cais Inteligência em Cibersegurança RNP

From RISK to ACTION

The CAIS-RNP risk-based approach to cybersecurity

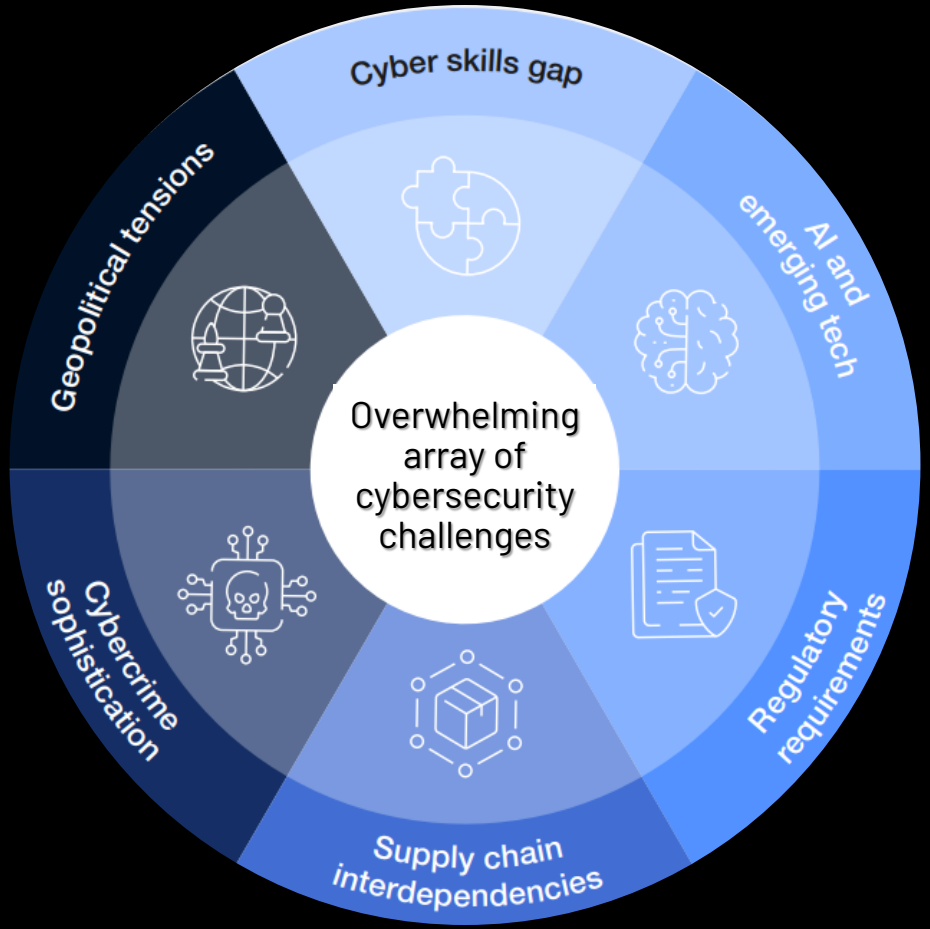
Ingrid Barbosa

Cybersecurity Analyst

IS SECURITY A FEELING OR A TANGIBLE CONDITION?

