cais Inteligência em Cibersegurança

RNP

Proteção e resiliência com o SOC de Coordenação e os SOCs Distribuídos

Ricardo Filipe T. M. de Melo
Analista de Segurança da Informação Core – SOC

Panorama Geral: Expansão dos SOCs e Cooperação em Segurança Cibernética

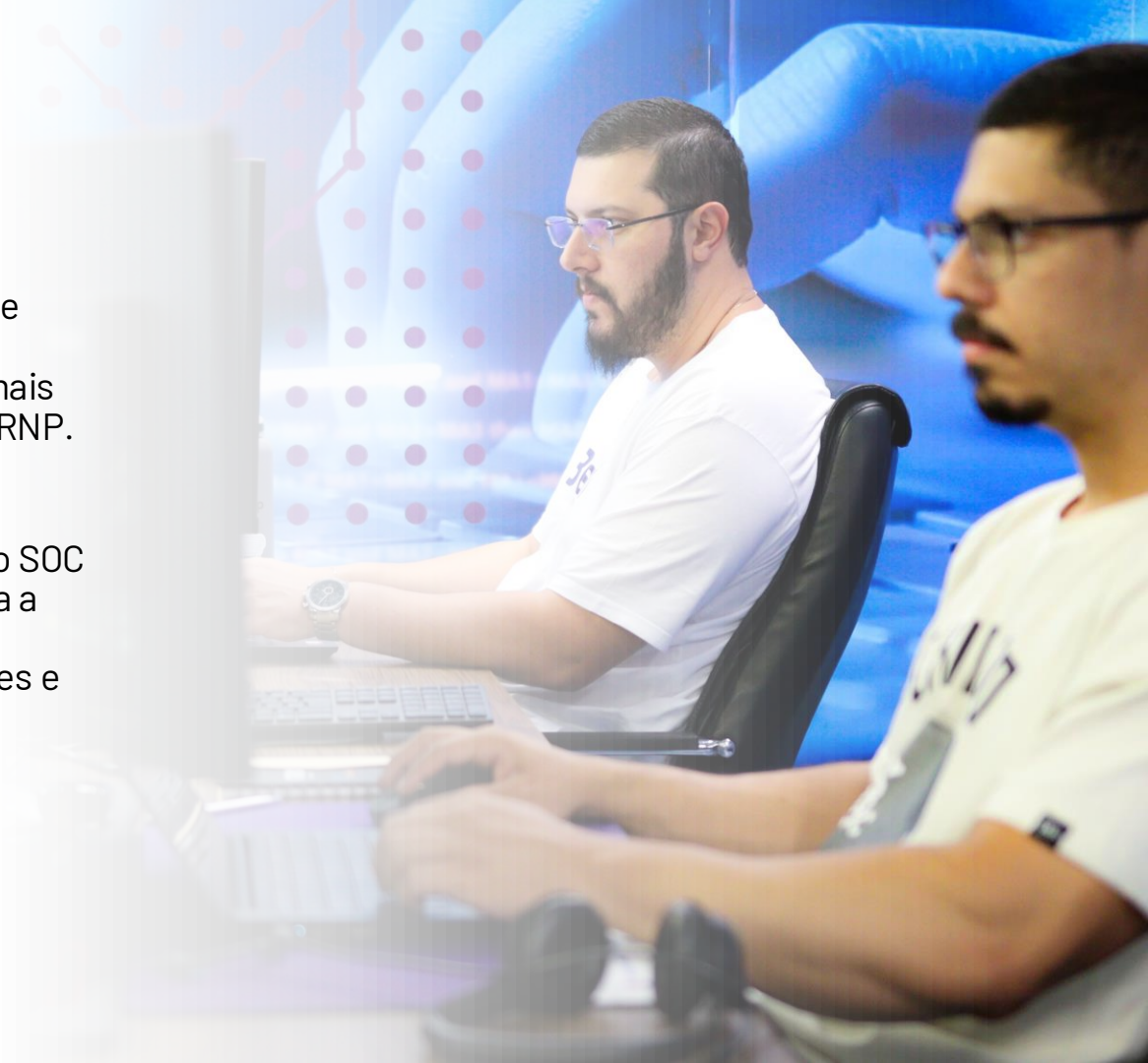
A crescente complexidade das ameaças cibernéticas exige uma atuação **coletiva, coordenada e estratégica.**

