cais Inteligência em Cibersegurança RNP

Segurança na rede e-Ciência: Ações proativas e reativas contra ameaças cibernéticas

Andre Landim

João Pedro de Lima Cassiano Pereira

Ricardo Filipe Terra M. Melo

5.760.000

5.760.000

Número de ataques cibernéticos que ocorrem na américa latina até o final dessa apresentação.

Cenário de Segurança Cibernética

1.600+

Ataques por segundo na América Latina

Source: The State of OT Cyber Security in LATAM 2024 Annual Report CS4CA

Cenário de Segurança Cibernética

1.600+

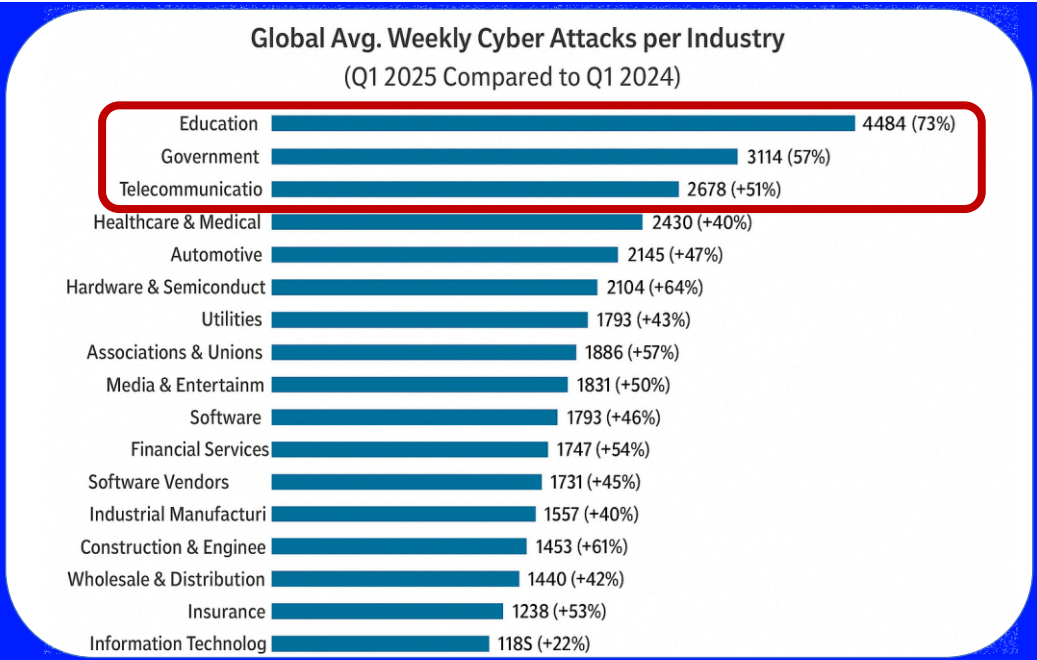
Ataques por segundo na América Latina

60%

Ações reativas ao invés de preventiva

Source: The State of OT Cyber Security in LATAM 2024 Annual Report CS4CA

Cenário de Segurança Cibernética



Source: Global Cybersecurity Outlook 2025 – The World Economic Forum

1.600+

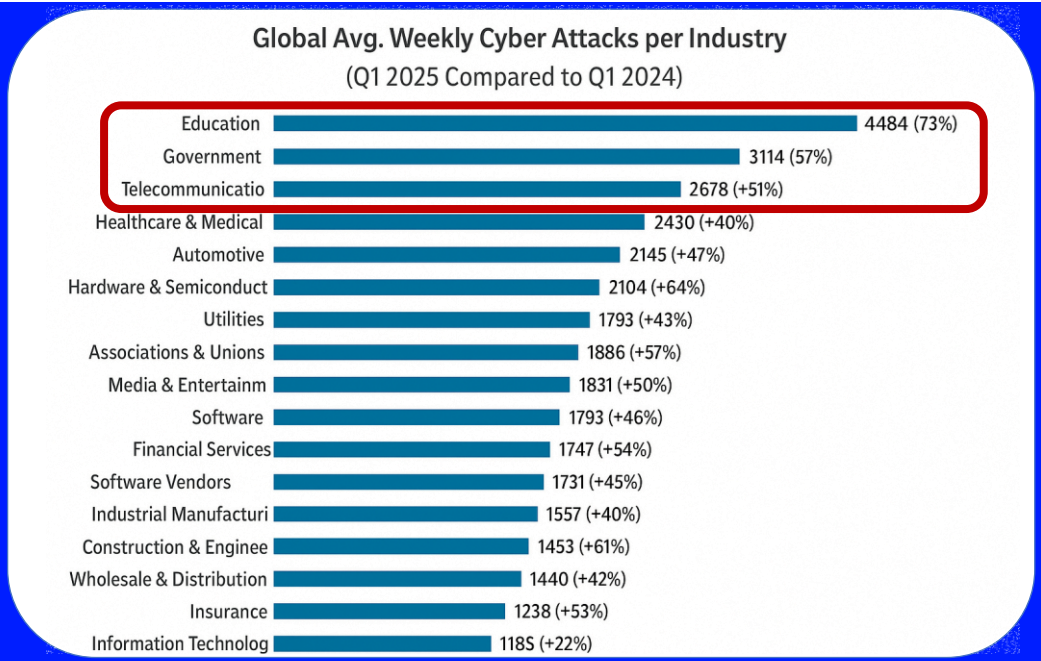
Ataques por segundo na América Latina

60%

Ações reativas ao invés de preventiva

Source: The State of OT Cyber Security in LATAM 2024 Annual Report CS4CA

Cenário de Segurança Cibernética



Source: Global Cybersecurity Outlook 2025 – The World Economic Forum

1.600+

Ataques por segundo na América Latina

60%

Ações reativas ao invés de preventiva

Home > Ataque hacker

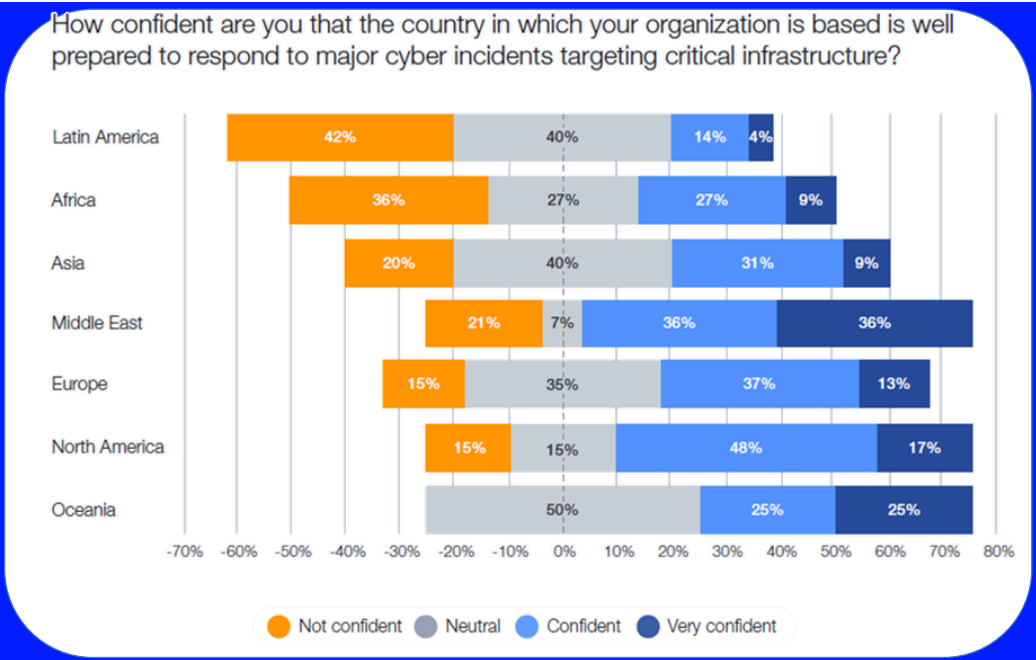
Brasil é líder do ranking de ataques DDoS na América Latina pela 10ª vez; entenda