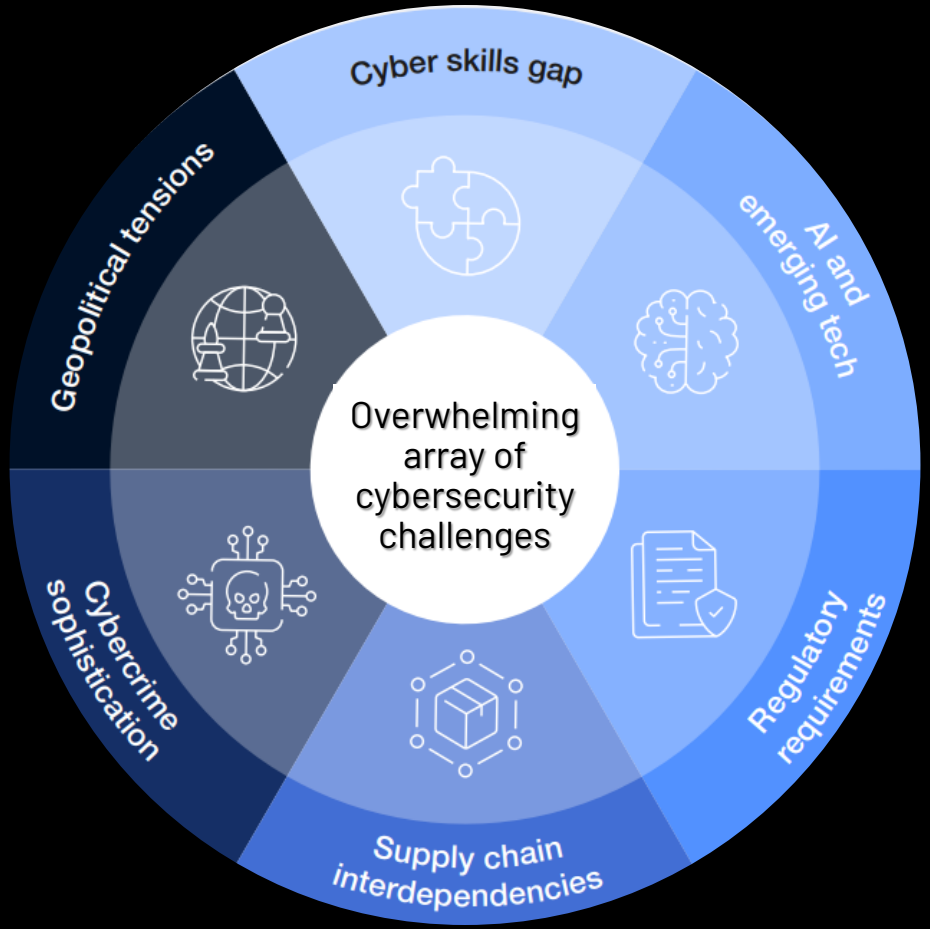
TLP:CLEAR

THE DANGERS OF A MISTAKEN SENSE OF SECURITY



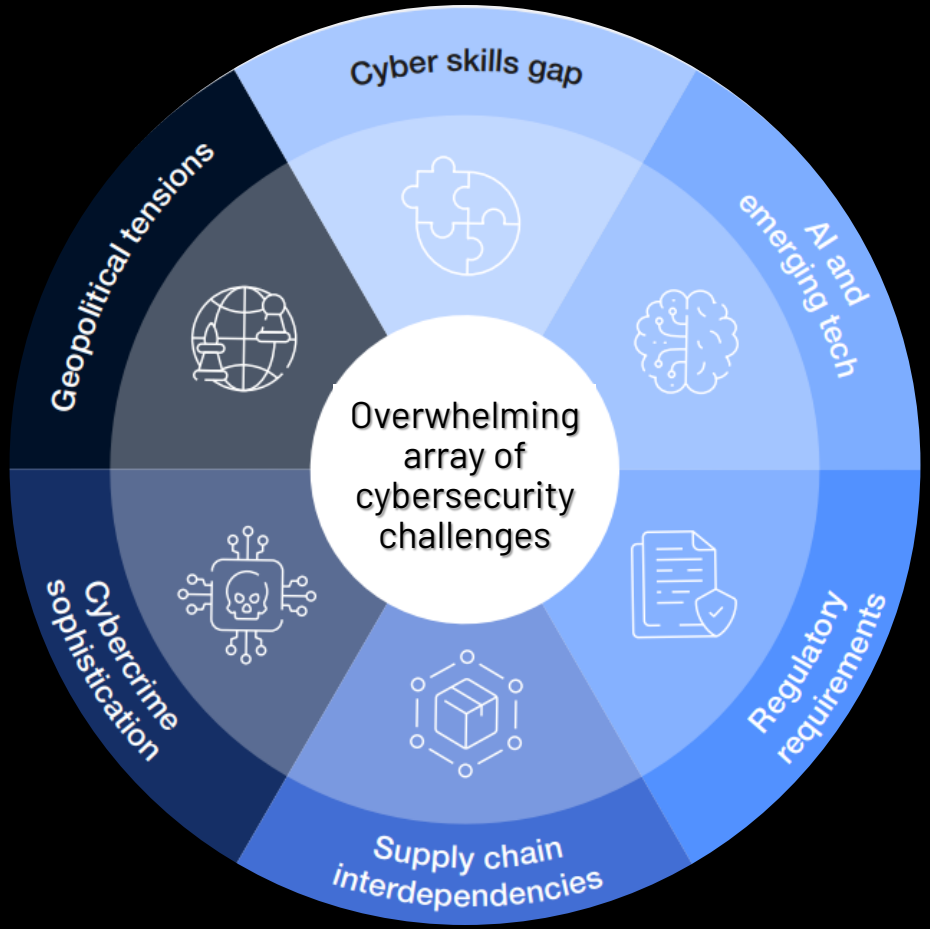
Source: Global Cybersecurity Outlook 2025 – The World Economic Forum