A estruturação do SOC-RNP, integrada a frentes de segurança ofensiva, defensiva, governança e privacidade, fortalece a resiliência das instituições conectadas. Para ampliar esse alcance, a RNP avança na criação de **SOCs Distribuídos**, em parceria com os estados, promovendo uma proteção digital mais **próxima, eficiente e contextualizada**.

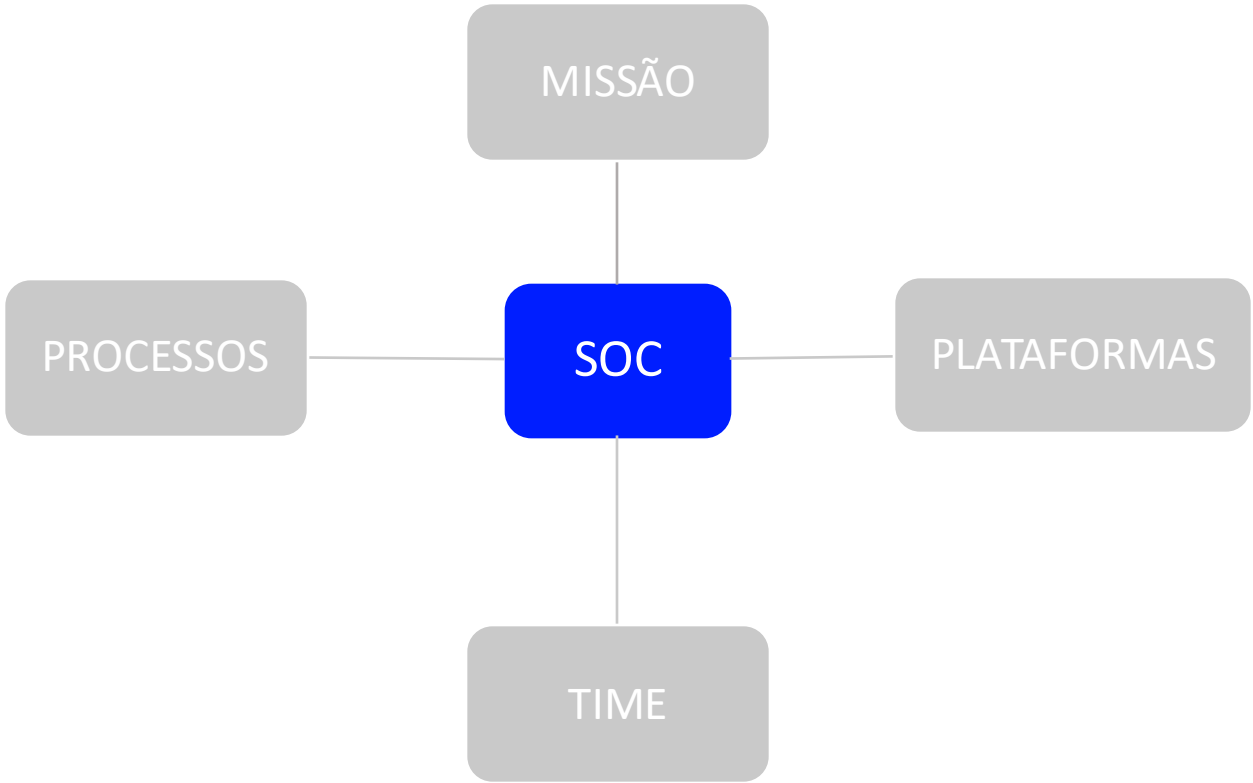
SOC-RNP

O **SOC-RNP** foi criado com o objetivo de fortalecer a cibersegurança das instituições de ensino, pesquisa e demais organizações que integram o sistema RNP.

