



Elevando o nível de cibersegurança e
privacidade

Fortalecendo o Sistema RNP

Alianças estratégicas reduzem riscos

Viabilizar inovação + ação preventiva (e compromissos) local e global



Sistema RNP 2025

Educação, Pesquisa e Inovação em Rede

Interiorização

19 Infovias estaduais
Rotas das Infovias estaduais
Rotas da Infovia nacional

REDECOMEP

183 cidades com redes comunitárias

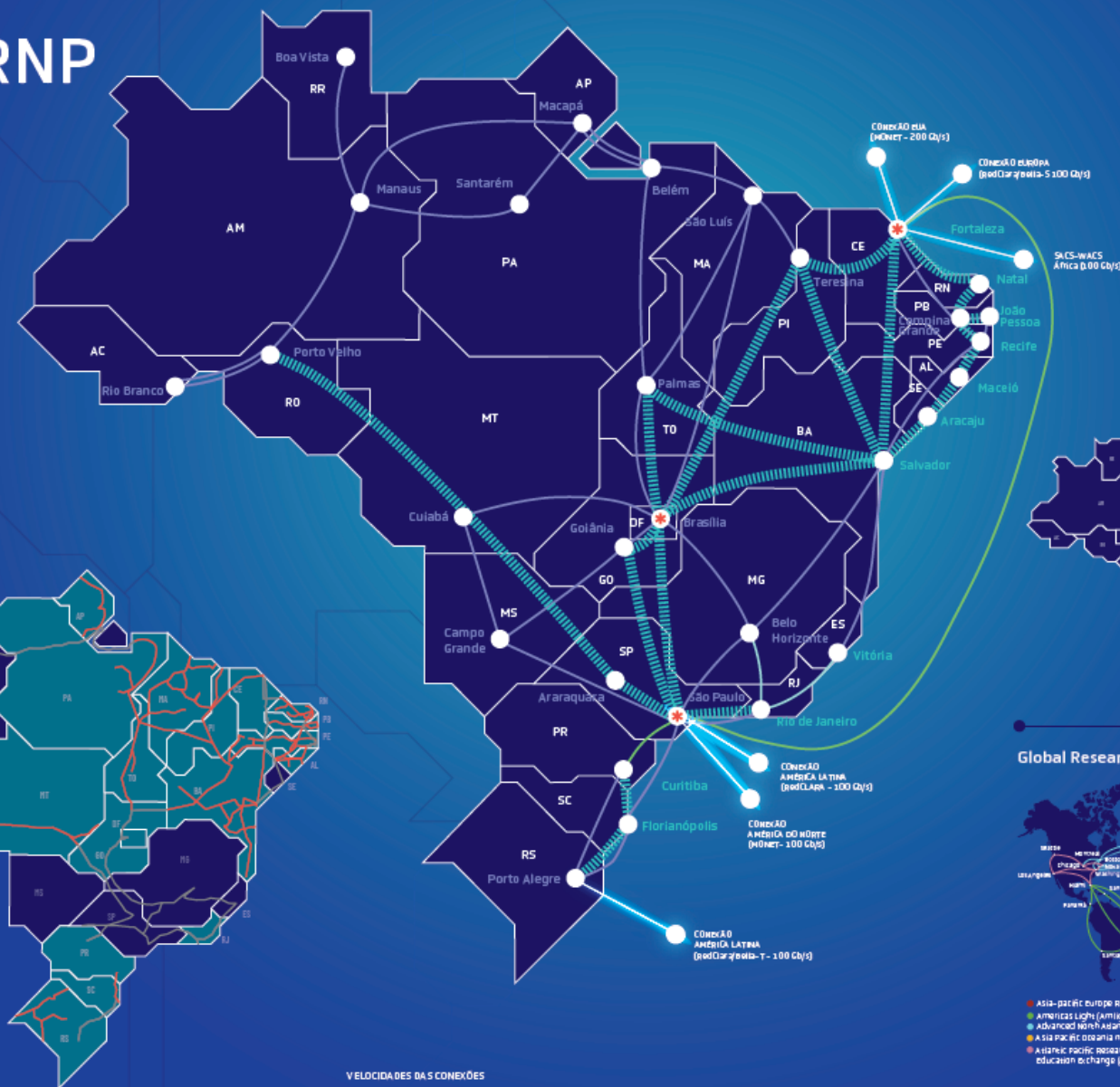
Nota: A velocidade de transferência máxima do sistema de rede é limitada pelo link mais lento da rede, ou seja, pelo link de menor capacidade.