We cannot protect everything



Source: Global Cybersecurity Outlook 2025 – The World Economic Forum

We cannot protect everything



Source: Global Cybersecurity Outlook 2025 – The World Economic Forum

and perhaps, we should not even try

Securing.What.Matters

Security
.Days

RNP

Securing.What.Matters

Security
.Days

But, what truly matters to you?

RNP

Securing.What.Matters

Security .Days

But, what truly matters to you?

Should I ...?

RNP

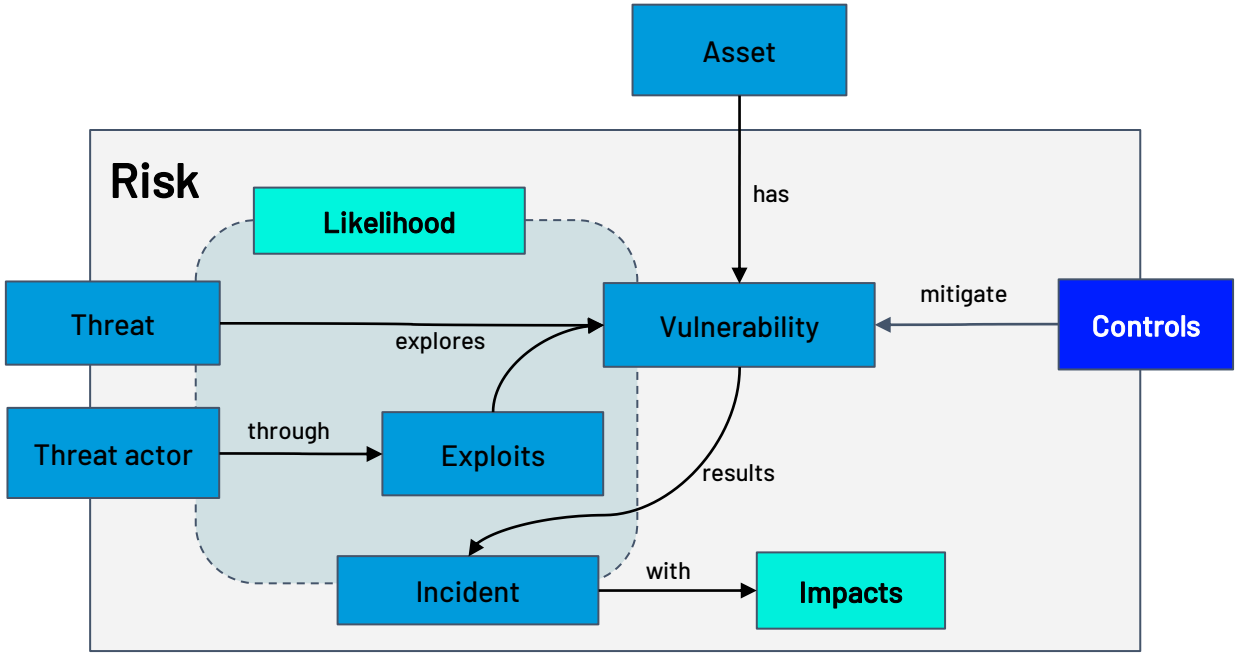
TLP:CLEAR

A risk-based security approach

“Preservation of the Confidentiality, Integrity, and Availability of information through a risk management process(...)”