23/10/2023 às 12:15 • 1 min de leitura

Source: The State of OT Cyber Security in LATAM 2024 Annual Report CS4CA

RNP

Cenário de Segurança Cibernética



Source: Global Cybersecurity Outlook 2025 – The World Economic Forum

1.600+

Ataques por segundo na América Latina

60%

Ações reativas ao invés de preventiva

Home › Ataque hacker

Brasil é líder do ranking de ataques DDoS na América Latina pela 10ª vez; entenda

23/10/2023 às 12:15 • 1 min de leitura

Source: The State of OT Cyber Security in LATAM 2024 Annual Report CS4CA

RNP

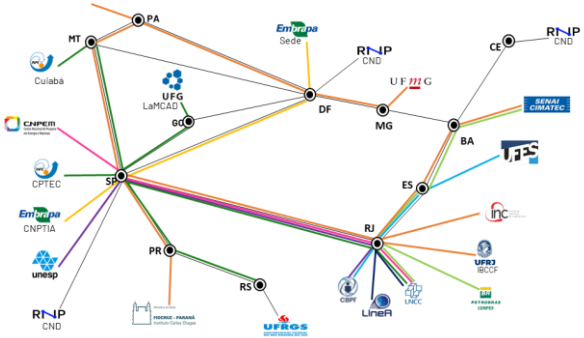
Cenário de Segurança Cibernética

Cenário Atual

Cenário de Segurança Cibernética

Cenário Atual

Impactar

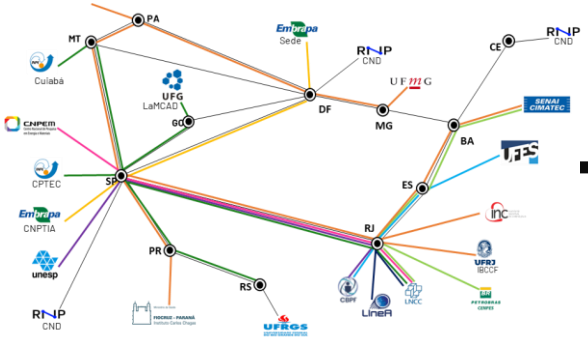


Rede e-Ciência

Cenário de Segurança Cibernética

Cenário Atual

Impactar



Rede e-Ciência

Ações

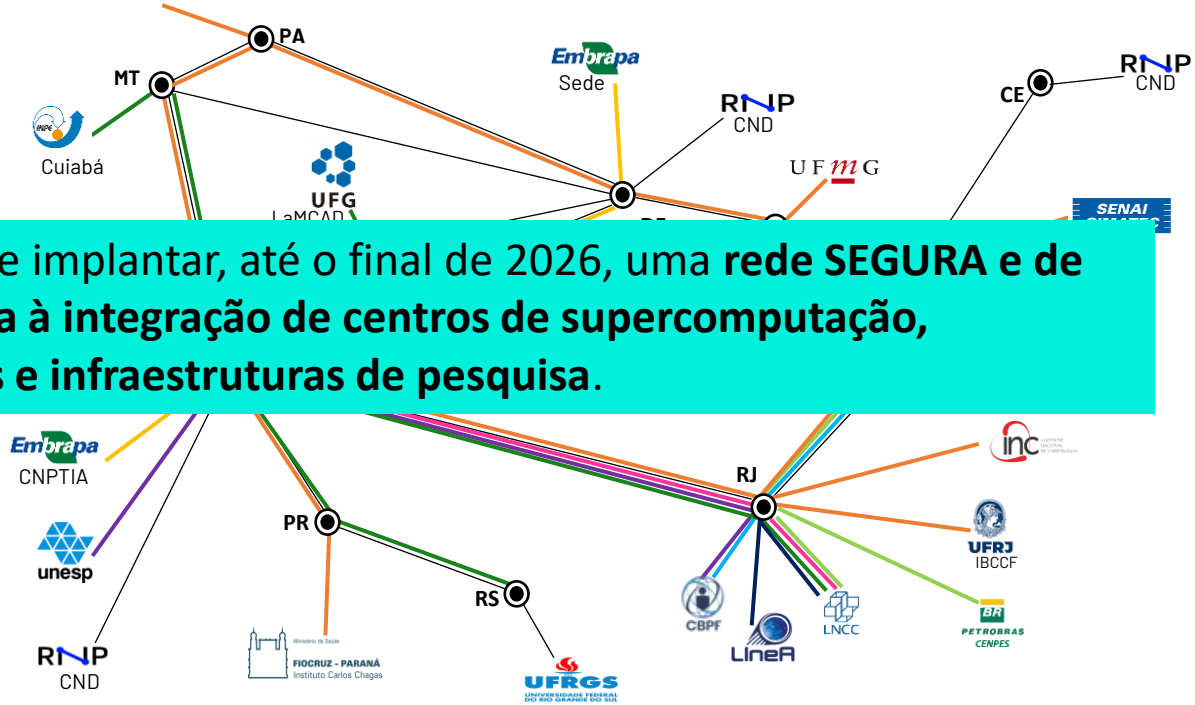
cais

Rede e-Ciência

DEMANDAS CIENTÍFICAS E CONEXÕES

1. **METEOROLOGIA**
   UFG - INPE CPTEC - INPE Cuiabá
   UFRGS - LNCC
2. **COSMOLOGIA** e **FÍSICA DE ALTAS ENERGIAS**
   Unesp – CBPF – UFES
3.
4.
5. **AGRICULTURA E GENÔMICA**
   Embrapa CNPTIA – Embrapa Sede
6. **GEOFÍSICA**
   LNCC – Cenpes – Senai-Cimatec
7. **SAÚDE**
   FIOCRUZ (PR) – UFMG – UFPA – UFRJ (IBCCF)
   INC – Senai-Cimatec

O projeto tem o objetivo de implantar, até o final de 2026, uma **rede SEGURA e de alto desempenho dedicada à integração de centros de supercomputação, laboratórios multiusuários e infraestruturas de pesquisa**.



RNP

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.

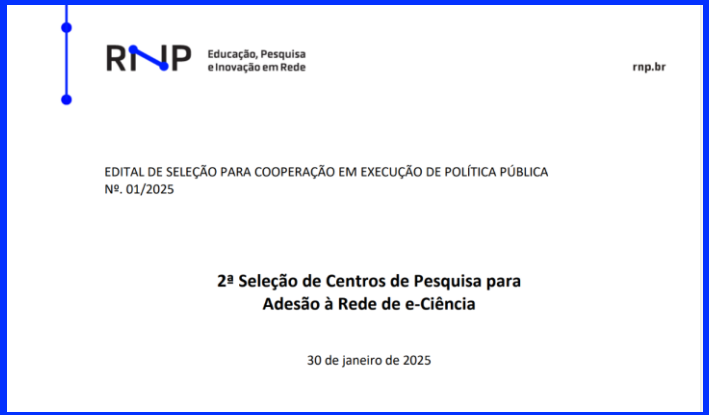
Há 26 anos, o CAIS-RNP garante a segurança em centenas de instituições de educação e pesquisa brasileiras. A área de inteligência em cibersegurança da RNP desenvolve ações preventivas, educativas e corretivas em incidentes e ameaças na rede acadêmica, que enfrenta diariamente os desafios ligados ao aumento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

Segurança by Design

Segurança by Design

Edital	Normas e Documentações	Arquitetura e Hardening	Pentest e Análise de Vulnerabilidades
Análise de Riscos	Continuidade de Negócios	Monitoramento SOC	Resposta a Incidentes

Edital da rede e-Ciência



RNP Educação, Pesquisa e Inovação em Rede

rnp.br

EDITAL DE SELEÇÃO PARA COOPERAÇÃO EM EXECUÇÃO DE POLÍTICA PÚBLICA
Nº. 01/2025

2ª Seleção de Centros de Pesquisa para Adesão à Rede de e-Ciência

30 de janeiro de 2025

Edital da rede e-Ciência

Avaliação de Documentos:

- Política de Segurança da Informação;
- Normativo sobre Gestão de Acesso físico e lógico;
- Normativo sobre Segurança física e do ambiente
- Certificações**