Inaugurado em 29 de agosto de 2023, o SOC atua na identificação e resposta rápida a incidentes de segurança, com foco na interrupção do ciclo de vida dos ataques e na mitigação de impactos.

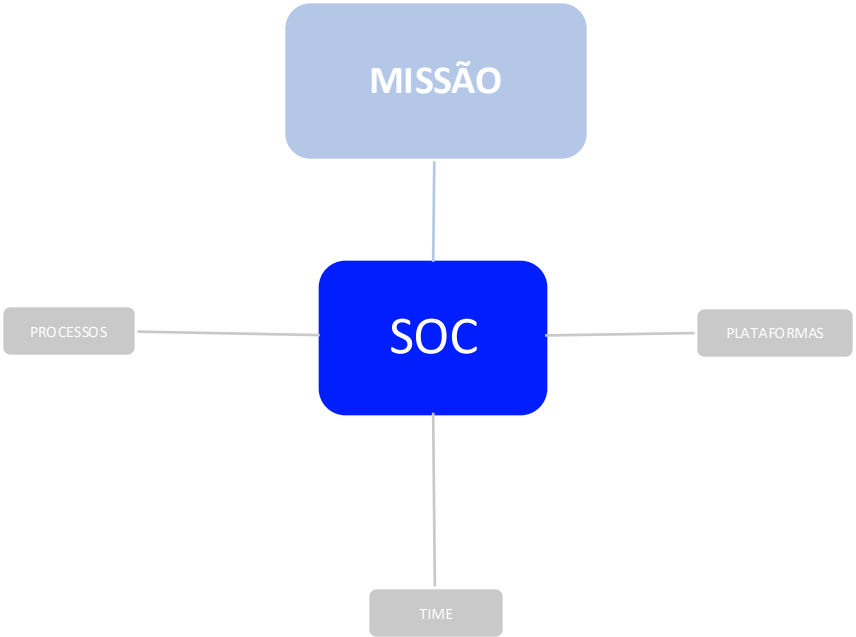


Abordagem holística

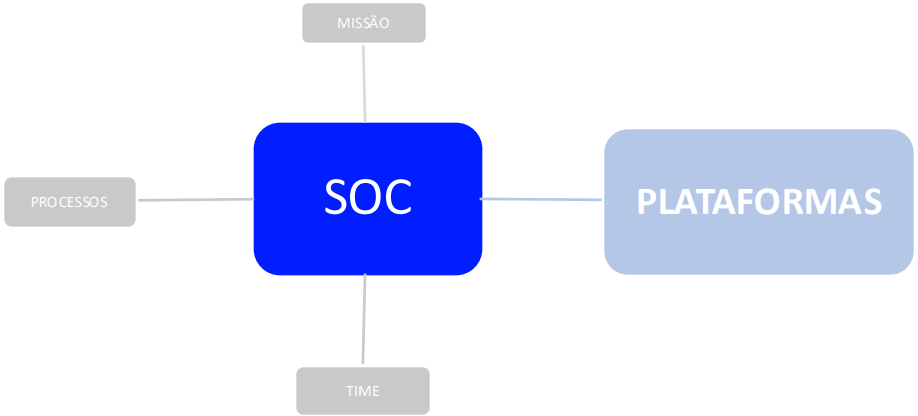


Abordagem holística

Visibilidade de Segurança	Agir com rapidez na detecção e resposta a incidentes	Interromper o ciclo de vida dos ataques	Prevenir ataques e reduzir seus impactos	Gerar capacidade	Inteligência de Segurança

