cais Inteligência em Cibersegurança RNP

Transformando Incidentes em Inteligência

A Sinergia entre Gestão de Riscos e Resposta a Incidentes

Ingrid Barbosa

CAIS - RNP

SEXTA-FEIRA – 11:00

SEXTA-FEIRA – 12:00

DOMINGO – 03:00

Como evitamos que isso aconteça de novo?

Estamos documentando...

mas estamos aprendendo?

RESPONDER
DOCUMENTAR
ESQUECER
REPETIR

Transformar incidentes em INTELIGÊNCIA

RNP

TLP:CLEAR

Temos mais tecnologia do que nunca

Mas os mesmos problemas continuam acontecendo

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

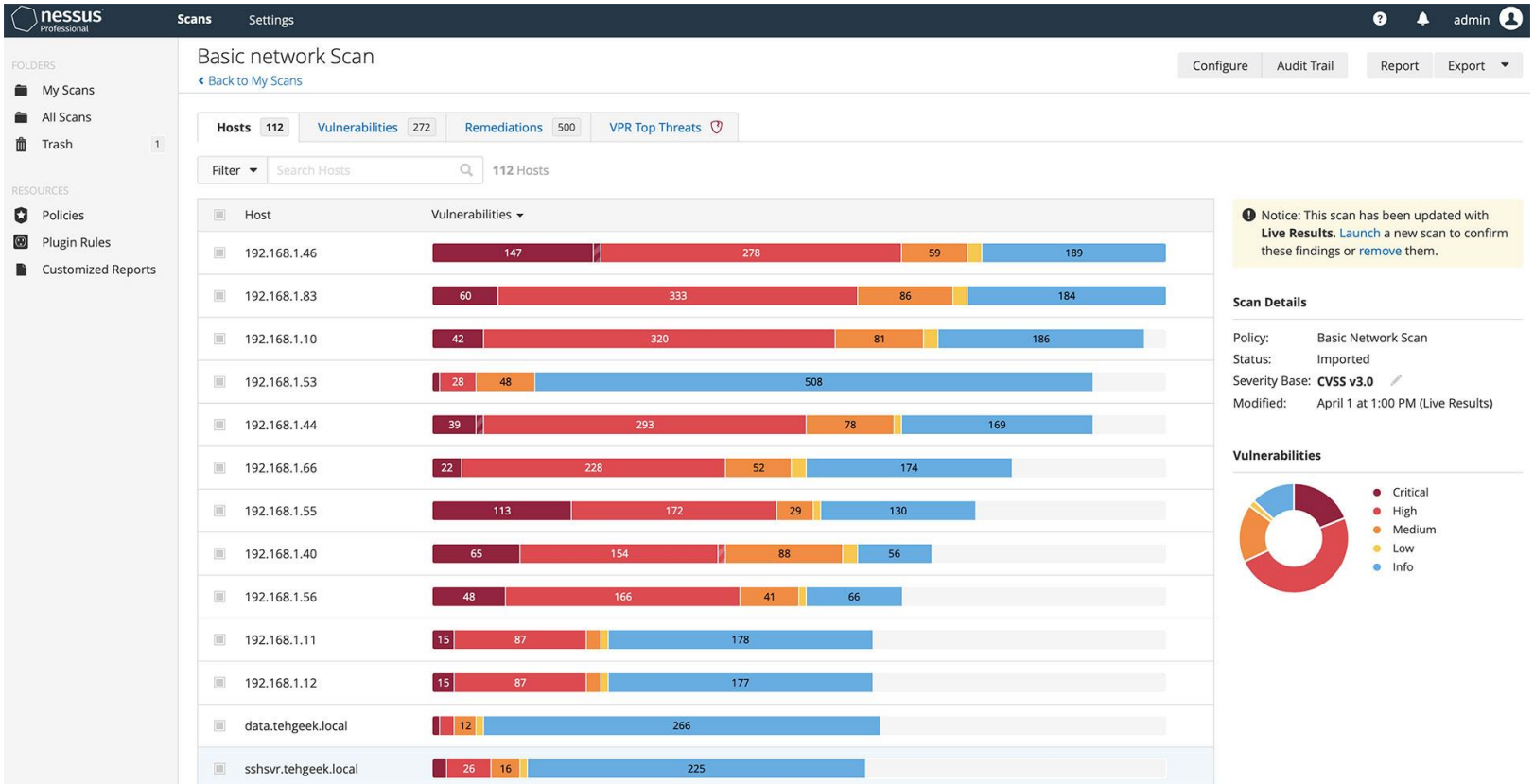
20% complete

Estamos buscando as melhores soluções ...