Edital da rede e-Ciência

Avaliação de Documentos:

- Política de Segurança da Informação;
- Normativo sobre Gestão de Acesso físico e lógico;
- Normativo sobre Segurança física e do ambiente
- Certificações**

Controles de segurança:

- Segregação física do espaço para área segura;
- Controle de acesso físico do local;
- Monitoramento por câmera;
- Controle de combate a incêndio;
- Controle e monitoramento de temperatura e umidade;
- Proteção contra falha de energia e descarga elétrica;
- Acompanhamento de visitantes em áreas seguras;

Edital da rede e-Ciência

Avaliação de Documentos:

- Política de Segurança da Informação;
- Normativo sobre Gestão de Acesso físico e lógico;
- Normativo sobre Segurança física e do ambiente
- Certificações**

Controles de segurança:

- Segregação física do espaço para área segura;
- Controle de acesso físico do local;
- Monitoramento por câmera;
- Controle de combate a incêndio;
- Controle e monitoramento de temperatura e umidade;
- Proteção contra falha de energia e descarga elétrica;
- Acompanhamento de visitantes em áreas seguras;

Edital da rede e-Ciência

- Evidências dos controles existentes para avaliação ou Certificação;
- Envio é permitido em um documento de evidências;

- Caso a ICT candidata não disponha de nenhum dos documentos acima, solicitamos a elaboração e envio de um documento que apresente evidências, tais como fotos, vídeos, capturas de tela e documentos, que permitam à equipe técnica da RNP verificar os seguintes controles de segurança:
    a. Segregação física do espaço para área segura;
    b. Controle de acesso físico do local;
    c. Revisão dos acessos concedidos;
    d. Monitoramento por câmera;
    e. Controle de combate a incêndio;
    f. Controle e monitoramento de temperatura e umidade;
    g. Proteção contra descarga elétrica;
    h. Proteção contra falha de energia (UPS/Grupo Motor Gerador);

Edital da rede e-Ciência

- Evidências dos controles existentes para avaliação ou Certificação;
- Envio é permitido em um documento de evidências;

- Caso a ICT candidata não disponha de nenhum dos documentos acima, solicitamos a elaboração e envio de um documento que apresente evidências, tais como fotos, vídeos, capturas de tela e documentos, que permitam à equipe técnica da RNP verificar os seguintes controles de segurança:
  a. Segregação física do espaço para área segura;
  b. Controle de acesso físico do local;
  c. Revisão dos acessos concedidos;
  d. Monitoramento por câmera;
  e. Controle de combate a incêndio;
  f. Controle e monitoramento de temperatura e umidade;
  g. Proteção contra descarga elétrica;
  h. Proteção contra falha de energia (UPS/Grupo Motor Gerador);

RNP MINISTÉRIO DA CULTURA MINISTÉRIO DA DEFESA MINISTÉRIO DA SAÚDE MINISTÉRIO DAS COMUNICAÇÕES MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL

cais Inteligência em Cibersegurança

Parecer técnico de Segurança

RNP

Normas e Documentações

Normas e Documentações

Padrões de Segurança para a RNP e as unidades conectadas

- **Política de Segurança da Informação e Privacidade e Proteção de Dados para Rede de e-ciência**

RNP Educação, Pesquisa e Inovação em Rede

SEG.P.006 Política de Segurança da Informação e Privacidade e Proteção de Dados para Rede de e-ciência

CAIS | Rede Nacional de Ensino e Pesquisa

- Diretrizes:
  - Dados pessoais;
  - Incidentes;
  - Conformidade;
  - Segurança institucional;
  - Riscos;
  - Controles

RNP

Normas e Documentações

Padrões de Segurança para a RNP e as unidades conectadas

- Autenticação e Autorização;
- Protocolos e Serviços desnecessários;
- Registro e Auditorias;
- Patches de Segurança e vulnerabilidades;
- Imagem Padrão

- **Norma e processo de Hardening (RNP)**

Arquitetura e Hardening

Arquitetura e *Hardening*

Objetivo

Atuar em conjunto com as diversas áreas do projeto buscando elevação do grau de segurança tecnológica do ambiente.

Arquitetura e *Hardening*

Pontos abordados

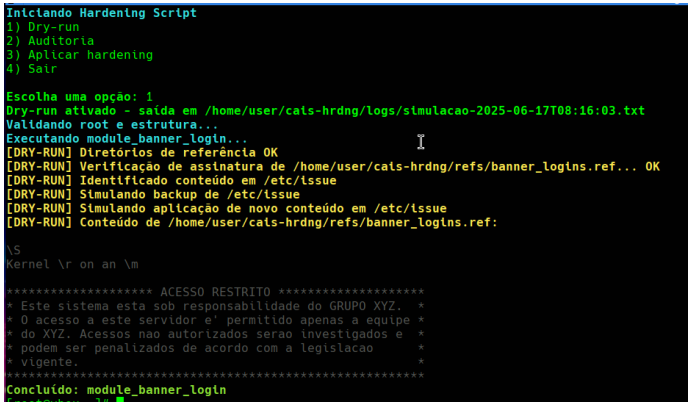
- Avaliar topologias (lógicas/físicas), recomendando controles de segurança, sejam melhorias ou novos controles;
- Modelagem de ameaças;
- Aplicação de configurações específicas;
  - Ex.: regras de *firewall*, *IAM*, criptografia, *hardening*, etc;
- Observabilidade & Telemetria;
- Resiliência;
- Governança de dados (apontamentos);
- Riscos tecnológicos & operacionais (apontamentos);
- ...

- Políticas e normativos da RNP e/ou que interagem com o SRNP;
- *Center for Internet Security (CIS Controls & CIS Benchmarks);*
- *NIST SP 800-215 - Guide to a Secure Enterprise Network Landscape;*
- *NSA - Cybersecurity Technical Report Network Infrastructure Security;*
- *S.T.R.I.D.E Framework*
- *OSSTMM*
- ...

Arquitetura e *Hardening*

Forma de atuação

- Avaliação de topologia
  - HLD/LLD
- Casos de uso
  - Visão do usuário e do administrador (operador);
- Avaliações operacionais
  - Recursos de componentes utilizados
- Aplicação de *hardening*
  - *Hardening* inicial (SO, equipamentos de conectividade, etc);
  - Monitoramento e evolução
    - Automatizações



Pentest e
Análise de Vulnerabilidades

Segurança Ofensiva (Pentest)

1. Enumeração e Reconhecimento:

- Identificar os serviços em execução em cada segmento da rede.
- Mapear portas abertas (scan de portas) e suas aplicações.
- Enumerar endereços IP, dispositivos e seus banners para identificar versões vulneráveis

Segurança Ofensiva (Pentest)

2. Testes em Componentes Críticos:

Switch (Borda) :

- Teste de configurações padrão (credenciais padrão, vulnerabilidades conhecidas).
- Exploração de falhas em autenticação ou controle de acesso.

Switch Science DMZ :

- Analisar a segmentação entre a Science DMZ e a Rede de Missão Crítica.
- Teste de isolamento da DMZ em relação a ataques internos.
- Verificar se os dados trafegam por canais criptografados.
- Captura e análise de tráfego para tentar interceptar credenciais ou informações sensíveis.