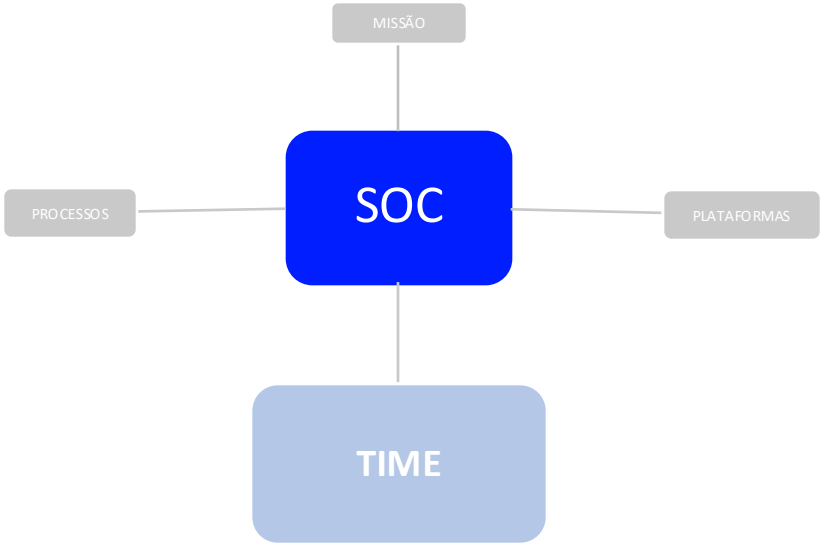


Abordagem holística



- Anti-DDoS
- WAAP
- Gestão de Vulnerabilidades
- Threat Intelligence
- Security Ratings
- SIEM
- XDR
- Proteção para Ambientes em Nuvem
- Firewall CND

Abordagem holística



SOC DE COORDENAÇÃO

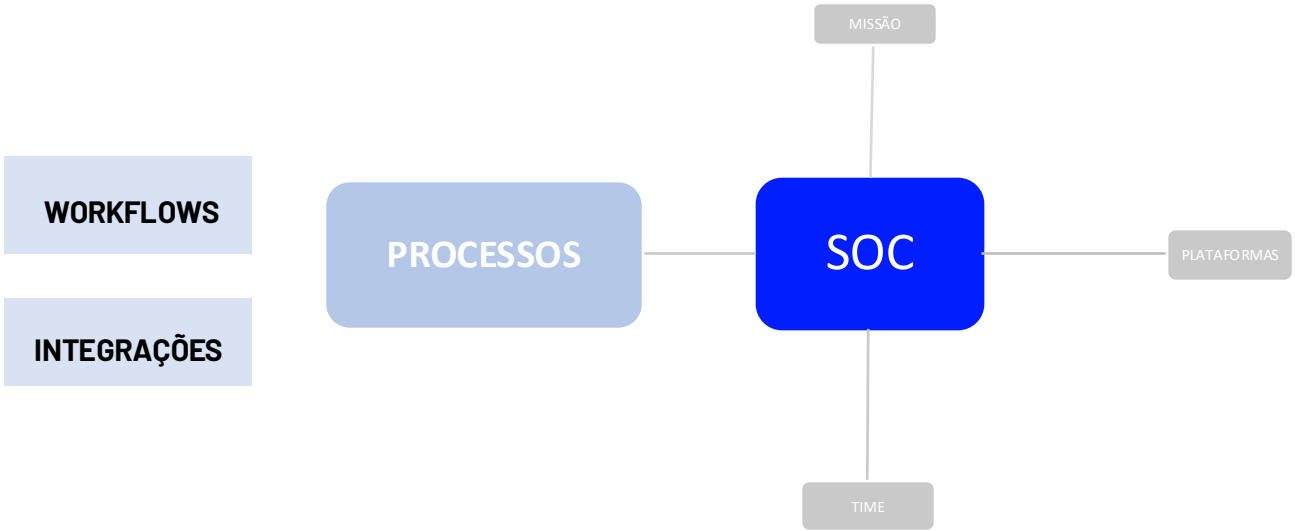
SOC DISTRIBUÍDO

NÍVEIS 1, 2 E 3

INTEGRAÇÃO

COBERTURA

Abordagem holística



O que é o SOC Distribuído?

