração de Relatório

- 01 Contexto** Perfil, função e condições em que o teste ocorreu
- 02 Passos** O necessário para reproduzir sem ambiguidade
- 03 Resultado** Comportamento esperado e observado

Os achados reportados precisam ser tão detalhados de modo a possibilitar sua reprodução na correção e no reteste.

Diferenciais na Fase de Reportação



Achados críticos precisam chegar cedo aos responsáveis



A apresentação de resultados complementa o relatório

O reteste fecha o ciclo

Achado

Correção

Revalidação

Sem repetir o cenário, não sabemos se o controle voltou a funcionar.

 O diálogo com desenvolvimento acelera a correção



Visão das etapas



Problemas recorrentes...

- 01 Documentação** Às vezes a topologia surge durante o teste
- 02 Homologação** Nem sempre existe um ambiente equivalente
- 03 Medo e Resistência** Algumas equipes tendem a ser resistências quanto a realização de testes de segurança em seus ambientes.

Um caso que reuniu essas etapas

Aplicação corporativa com MFA por código temporário

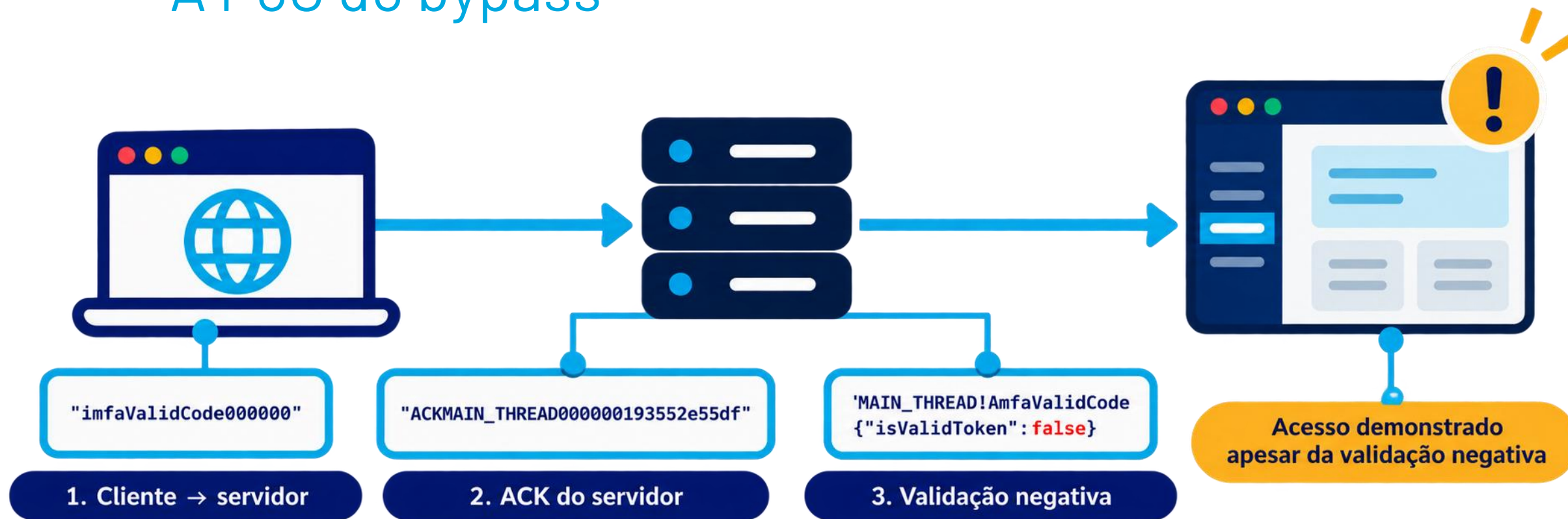
O teste encontrou uma forma de contornar o segundo fator no fluxo analisado.