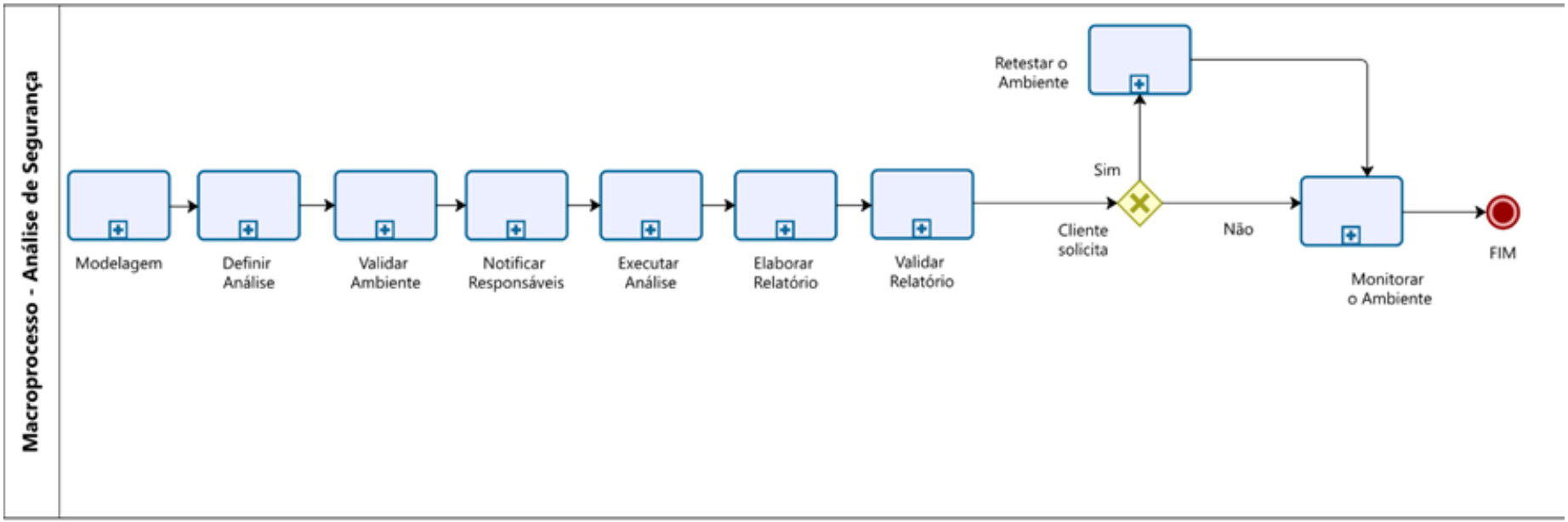
Roteadores SDWAN:

- Testes de resistência a ataques DoS (Denial of Service).
- Verificar exposição de interfaces administrativas na rede.

Servidores (PerfSonar, DTN)

- Identificar vulnerabilidades específicas em serviços rodando (PerfSonar e transferências de dados DTN).
- Testes de acesso a contas de serviços.

Segurança Ofensiva (Pentest)



Segurança Defensiva (Análise de vulnerabilidades)

- Realizar varreduras **automatizadas mensais** nos ativos do ambiente E-Ciência;

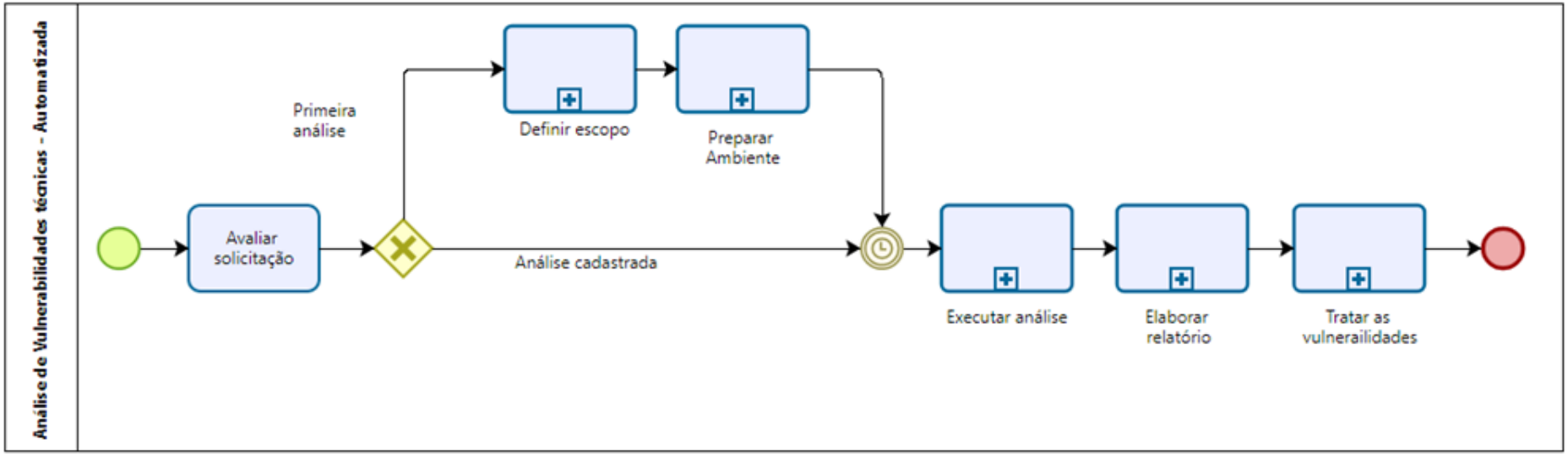
- Classificar as vulnerabilidades identificadas com base em **visão de riscos** (CVSS e VPR) e impacto no ambiente de produção;

- Indicadores mensais com a visão **Quantitativa e Qualitativa;**

- Acompanhar a **aplicação de correções** e reexecução dos scans para validar a remediação;

- Avaliar a **efetividade** das ações corretivas adotadas e propor melhorias nos processos de segurança.

Segurança Defensiva (Análise de vulnerabilidades)



Análise de Riscos

“Preservação da Confidencialidade, Integridade e Disponibilidade da informação através de um processo de gestão de riscos (...)”

ISO/IEC 27001:2022

“Preservação da Confidencialidade, Integridade e Disponibilidade da informação através de um processo de gestão de riscos (...)”

ISO/IEC 27001:2022

Cenário de Segurança Cibernética

Eu deveria...?


cais RNP

ISO 31000 GUIDANCE ON RISK MANAGEMENT

ISO

31000

ISO

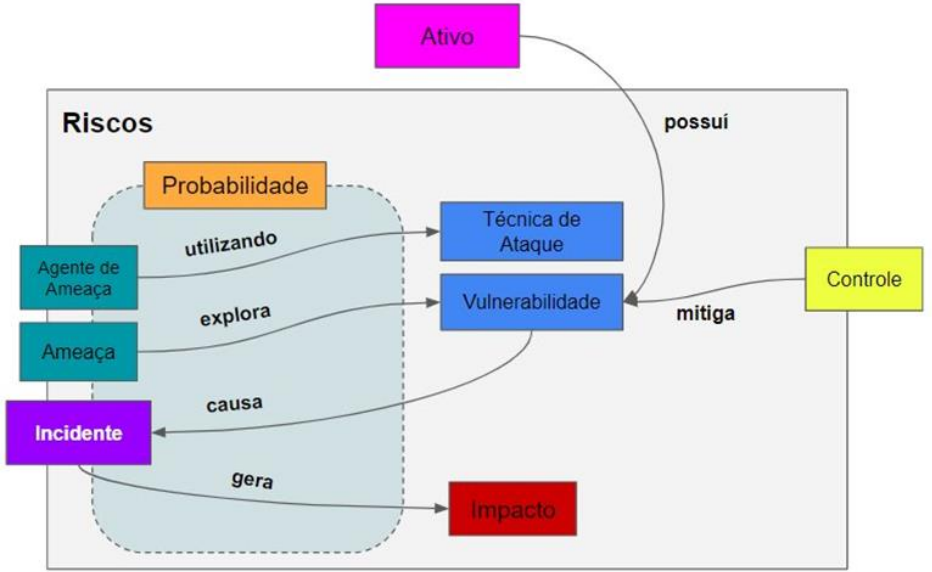
27005

ISO

27001

cais RNP

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 as ligações com a rede e-Ciência

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e as ligações com a rede e-Ciência

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

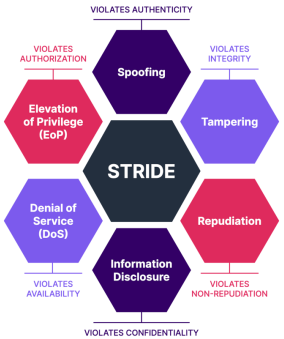
- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e as ligações com a rede e-Ciência

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 as ligações com a rede e-Ciência

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

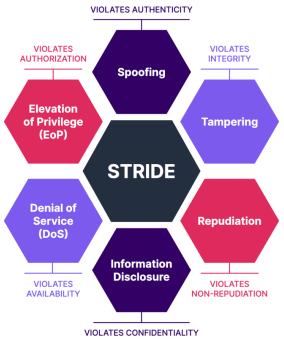
- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e as ligações com a rede e-Ciência

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 as ligações com a rede e-Ciência

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...