ACESSE O QR CODE PARA
INFORMAÇÕES SOBRE
A NOSSA REDE E ABRANGÊNCIA NACIONAL.

NOSSO CASO:

Segurança e Privacidade no Sistema RNP



VELOCIDADE DAS CONEXÕES

Capacidade para expansão 4 Tbps 300 Gbps 200 Gbps 100 Gbps 3 CNs implementados

Classes de organizações usuárias

- Instituições de educação superior e pesquisa
- Agências de fomento e pesquisa
- Estabelecimentos de saúde com ensino e pesquisa
- Museus e instituições culturais
- Ambientes promotores de inovação (parques e polos tecnológicos)
- Empresas inovadoras

Abrangência

800 organizações atendidas
140 unidades de saúde integradas à RNP
27 pontos de presença estaduais
1,8 mil pontos conectados

POPs	estado	atendimento	estado	atendimento	estado	atendimento
AC	UFPA	MS	UFPA	RJ	CEFF	
AL	PAPEAL	MS	UFMG	RN	UFEN	
AM	UFAM	MS	UFMT	RN	UNIR	
AP	UNIRAP	MT	UFMT			
BA	UFBA	PA	UFPA	MS	UFMG	
CE	UFCE	PA	UFPA	SC	UFSC	
DF	DFDF	PE	ITEP	SE	UFSE	
ES	UFES	RJ	DA PRON	SP	UFSP	
GO	UFGO	RR	UFRR	TO	UFST	



RNP e os avanços em cibersegurança e privacidade

Apoio Metodológico



- Prover recursos de apoio à comunidade de ensino, pesquisa e inovação para avanços do nível de segurança e privacidade.

Apoio consultivo



- Ofertar serviços de consultoria especializada para contar com uma solução conforme as necessidades da instituição.