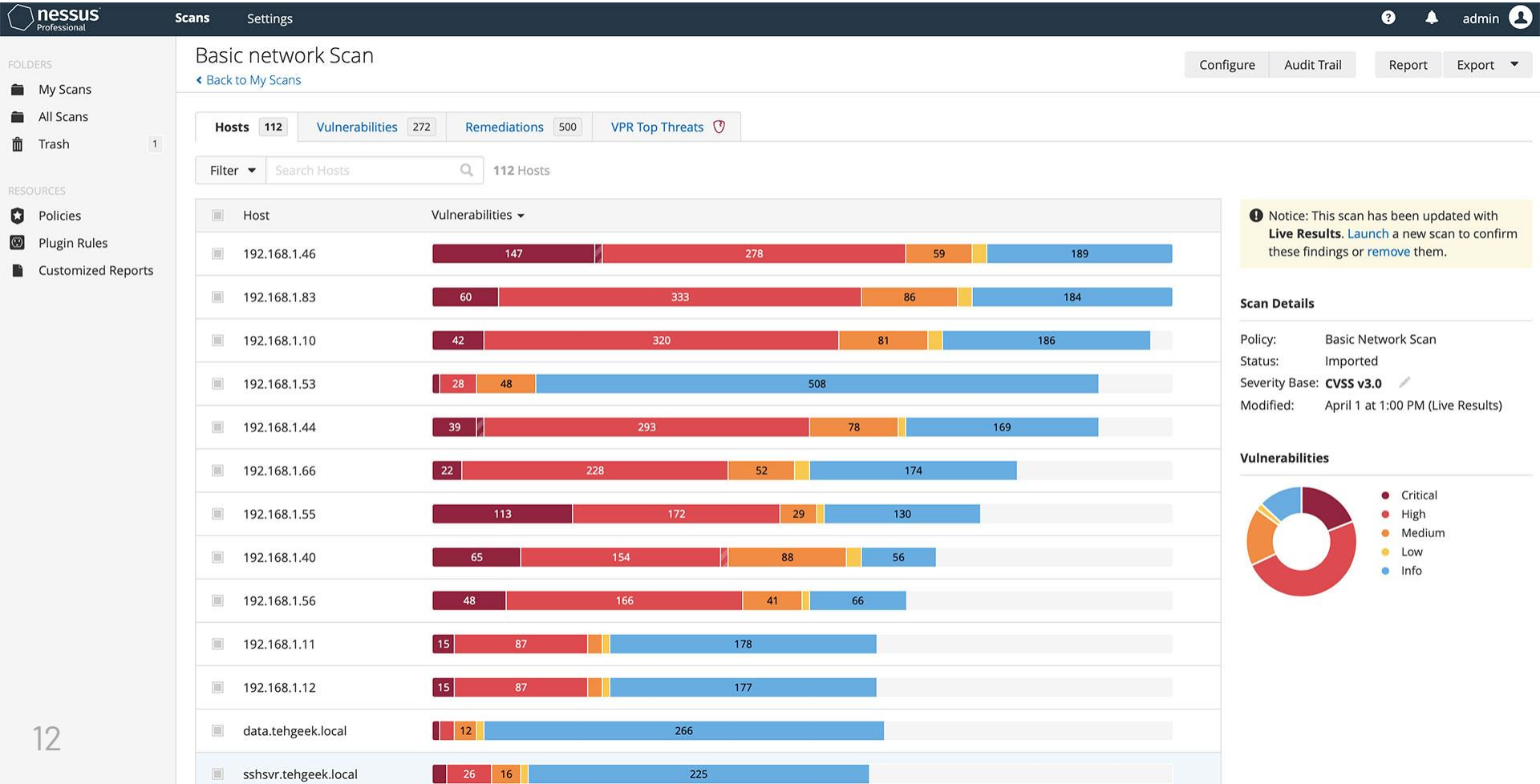
...mas falhando no básico

RESPONDER
DOCUMENTAR
ESQUECER
REPETIR

Relatórios mostram falhas



mas não mostram contexto


nessus Professional
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash 1
RESOURCES
Policies
Plugin Rules
Customized Reports
Basic network Scan
Back to My Scans
Configure
Audit Trail
Report
Export
Hosts 112
Vulnerabilities 272
Remediations 500
VPR Top Threats
Filter
Search Hosts
112 Hosts
Host
Vulnerabilities
192.168.1.46 147 278 59 189
192.168.1.83 60 333 86 184
192.168.1.10 42 320 81 186
192.168.1.53 28 48 508
192.168.1.44 39 293 78 169
192.168.1.66 22 228 52 174
192.168.1.55 113 172 29 130
192.168.1.40 65 154 88 56
192.168.1.56 48 166 41 66
192.168.1.11 15 87 178
192.168.1.12 15 87 177
data.tehgeek.local 12 266
sshsvr.tehgeek.local 26 16 225
Notice: This scan has been updated with Live Results. Launch a new scan to confirm these findings or remove them.
Scan Details
Policy: Basic Network Scan
Status: Imported
Severity Base: CVSS v3.0
Modified: April 1 at 1:00 PM (Live Results)
Vulnerabilities
Critical
High
Medium
Low
Info