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e as ligações com a rede e-Ciência

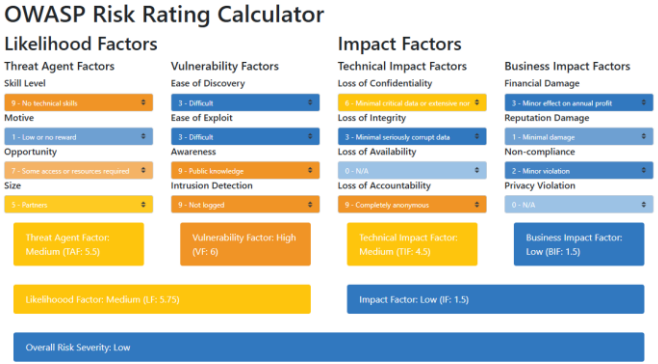
Avaliação de Riscos

-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...



Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e as ligações com a rede e-Ciência

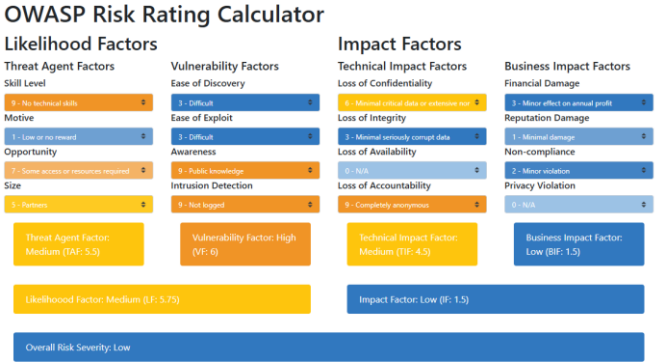
Avaliação de Riscos

-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

Gerenciamento de Riscos Cibernéticos

Contexto e Escopo

- Entrevistas, coleta de informações e definição do escopo
- Compreender a instituição, o negócio e as ligações com a rede e-Ciência

Avaliação de Riscos

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

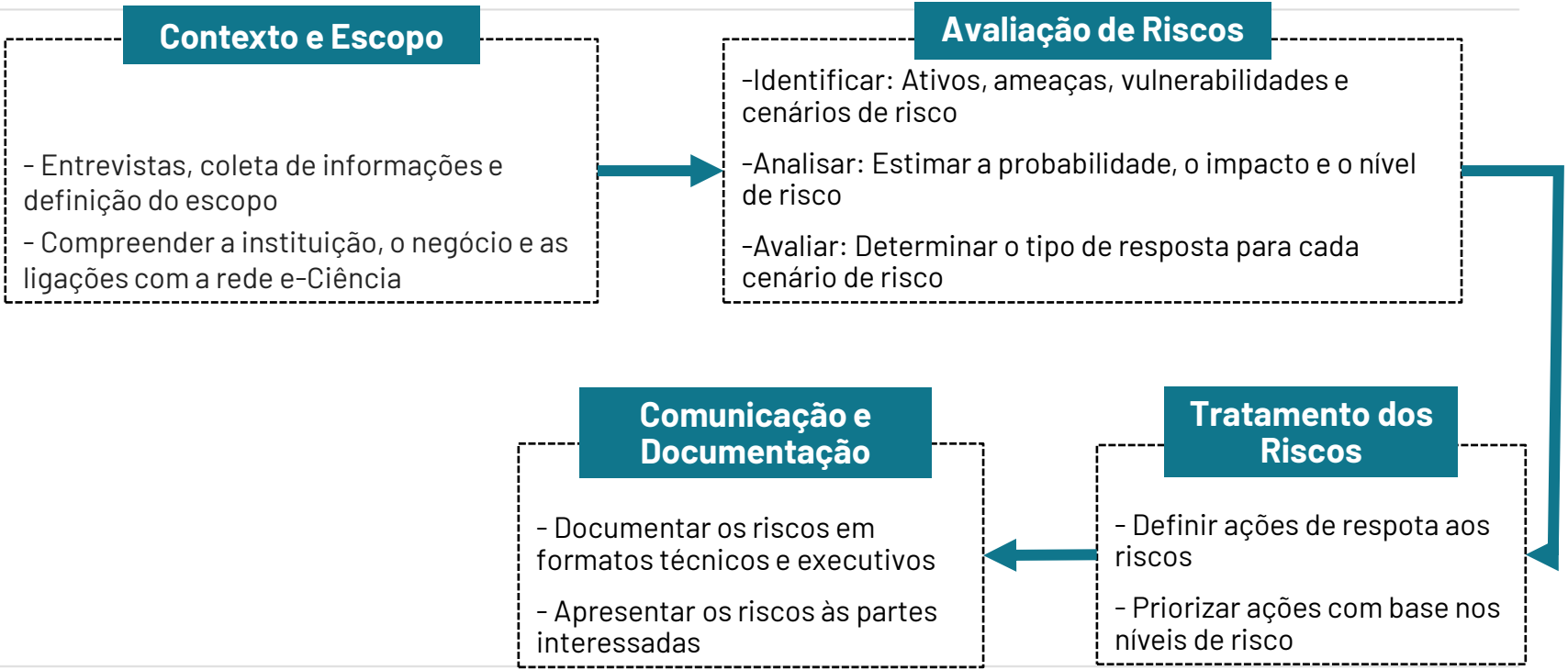
-Analisar: Estimar a probabilidade, o impacto e o nível de risco