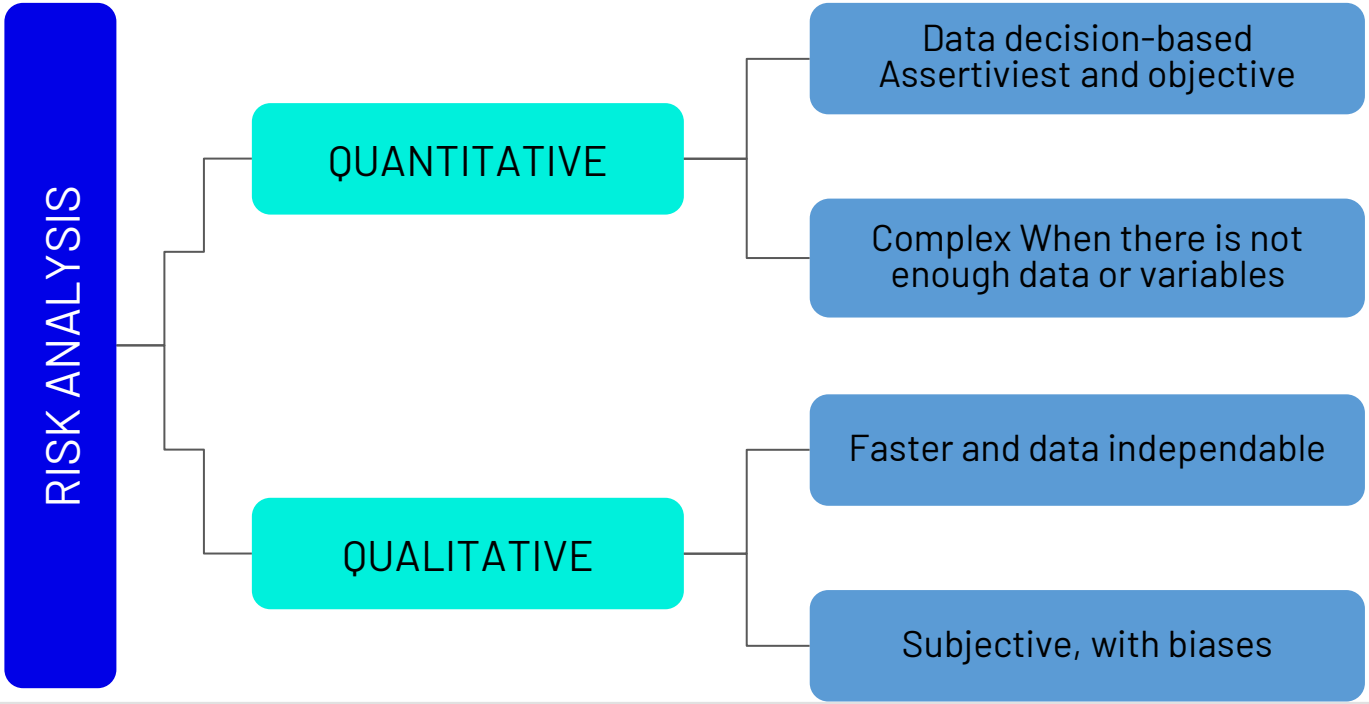
ISO/IEC 27001:2022

Cyber Risks



Risk Analysis

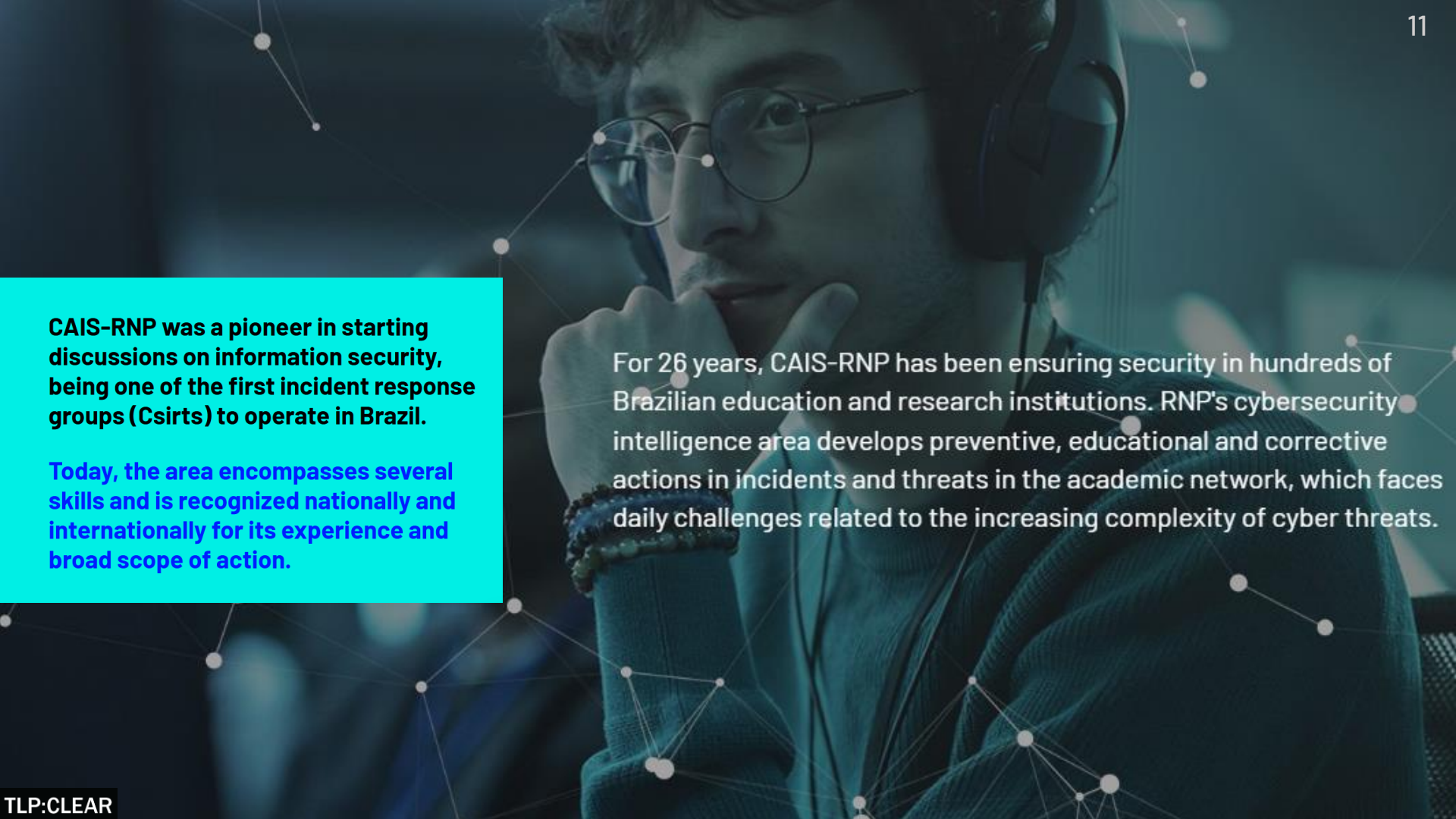
Risk Analysis



How regularly do your NREN adopt cybersecurity risk assessments?

1 - Lack of clarity to bridge theory and practice

2 - The tendency to prioritize what appears urgent over what is strategically important



CAIS-RNP was a pioneer in starting discussions on information security, being one of the first incident response groups (Csirts) to operate in Brazil.

Today, the area encompasses several skills and is recognized nationally and internationally for its experience and broad scope of action.

For 26 years, CAIS-RNP has been ensuring security in hundreds of Brazilian education and research institutions. RNP's cybersecurity intelligence area develops preventive, educational and corrective actions in incidents and threats in the academic network, which faces daily challenges related to the increasing complexity of cyber threats.

SHARE TO EXPAND:

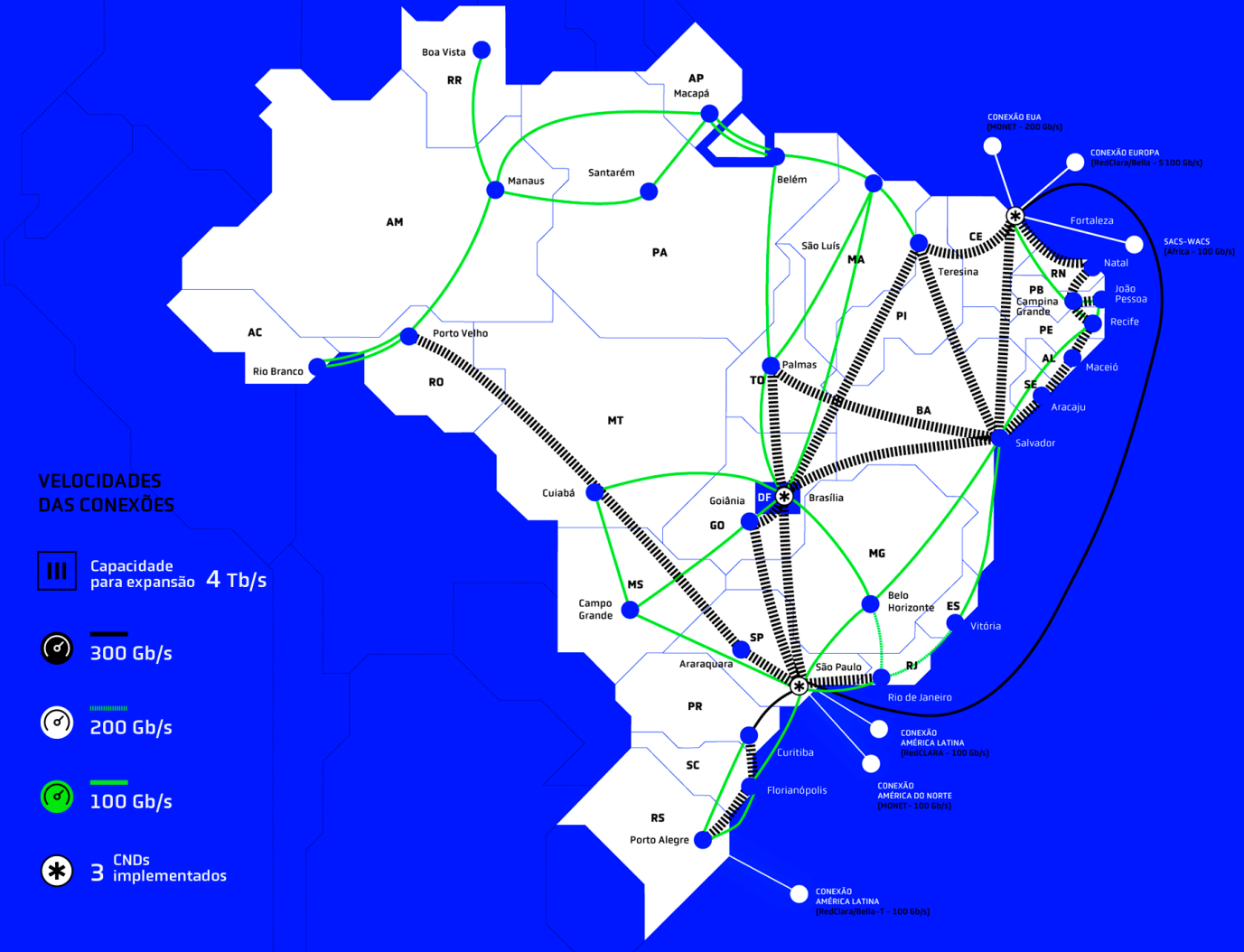
WE CONNECT PEOPLE
IN AN ENVIRONMENT CREATED FOR
THE PRODUCTION OF KNOWLEDGE
AND WE PROVIDE SAFE AND
HIGH CAPACITY SERVICES

500
Connected organizations

+ 3.5 million
User

70
Community connections

+ 100 Gbps
Connections


Boa Vista
RR
AP
Macapá
CONEXÃO EUA
(MONET - 200 Gb/s)
CONEXÃO EUROPA
(RedClara/Bella - S 100 Gb/s)
Manaus
Santarém
Belém
Fortaleza
SACS-WACS
(África - 100 Gb/s)
AM
PA
São Luís
MA
CE
Teresina
Natal
RN
João Pessoa
PB
Campina Grande
Recife
PE
PI
AC
Porto Velho
Rio Branco
RO
Palmas
TO
AL
Maceió
SE
Aracaju
BA
MT
Salvador
Cuiabá
Goiânia
DF
Brasília
GO
MG
MS
Campo Grande
Belo Horizonte
ES
Vitória
SP
Araraquara
São Paulo
RJ
Rio de Janeiro
PR
CONEXÃO AMÉRICA LATINA
(RedCLARA - 100 Gb/s)
Curitiba
SC
Florianópolis
CONEXÃO AMÉRICA DO NORTE
(MONET - 100 Gb/s)
RS
Porto Alegre
CONEXÃO AMÉRICA LATINA
(RedClara/Bella-T - 100 Gb/s)
VELOCIDADES DAS CONEXÕES
Capacidade para expansão 4 Tb/s
300 Gb/s
200 Gb/s
100 Gb/s
3 CNDs implementados