Não podemos nos proteger contra tudo

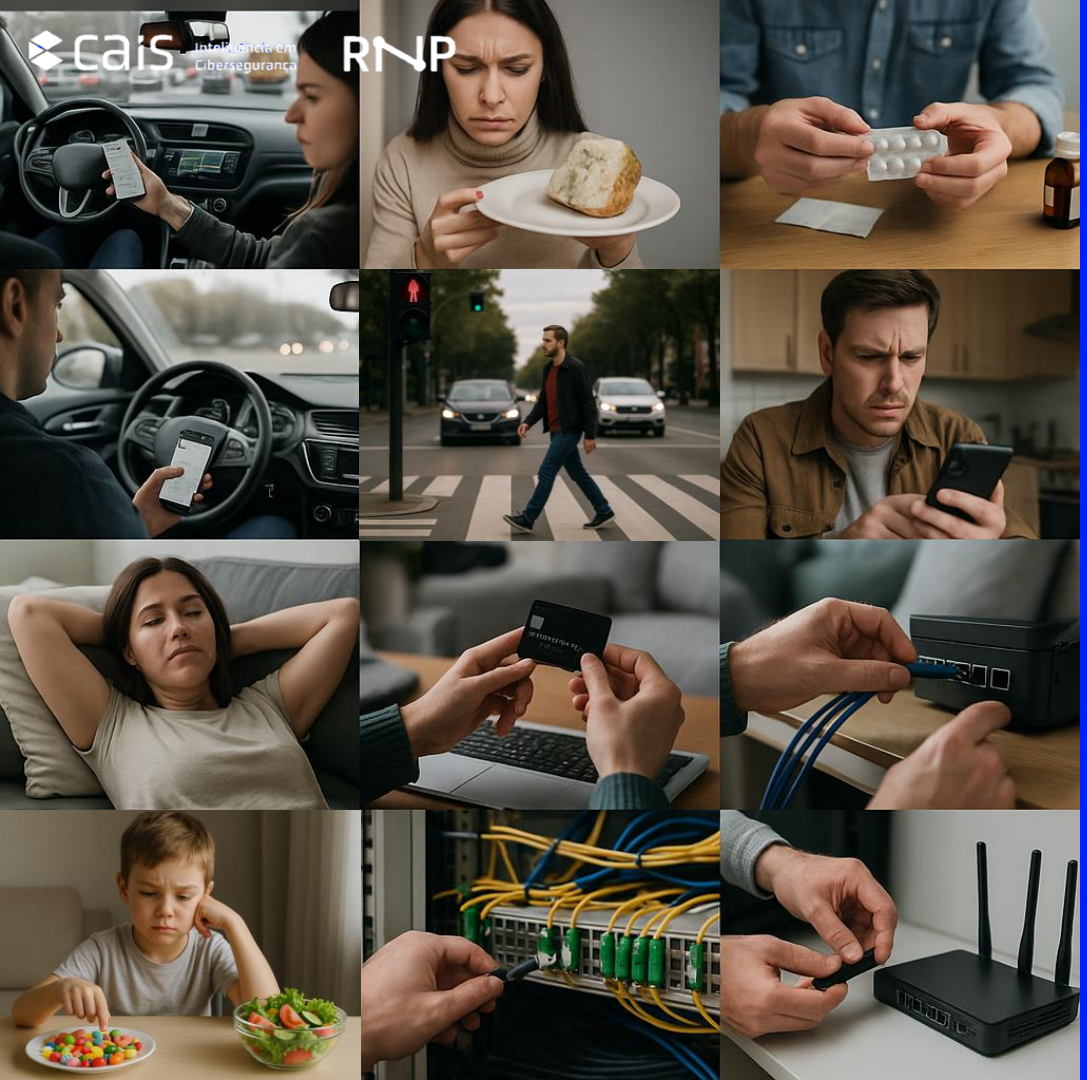
O risco é o que pode acontecer

O incidente é o que já aconteceu

INCIDENTE é o RISCO que se materializou

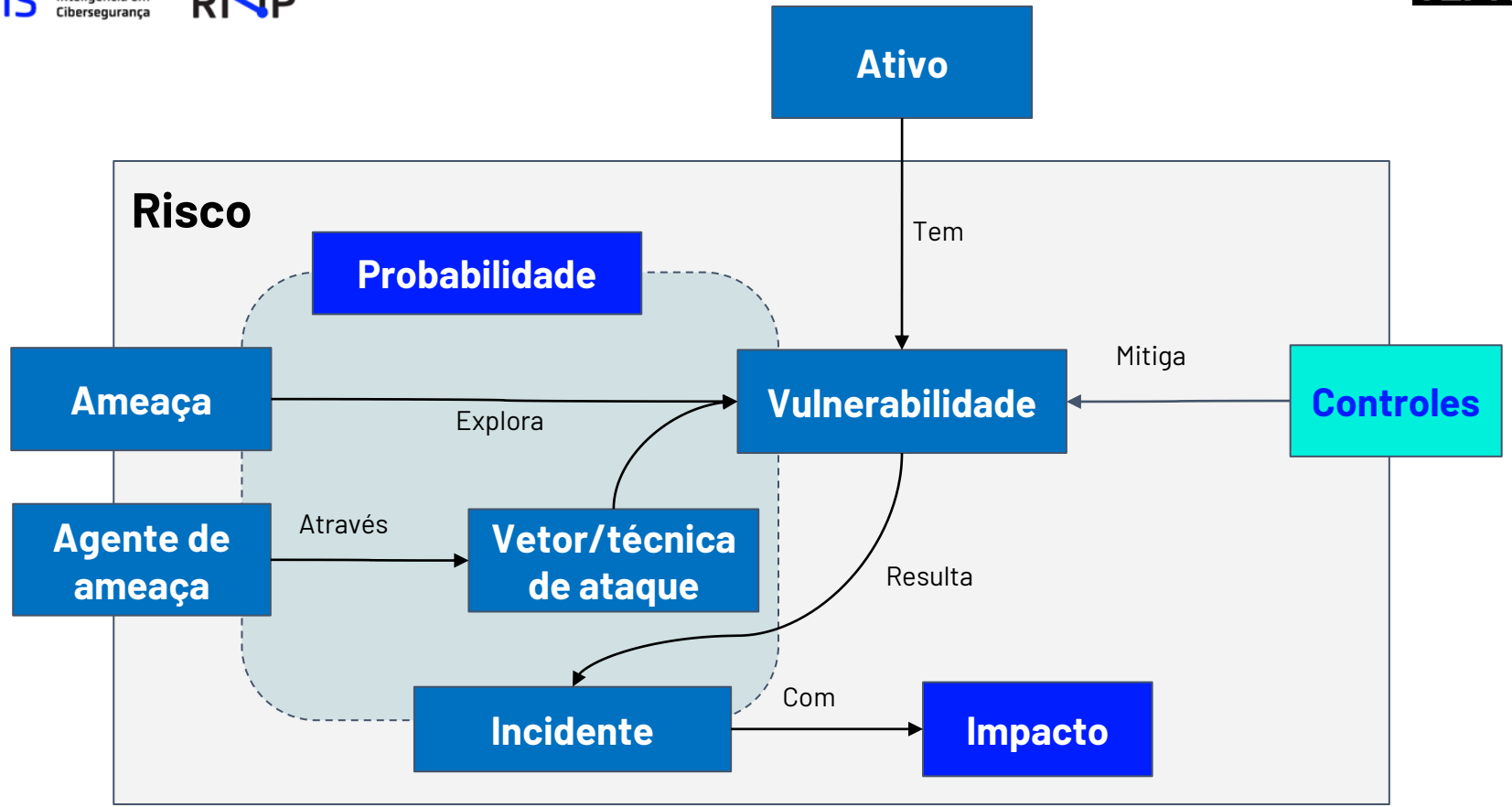
“Preservação da Confidencialidade, Integridade e Disponibilidade da Informação, a partir de um processo de gestão de riscos (...)”