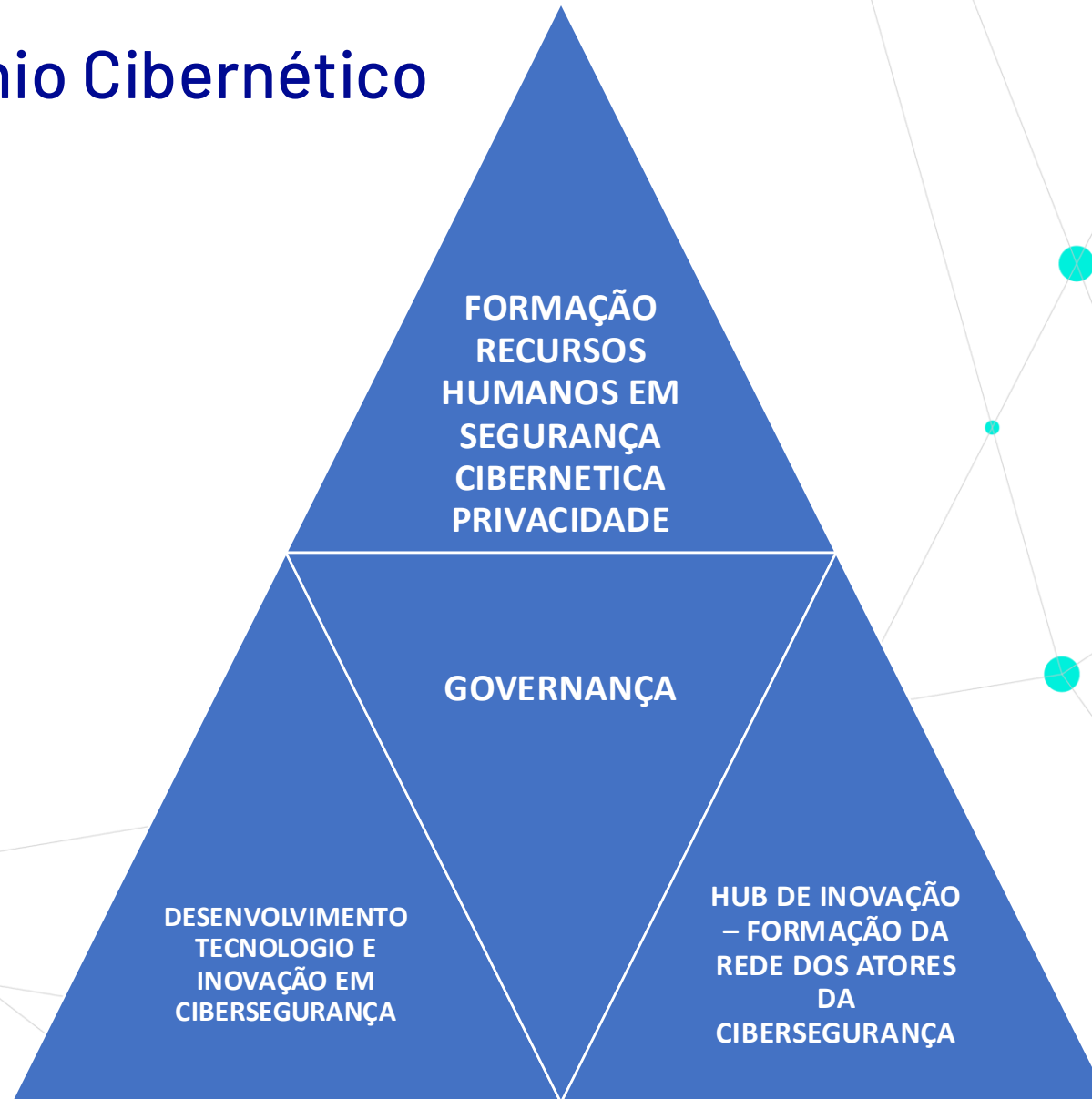
Capacitação



- Prover cursos específicos nos temas de cibersegurança e privacidade, com certificação profissional, desde seus fundamentos até a formação profissional.



Hackers do Bem no Domínio Cibernético



Alinhamento com marcos regulatórios

A segurança da informação nas universidades deve estar em conformidade com diversas normativas nacionais e internacionais.

O SOC RNP+ Contribui com a aderência às principais regulamentações do setor público.



Contribuição para atendimento normativo.

- **PPSI – Programa de Privacidade e Segurança da Informação**
Monitoramento contínuo, análise de vulnerabilidades e resposta a incidentes para atender aos controles de segurança exigidos.
- **LGPD – Lei Geral de Proteção de Dados**
Proteção contra vazamento de dados, controle de acessos e registros de eventos de segurança para garantir conformidade.
- **TCU-GOV e normativas de auditoria de segurança**
Relatórios detalhados, detecção de ameaças e gestão de riscos para suporte a auditorias e exigências regulatórias.

Escopo e objetivos do projeto

O SOC RNP+ fortalece a segurança cibernética das instituições do Sistema RNP, garantindo proteção contínua e aprimorando a governança da informação.

É um avanço estratégico que prepara as universidades para enfrentar os desafios digitais.

Monitoramento e resposta a ameaças

Identificação e mitigação de incidentes em tempo real, garantindo a continuidade das atividades.

Gestão padronizada de incidentes

Processos estruturados para resposta coordenada e eficaz a ataques.

Políticas e conformidade regulatória

Diretrizes de segurança alinhadas a PPSI, LGPD e TCU-GOV.