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

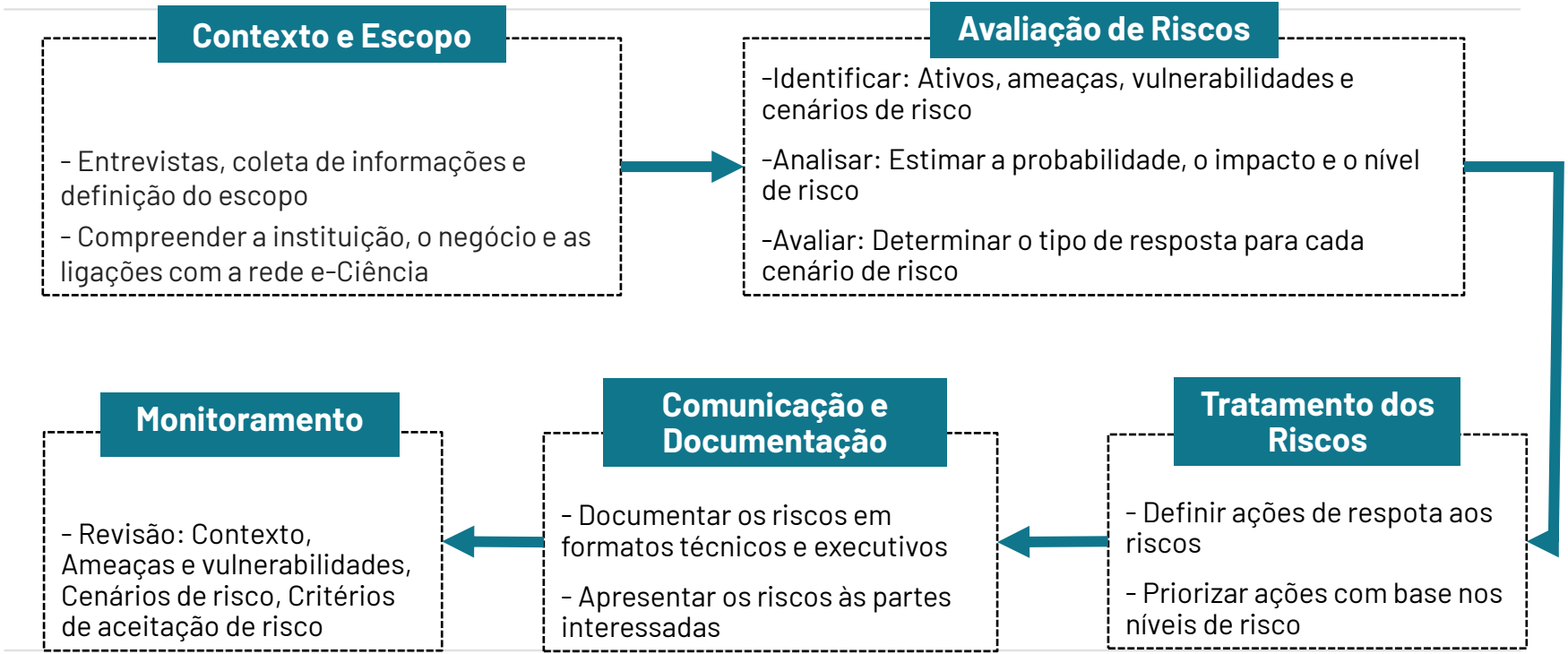
Tratamento dos Riscos

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

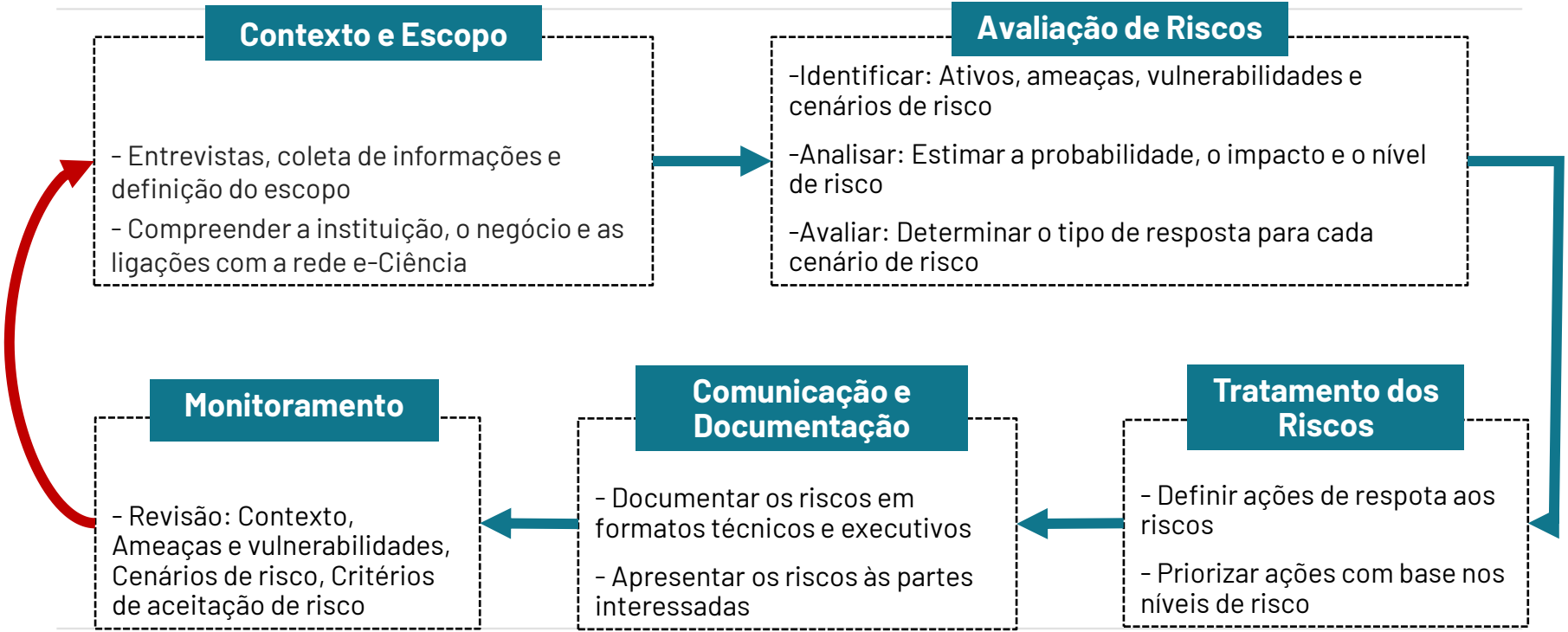
Gerenciamento de Riscos Cibernéticos



Gerenciamento de Riscos Cibernéticos



Gerenciamento de Riscos Cibernéticos



Riscos

Plano de Ação

Informações

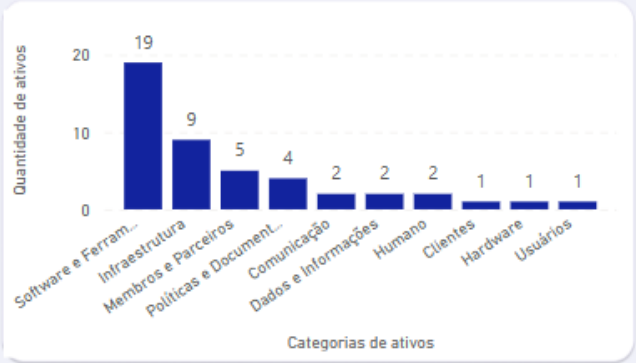
cais

Inteligência em Cibersegurança

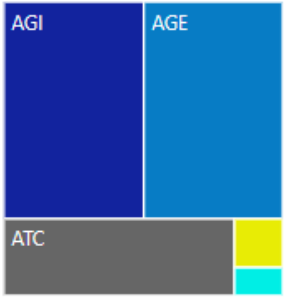
Ativos	Vulnerabilidades	Riscos
46	91	245

Medidor de Risco

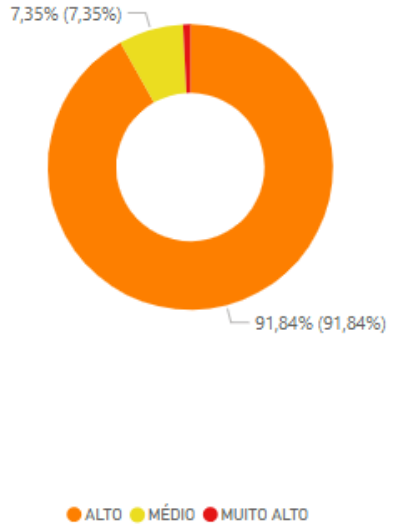
Probabilidade	BAIXO	IMPORTANTE	SIGNIFICATIVO	Total
PROVÁVEL				
OCASIONAL				
FREQUENTE				
Total				



Risco x Agentes de Ameaça



Nível dos Riscos



Vantagens da Análise de Riscos

- Identificação proativa das ameaças;

Vantagens da Análise de Riscos

- Identificação proativa das ameaças;
- Minimização de Impactos e Prejuízos;

Vantagens da Análise de Riscos

- Identificação proativa das ameaças;
- Minimização de Impactos e Prejuízos;
- Proteção contra Ataques Cibernéticos;

Vantagens da Análise de Riscos

- Identificação proativa das ameaças;
- Minimização de Impactos e Prejuízos;
- Proteção contra Ataques Cibernéticos;
- Melhoria na Confiabilidade e Desempenho;

Vantagens da Análise de Riscos

- Identificação proativa das ameaças;
- Minimização de Impactos e Prejuízos;
- Proteção contra Ataques Cibernéticos;
- Melhoria na Confiabilidade e Desempenho;
- Atendimento a Regulamentações e Compliance;