ISO/IEC 27001:2022

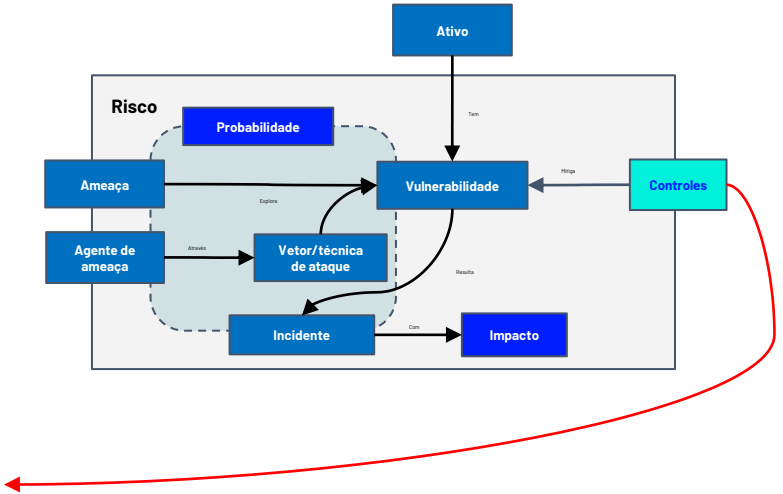


Avaliar riscos é uma habilidade inerente dos seres humanos

Mas nossas decisões são baseadas em nossas vivências


Ativo
Tem
Risco
Probabilidade
Ameaça
Explora
Vulnerabilidade
Mitiga
Controles
Agente de ameaça
Através
Vetor/técnica de ataque
Resulta
Incidente
Com
Impacto

Efetividade dos controles



Com qual frequência sua organização toma decisões formais baseada em riscos?

1 – Falta de claridade em como levar os conceitos teóricos para a prática

2 – Tendência de priorizar o que parece urgente, em detrimento do que é realmente importante

TLP:CLEAR

cais

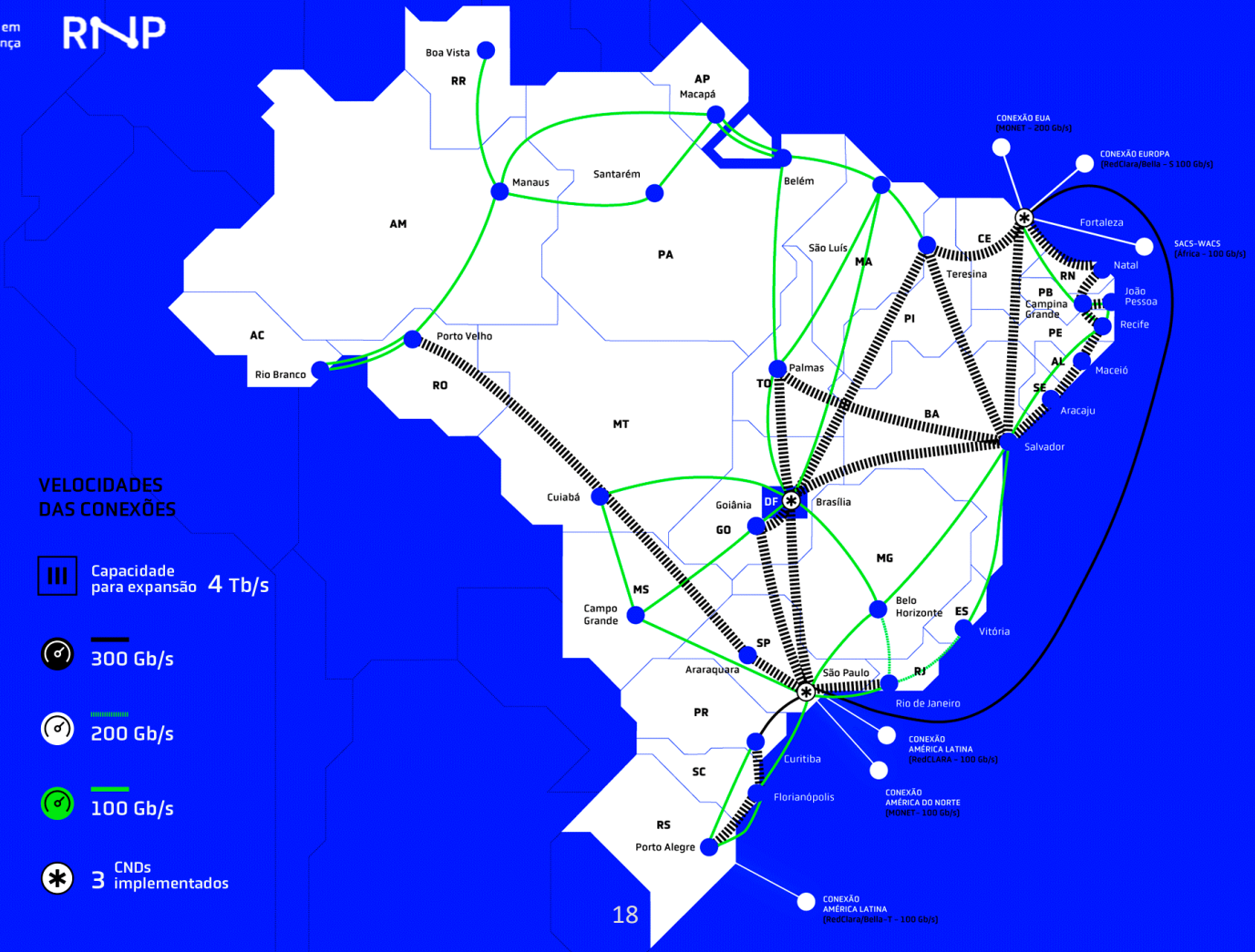
O CAIS-RNP foi pioneiro ao começar discussões em segurança da informação, sendo um dos primeiros grupos de resposta a incidentes (Csirts) a atuar no Brasil.