Como investigamos o MFA

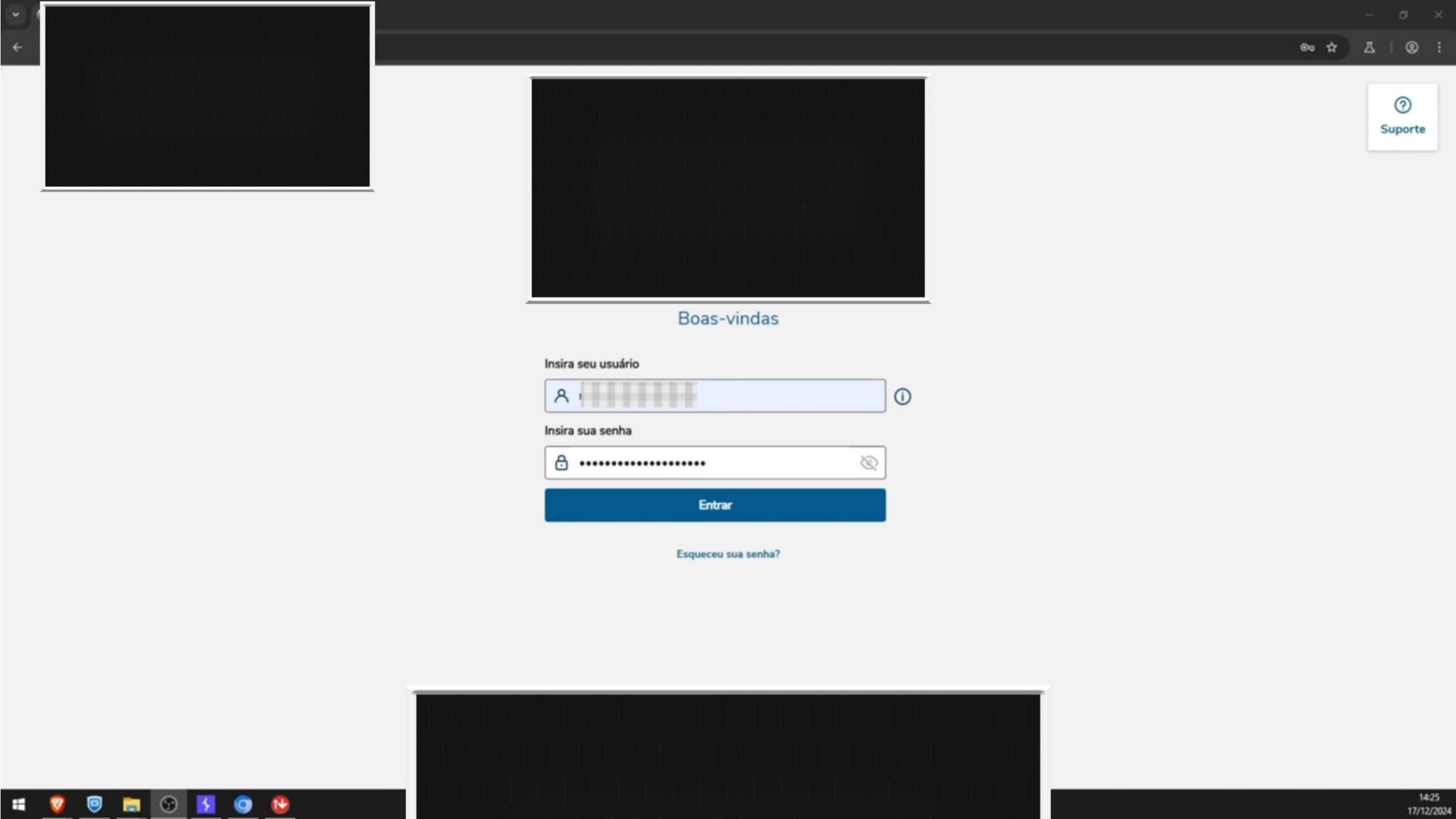
- 01 Credenciais** Primeira etapa de autenticação
- 02 Código** Validação do segundo fator por WebSocket
- 03 Acesso** Funções que deveriam exigir o MFA concluído

Simplicidade em ferramentas: Proxy HTTP já é suficiente

A PoC do bypass



O Controle de Acesso era feito em client-side




Suporte

Boas-vindas

Insira seu usuário

Insira sua senha

Entrar

[Esqueceu sua senha?](#)



Impacto, correção e reteste

O bypass permitia avançar sem concluir o MFA

A equipe de desenvolvimento tratou a falha

O reteste confirmou que a correção funcionou

O que sustenta um pentest efetivo

- | | | |
|-----------|---------------------|---|
| 01 | Preparação | Escopo e regras claras orientam todo o trabalho |
| 02 | Profundidade | Ferramentas ajudam, mas a análise manual encontra os desvios |
| 03 | Fechamento | Comunicação, correção e reteste fecham o ciclo |
| 04 | Continuidade | Pentests periódicos mantêm a avaliação alinhada às mudanças do ambiente |



PERGUNTAS

Perguntas

Matheus Camargo · CAIS/RNP
matheus.camargo@rnp.br

Obrigado



MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