Capacitação e conscientização

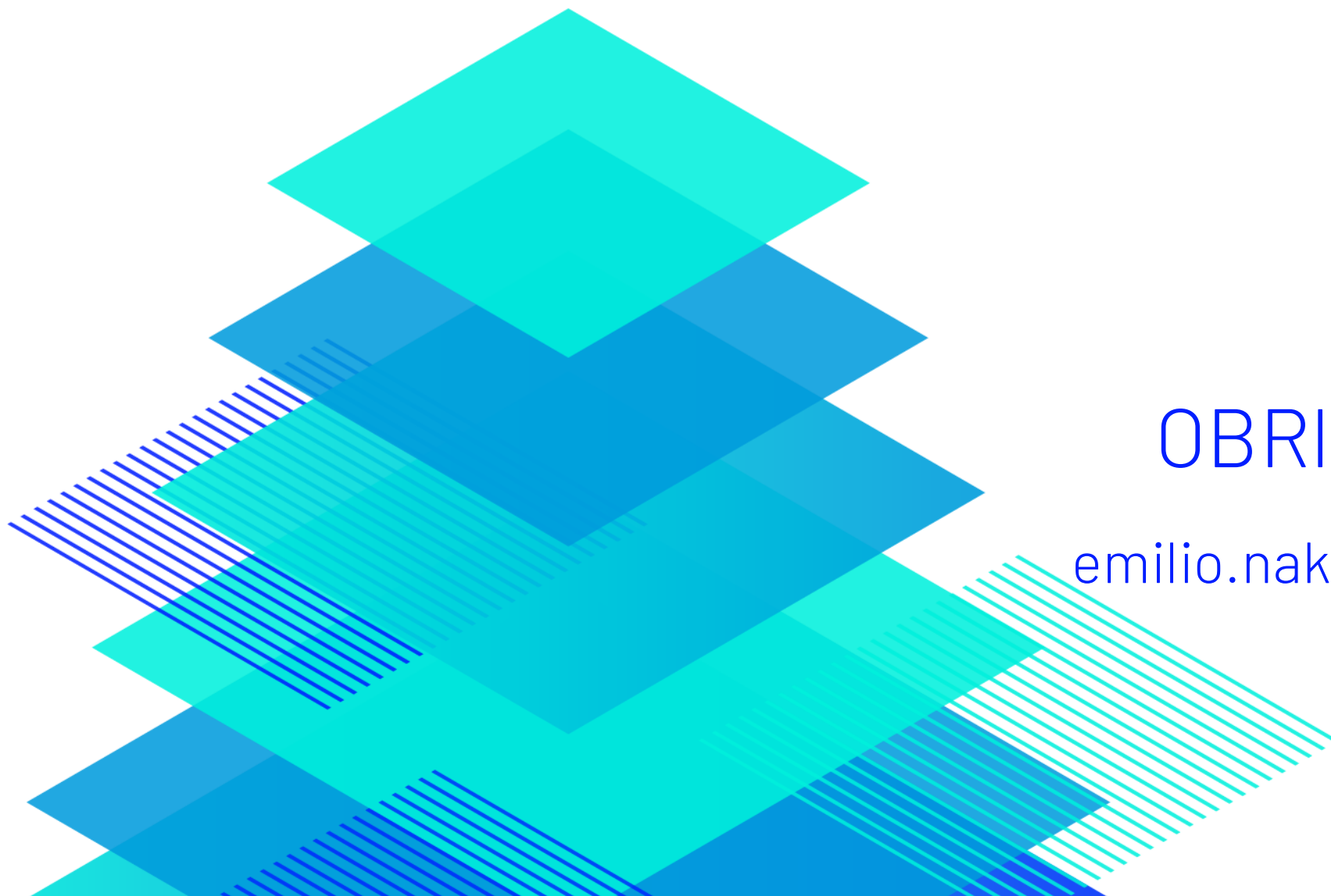
Treinamentos para equipes de TI e campanhas educativas sobre boas práticas de segurança.

Planos do SOC RNP+

	Básico	Intermediário
Monitoramento e mitigação de ataques de negação de serviço.	•	•
Email de Indicadores mensais.	•	•
Email de Indicadores semanais.		•
Gestão de vulnerabilidades (externas).		•
Visibilidade de ataques cibernéticos, vulnerabilidades, ameaças e ataques.		•
Classificação de riscos cibernéticos.		•
Evolução histórica dos riscos cibernéticos.		•
Relatório mensal com análise.		•
Notificação / interação.		•
Reunião mensal.		•
Monitoramento e mitigação de ataques na camada de aplicação.		•
Monitoramento de Credencias vazadas na Deep e Dark WEB		•
Correlação de Eventos (Limitado aos ADs)		•
Monitoramento interno endpoints.*		•



**Custo adicional pode ser aplicado, a depender do porte institucional*



OBRIGADO !!!

emilio.nakamura@rnp.br