Hoje, a área abrange diversas competências e é reconhecida nacional e internacionalmente pela experiência e amplo escopo de atuação.

Há 26 anos, o CAIS-RNP garante a segurança em centenas de instituições de educação e pesquisa brasileiras. A área de inteligência em cibersegurança da RNP desenvolve ações preventivas, educativas e corretivas em incidentes e ameaças na rede acadêmica, que enfrenta diariamente os desafios ligados ao aumento da complexidade de ameaças cibernéticas.

cais Inteligência em Cibersegurança RNP

TLP:CLEAR



VELOCIDADES DAS CONEXÕES

Capacidade para expansão 4 Tb/s

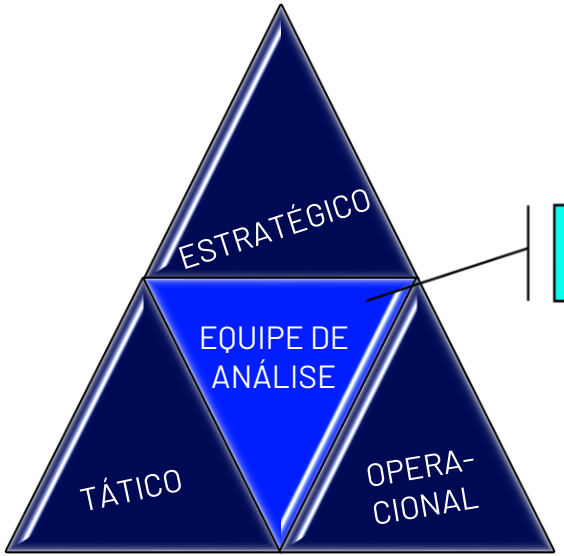
300 Gb/s

200 Gb/s

100 Gb/s

3 CNDs implementados

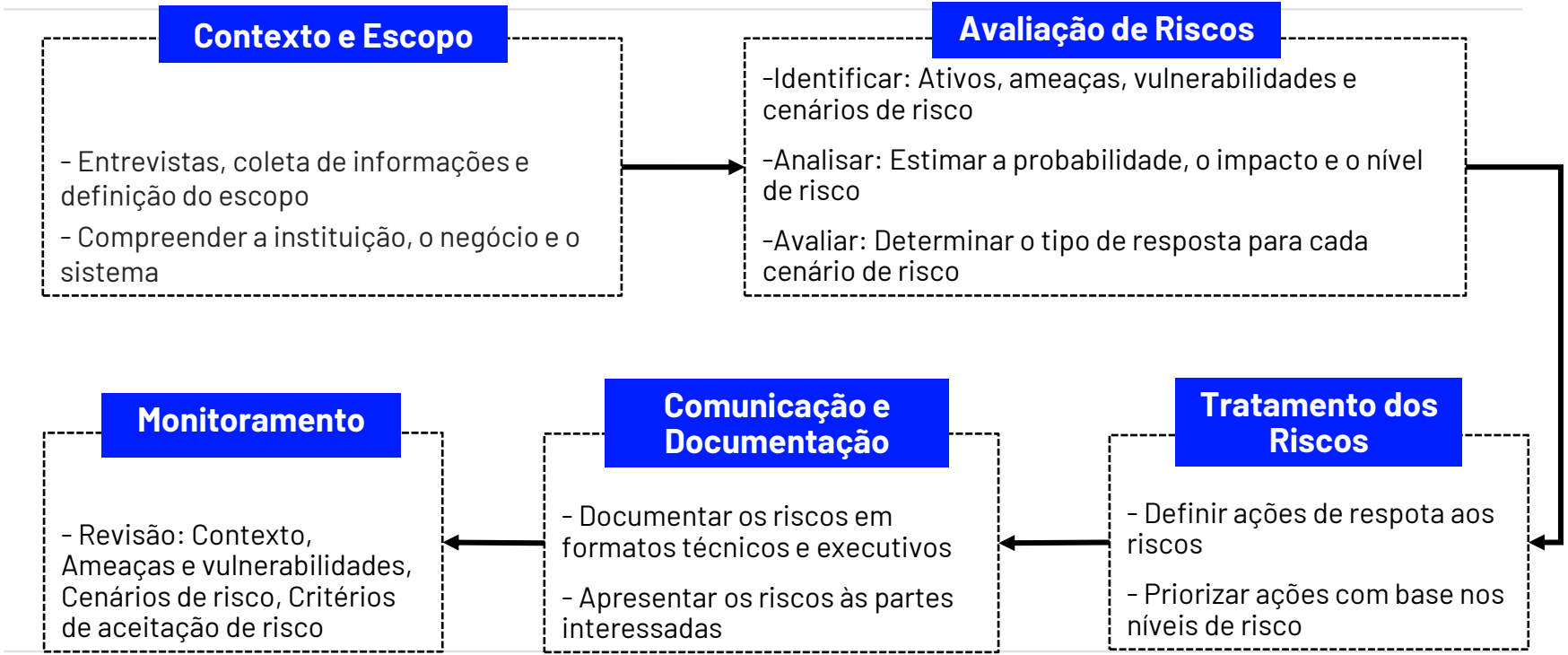
Abordagem tridimensional



RNP + CLIENTE

- ENTREVISTAS
- ANÁLISE DE DOCUMENTAÇÃO
- VISITAS TÉCNICAS

Gerenciamento de Riscos Cibernéticos



Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Setor financeiro – envolve valores monetários diretamente – desenvolvedores de empresa terceira – nível júnior, menor cultura organizacional voltada para ética e integridade. Desenvolvedor com permissões de acesso e escrita em servidor crítico.

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

-Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco

-Analisar: Estimar a probabilidade, o impacto e o nível de risco

-Avaliar: Determinar o tipo de resposta para cada cenário de risco

Ativo: Workforce (humano) – desenvolvedor júnior terceirizado

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

-Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco

-Analisar: Estimar a probabilidade, o impacto e o nível de risco

-Avaliar: Determinar o tipo de resposta para cada cenário de risco

Spoofing - Falsificação

Privilégios desnecessários ou mal controlados

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

-Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco

-Analisar: Estimar a probabilidade, o impacto e o nível de risco

-Avaliar: Determinar o tipo de resposta para cada cenário de risco

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

-Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco

-Analisar: Estimar a probabilidade, o impacto e o nível de risco

-Avaliar: Determinar o tipo de resposta para cada cenário de risco

Falha, Destruição, Perda, Mau Funcionamento, Roubo, Interrupção e outros...

Roubo de valores monetários mascarado de atividade legítima

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

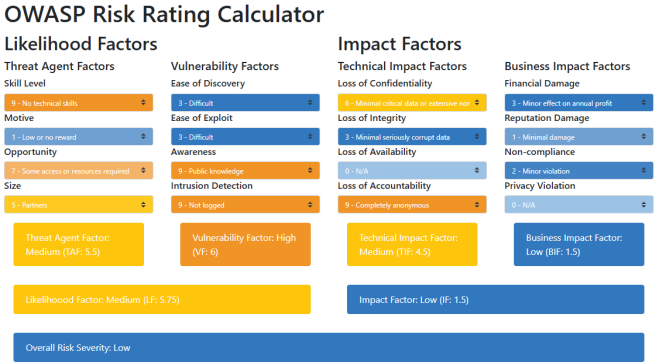
Avaliação de Riscos

-Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco

-Analisar: Estimar a probabilidade, o impacto e o nível de risco

-Avaliar: Determinar o tipo de resposta para cada cenário de risco

Falha, Destruição, Perda, Mau Funcionamento, Roubo, Interrupção e outros...



OWASP Risk Rating Calculator

Likelihood Factors

Threat Agent Factors

Skill Level

9 - No technical skills

Motive

1 - Low or no reward

Opportunity

7 - Some access or resources required

Size

5 - Partners

Vulnerability Factors

Ease of Discovery

3 - Difficult

Ease of Exploit

3 - Difficult

Awareness

9 - Public knowledge

Intrusion Detection

9 - Not logged

L = Média

Impact Factors

Technical Impact Factors

Loss of Confidentiality

6 - Minimal critical data or extensive nor

Loss of Integrity

3 - Minimal seriously corrupt data

Loss of Availability

0 - N/A

Loss of Accountability

9 - Completely anonymous

Financial Impact Factors

Financial

3 - Minor effect on annual

Reputation Damage

1 - Minimal damage

Non-compliance

2 - Minor violation

Privacy Violation

0 - N/A

L = Muito Alto

Threat Agent Factor: Medium (TAF: 5.5)

Vulnerability Factor: High (VF: 6)

Technical Impact Factor: Medium (TIF: 4.5)

Business Impact Factor: Low (BIF: 1.5)

Likelihoood Factor: Medium (LF: 5.75)

Impact Factor: Low (IF: 1.5)

Overall Risk Severity: Low

L = Alto

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

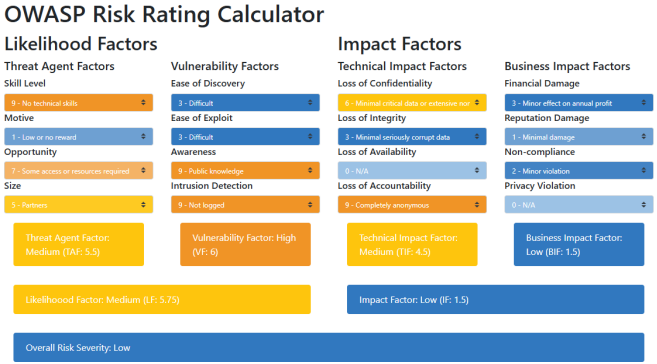
Avaliação de Riscos

-Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco

-Analisar: Estimar a probabilidade, o impacto e o nível de risco

-Avaliar: Determinar o tipo de resposta para cada cenário de risco

Falha, Destruição, Perda, Mau Funcionamento, Roubo, Interrupção e outros...