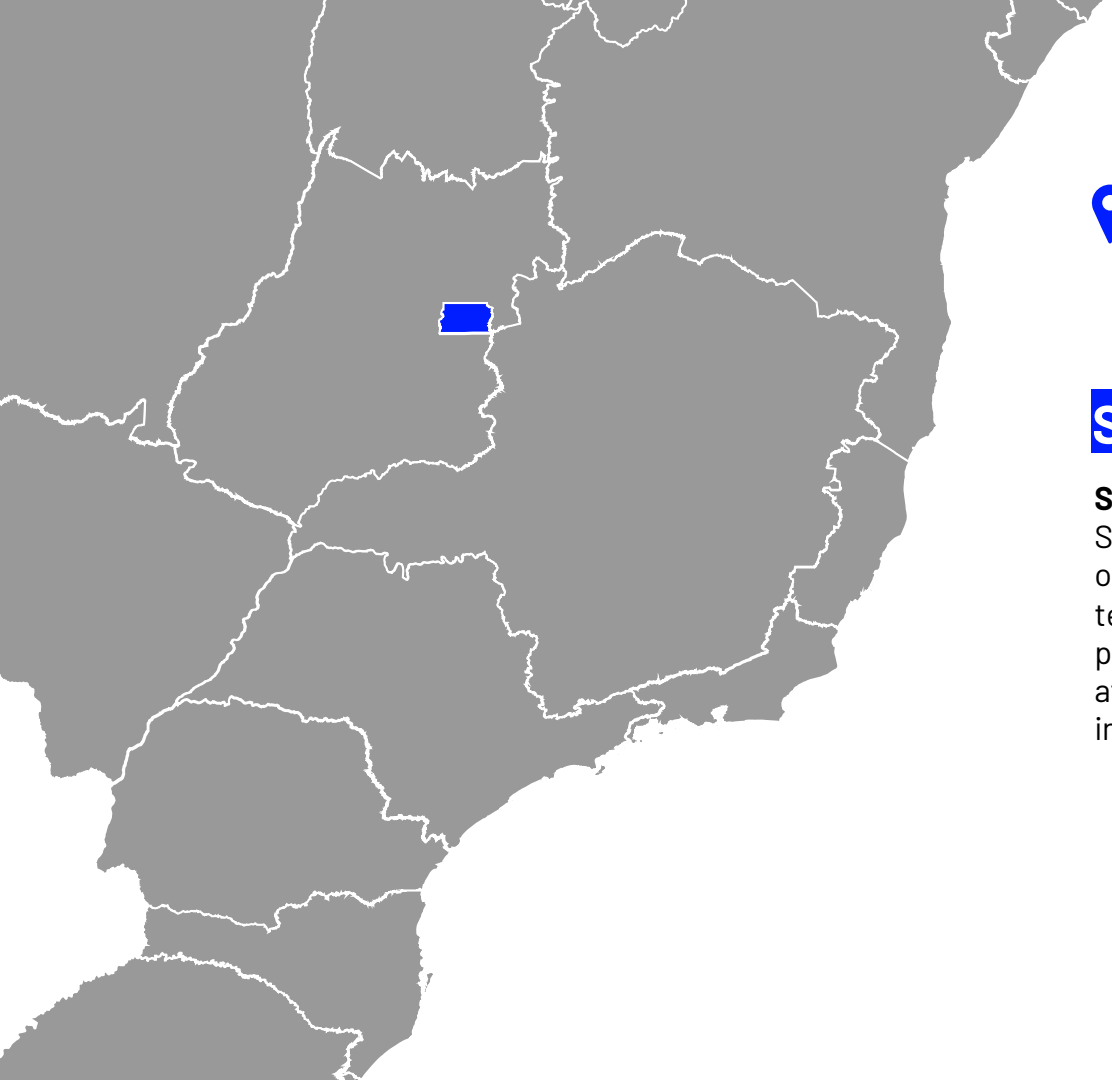
Estrutura local de cibersegurança implantada **nos estados** que opera de forma integrada com o **SOC-RNP**. Atua na resposta rápida e contextualizada a incidentes, fortalecendo a proteção regional das instituições conectadas.