Vantagens da Análise de Riscos

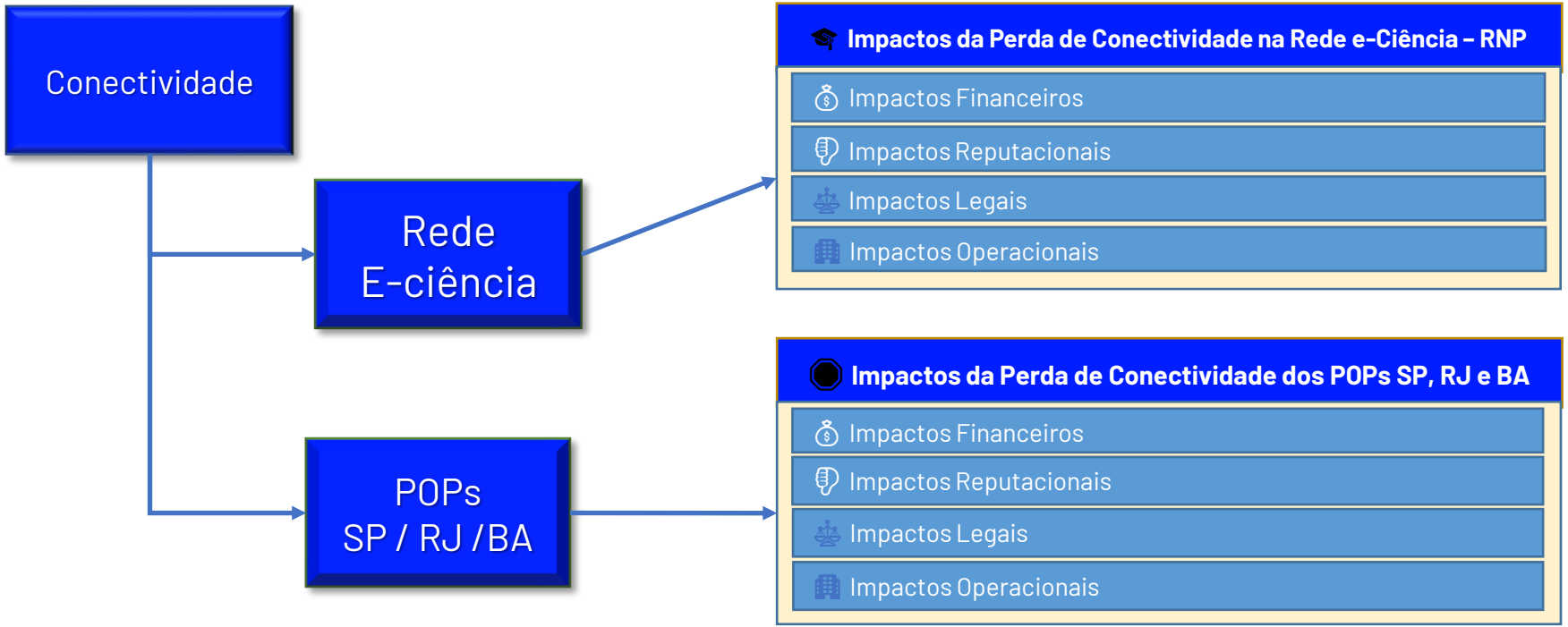
- Identificação proativa das ameaças;
- Minimização de Impactos e Prejuízos;
- Proteção contra Ataques Cibernéticos;
- Melhoria na Confiabilidade e Desempenho;
- Atendimento a Regulamentações e Compliance;
- Otimização de Recursos e Custos;

Vantagens da Análise de Riscos

- Identificação proativa das ameaças;
- Minimização de Impactos e Prejuízos;
- Proteção contra Ataques Cibernéticos;
- Melhoria na Confiabilidade e Desempenho;
- Atendimento a Regulamentações e Compliance;
- Otimização de Recursos e Custos;
- Cultura de Segurança e Melhoria Contínua.

Continuidade de Negócios

Continuidade de Negócios



Continuidade de Negócios

Rede de E-Ciência no Projeto de Gestão de Continuidades de Negócio

Monitoramento e Resposta a Incidentes

Desafios Monitoramento na Rede e-ciência

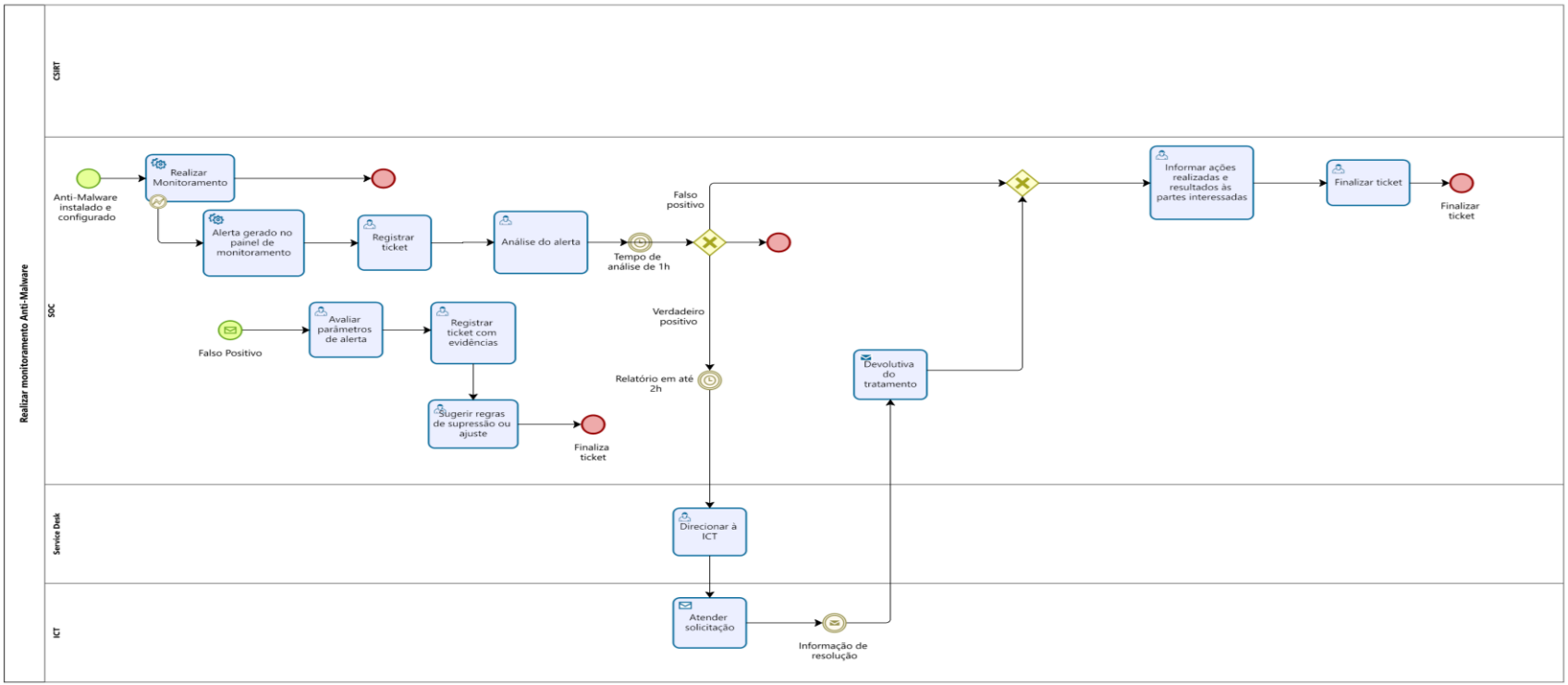
- Rede apartada da infraestrutura tradicional -> sem visibilidade da Camada 3 e 4
- DTNs otimizados para performance de envio -> risco de degradação com agentes de segurança
- Dificuldade em mapear dinamicamente os pontos de possíveis ataques.
- Desafios de mitigação; identificação e análise de artefato; necessário ações de mitigação prudentes;

SOC

Camadas de visibilidade em segurança

- Realizaremos o monitoramento contínuo em regime de 24x7:
- Detecção de alterações de integridade dos diretórios críticos do sistema (etc/passwd etc);
- Detecção de comandos executados no bash;
- Monitoramento das criações de conexões de rede;
- Monitoramento de tentativas de login mal-sucedidas;
- Outras regras pensadas no cenário do DTN.