1. Evitar
2. Mitigar
3. Transferir
4. Aceitar

MITIGAR

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

-Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco

-Analisar: Estimar a probabilidade, o impacto e o nível de risco

-Avaliar: Determinar o tipo de resposta para cada cenário de risco

Tratamento dos Riscos

- Definir ações de resposta aos riscos
- Priorizar ações com base nos níveis de risco

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

-Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco

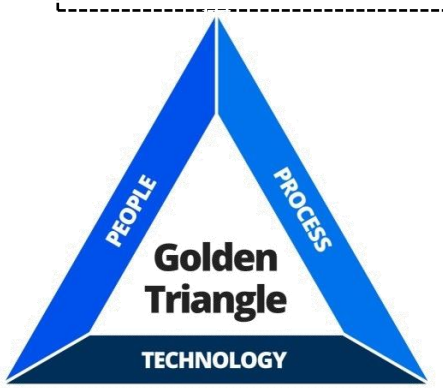
-Analisar: Estimar a probabilidade, o impacto e o nível de risco

-Avaliar: Determinar o tipo de resposta para cada cenário de risco

Tratamento dos Riscos

- Definir ações de resposta aos riscos

- Priorizar ações com base nos níveis de risco



- Revisão de normas de acesso
- Processo de Gestão de acessos
- Regras no SIEM baseado em comportamento
- Treinamento (ética, engenharia social, corrupção

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

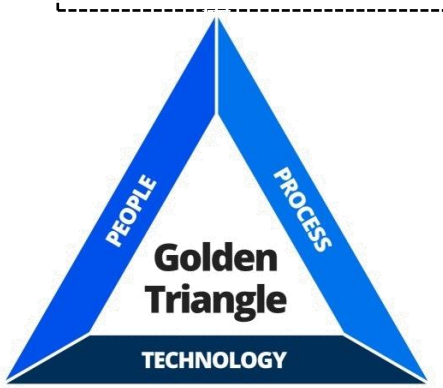
- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

-Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco

-Analisar: Estimar a probabilidade, o impacto e o nível de risco

-Avaliar: Determinar o tipo de resposta para cada cenário de risco



RISCOS ASSOCIADOS

CRITICIDADE DOS RISCOS

SCORE

Tratamento dos Riscos

- Definir ações de resposta aos riscos
- Priorizar ações com base nos níveis de risco

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e o sistema

Avaliação de Riscos

-Identificar: Ativos, ameaças, vulnerabilidades e cenários de risco

-Analisar: Estimar a probabilidade, o impacto e o nível de risco

-Avaliar: Determinar o tipo de resposta para cada cenário de risco

Tratamento dos Riscos

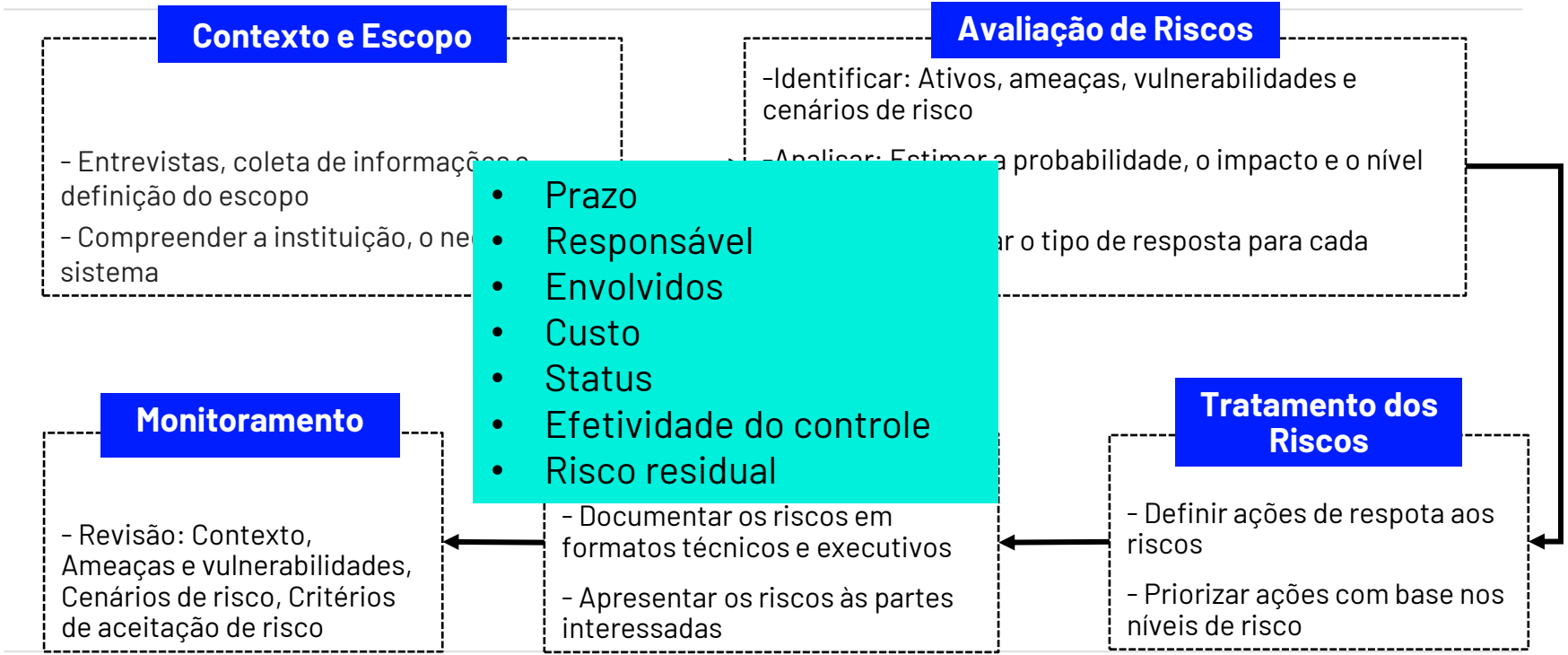
- Definir ações de respota aos riscos
- Priorizar ações com base nos níveis de risco