Por que é estratégico?

- Aumenta a visibilidade e resiliência
- Eleva a maturidade cibernética nos territórios
- Base para a construção da **Rede Federada de Cibersegurança**
- Promove o desenvolvimento de capacidades locais em cibersegurança

SOCs Distribuídos

Infraestrutura física e tecnológica local nos estados, com times de cibersegurança com a missão de proteger e monitorar ativamente as instituições locais contra ameaças cibernéticas.
Orquestrado, organizado e integrado com o SOC de Coordenação.



BRASÍLIA - DF
RNP

SOC de Coordenação

SOC-RNP, responsável por orquestrar os SOCs Distribuídos, garantindo as operações **24x7x365**, as atualizações tecnológicas, o cumprimento dos processos, a qualidade nas entregas e uma atuação eficiente e rápida em casos de incidentes de segurança.

Escala Operacional do SOC Distribuído

Cobertura 24x7

SOC Distribuído opera horário comercial (9h às 18h) de segunda a sexta.

SOC de Coordenação – Monitoramento contínuo em uma escala 12x36, garantindo uma cobertura contínua de 24 horas por dia, 7 dias por semana.

Transição de Turno

A transição de turno entre os SOCs regionais e o SOC de Coordenação é feita por meio de uma chamada no Teams, garantindo o repasse eficaz das informações e a continuidade do monitoramento.

Segurança Física

O monitoramento é realizado de forma presencial em uma sala com controle de acesso e câmeras de vigilância, garantindo a confidencialidade das informações monitoradas pelo SOC.

Estrutura

A estrutura do SOC Estadual foi pensada para otimizar o monitoramento e garantir a confidencialidade das informações.

- Sala Fechada
- Controle de acesso físico
- Câmera de vigilância
- Vídeo Wall
- Estrutura física (Mesa, cadeira...)
- Equipamentos para a operação

Rede Federada de cibersegurança

- Estrutura **colaborativa, descentralizada e em expansão**
- Formada pelos **SOCs Distribuídos integrados ao SOC-RNP**
- Fortalece a proteção digital em ensino, pesquisa e inovação
- Desenvolve capacidades locais de forma coordenada
- Atua com **padrões unificados** e **resposta coletiva a incidentes**

Rede Federada de cibersegurança

Alinhada às diretrizes nacionais

- Estratégia Nacional de Segurança Cibernética (e-Ciber)
- Programa de Privacidade e Segurança da Informação (PPSI)
- Lei Geral de Proteção de Dados (LGPD)

A Rede Federada eleva a maturidade e a conformidade em segurança, aumenta a resiliência e a capacidade de resposta das instituições, democratiza o acesso à proteção cibernética e estimula uma cultura nacional de cibersegurança.

Conclusão //

A implantação dos SOCs Distribuídos marca um passo decisivo na construção da Rede Federada de Cibersegurança.

Essa rede amplia a maturidade, a visibilidade e a capacidade de resposta das instituições em todo o território nacional, estimulando o desenvolvimento local e a cultura de cibersegurança.

Atuando de forma coordenada com o SOC-RNP, os SOCs Distribuídos consolidam uma abordagem integrada que fortalece a resiliência cibernética em todo o ecossistema de ensino, pesquisa e inovação.

OBRIGADO!