SOC (Monitoramento Passivo)



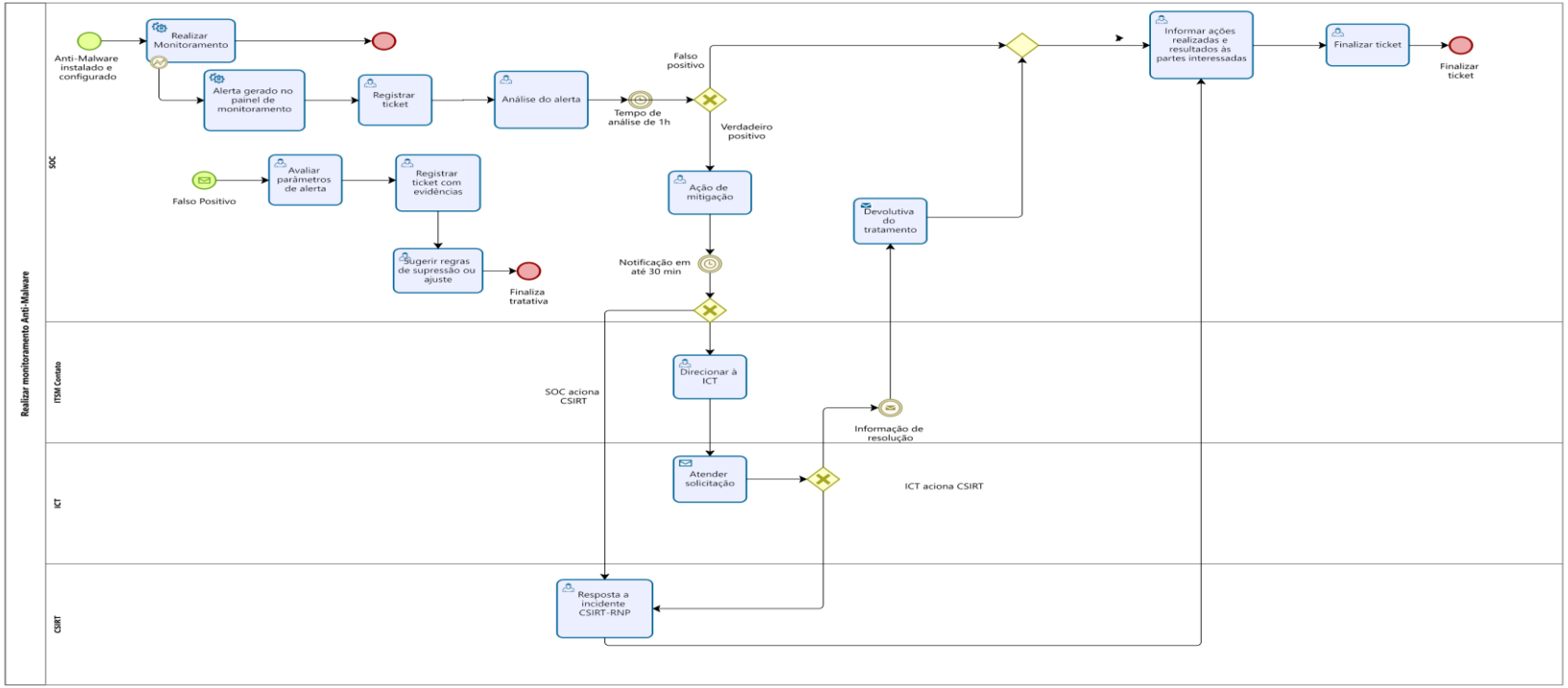
Escolha da Ferramenta

XDR como escolha para visibilidade e resposta além do tradicional EDR

SentinelOne escolhido por:

- Reconhecimento no Gartner Magic Quadrant
- Behavioral AI: análise em tempo real de atividades no Linux
- Visibilidade profunda (Deep Visibility) rastreia ações em tempo real
- Flexibilidade na criação de regras e resposta automatizada

SOC (Monitoramento Ativo)

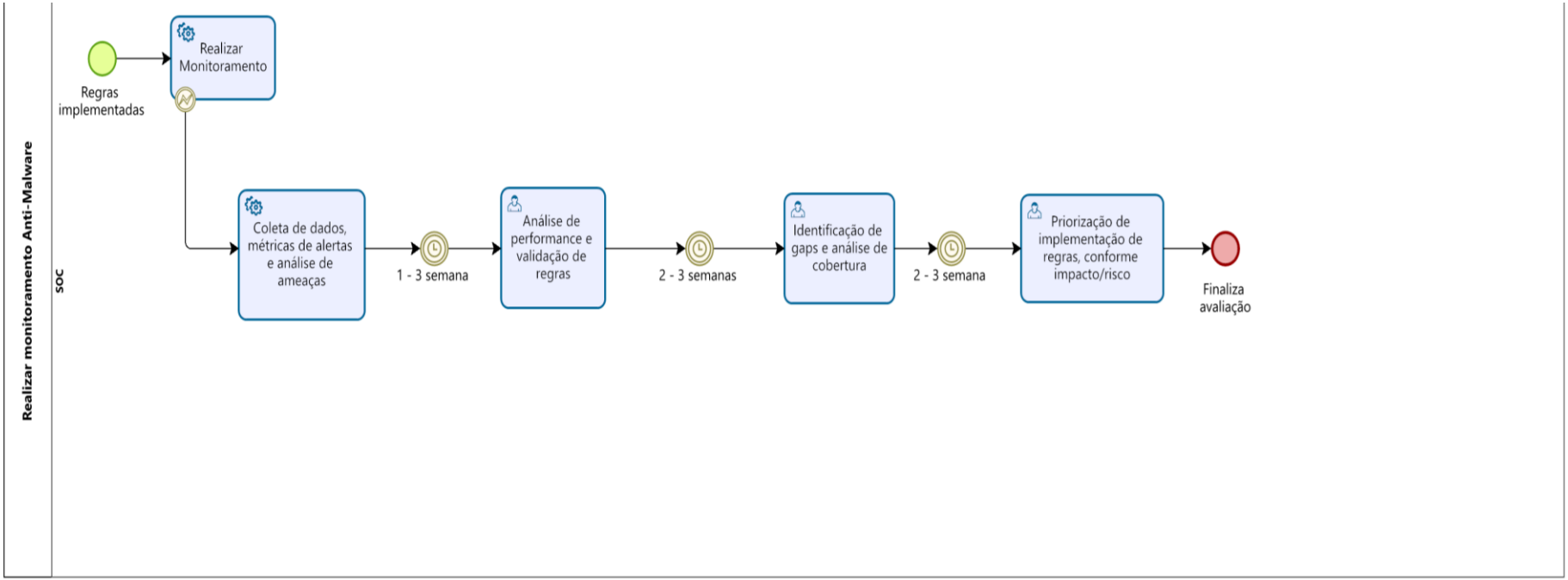


SOC

Mitigação

- Arquivos pode ficar em quarentena até a conclusão da investigação;
- O Agente move a ameaça e os executáveis que ele criou ou alterou para um caminho confinado e os criptografa;
- Capacidade de remover da quarentena;
- É possível deletar um arquivo em quarentena.

SOC (Regras)


Realizar monitoramento Anti-Malware
SOC
Regras implementadas
Realizar Monitoramento
Coleta de dados, métricas de alertas e análise de ameaças
1 - 3 semana
Análise de performance e validação de regras
2 - 3 semanas
Identificação de gaps e análise de cobertura
2 - 3 semana
Priorização de implementação de regras, conforme impacto/risco
Finaliza avaliação

“Não deixar que problemas de segurança:

“Não deixar que problemas de segurança:

- ***Atrapalhem o objetivo de implementar uma rede acadêmica segura de alto desempenho;***

“Não deixar que problemas de segurança:

- ***Atrapalhem o objetivo de implementar uma rede acadêmica segura de alto desempenho;***
- ***Impactar as instituições de Ciência e Tecnologia;***

“Não deixar que problemas de segurança:

- ***Atrapalhem o objetivo de implementar uma rede acadêmica segura de alto desempenho;***
- ***Impactar as instituições de Ciência e Tecnologia;***
- ***Atrapalhar ou atrasar as pesquisas no país;***

“Não deixar que problemas de segurança:

- ***Atrapalhem o objetivo de implementar uma rede acadêmica segura de alto desempenho;***
- ***Impactar as instituições de Ciência e Tecnologia;***
- ***Atrapalhar ou atrasar as pesquisas no país;***
- ***Afetar a imagem das instituições.”***

OBRIGADO!

andre.landim@rnp.br
joao.pereira@terceiro.rnp.br
ricardo.melo@terceiro.rnp.br