Comunicação e Documentação

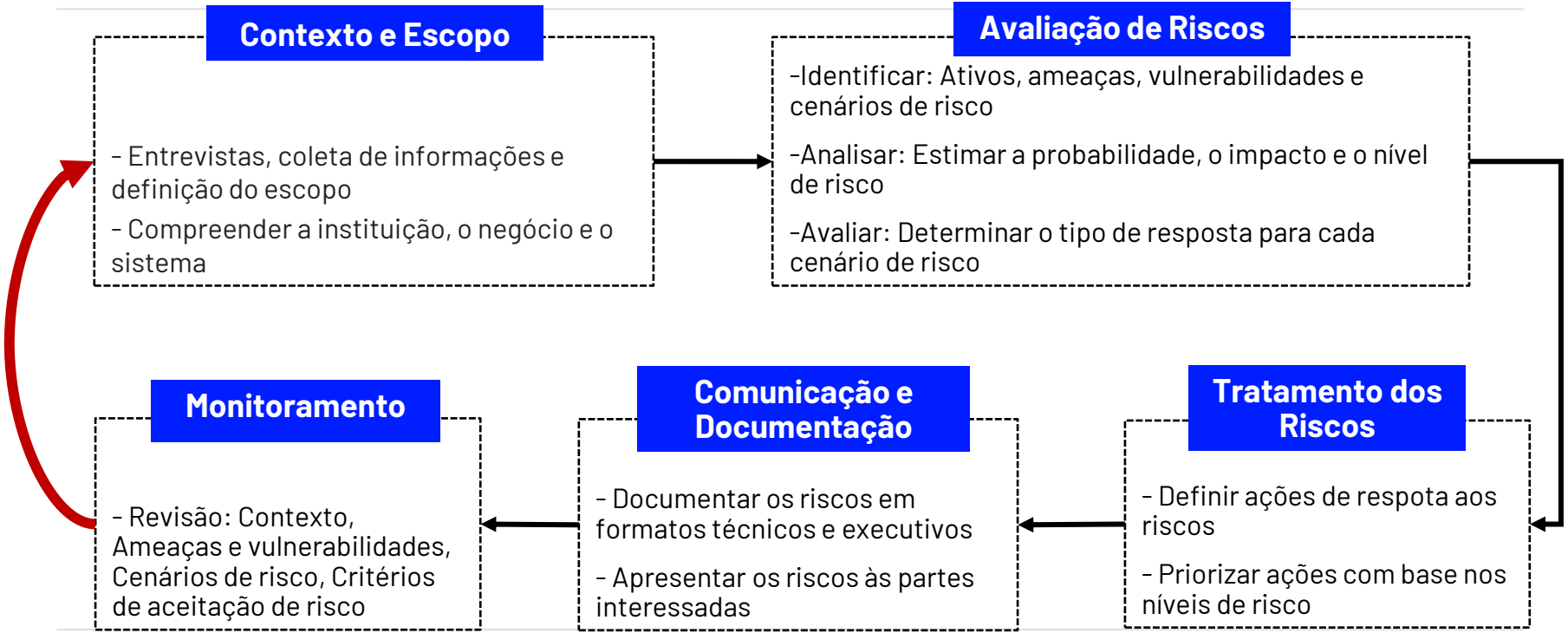
- Documentar os riscos em formatos técnicos e executivos
- Apresentar os riscos às partes interessadas

Carta de risco – Use a comunicação como força

Gerenciamento de Riscos Cibernéticos



Gerenciamento de Riscos Cibernéticos



Lições aprendidas

- A gestão de riscos é viva. Sempre pergunte: “O que mudou? O que aprendemos com o último incidente?”
- Comece pequeno, escale com inteligência. Inicie com escopos menores e expanda conforme a maturidade aumenta.
- Comunique-se diretamente, sem intermediários. Clareza gera engajamento.
- Espere (e supere) resistência. Desconforto é sinal de que o status quo está sendo desafiado.
- Na dúvida, assuma o pior. Em avaliações, sempre erre pelo lado da cautela.
- Comemore as conquistas. Mesmo pequenas mitigações de risco merecem reconhecimento.
- Colaboração é inegociável. A cibersegurança é responsabilidade de todos.
- A cultura devora a estratégia. Com prática, o pensamento orientado a riscos e integrado às equipes de resposta a incidentes começa a se tornar algo natural.

Incidentes mostram onde o risco é mais do que uma hipótese. Separados, riscos e incidentes só reagem. Juntos, antecipam.

Ingrid Barbosa
Information Security | Cyber risks | IoT and Smart Cities | Blockchain |

OBRIGADA!

ingrid.barbosa@rnp.br