ISO 31000 GUIDANCE ON RISK MANAGEMENT

ISO

31000

ISO

27005

International Organization for Standardization

ISO

27001

PREPARE CATEGORIZE SELECT IMPLEMENT ASSESS AUTHORIZE MONITOR

NIST

RMF

RISK MANAGEMENT FRAMEWORK

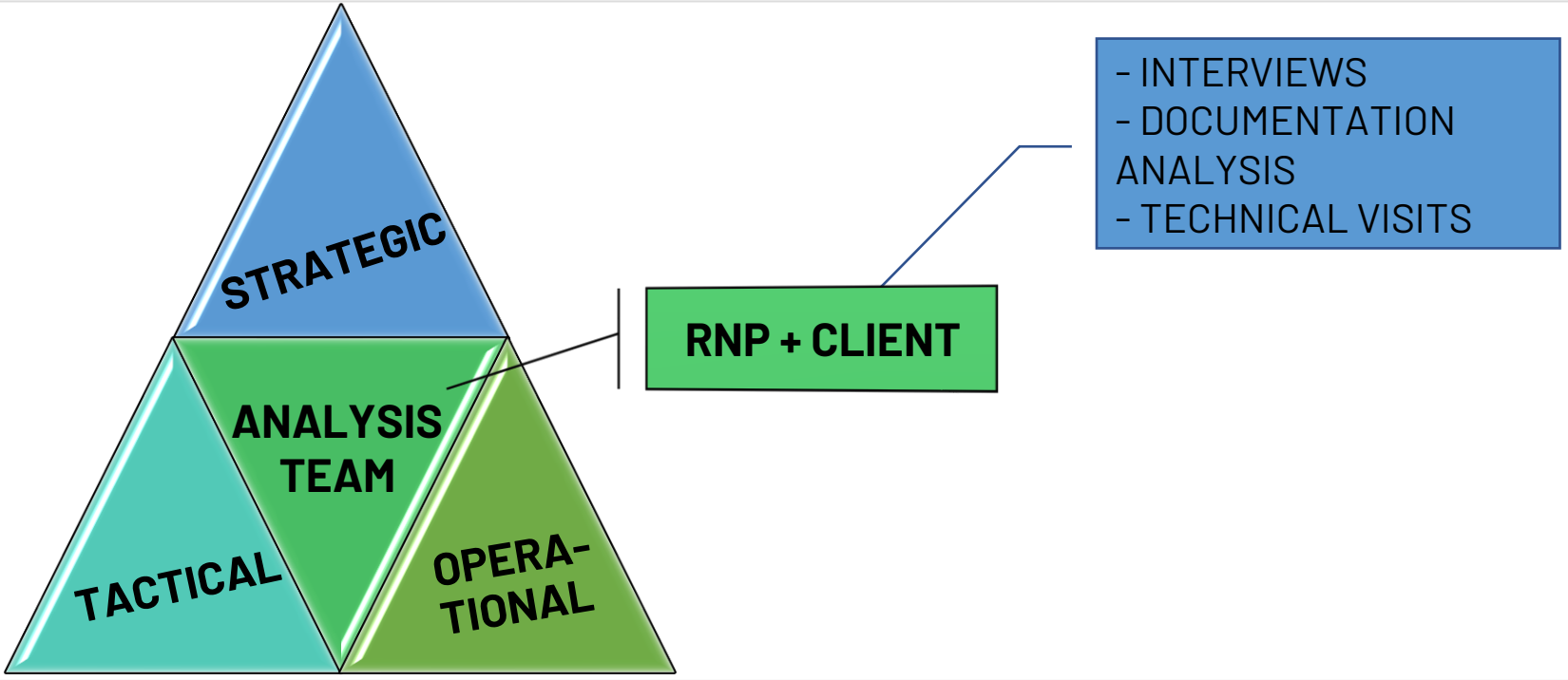
nist.gov/rmf

OWASP

Risk Assessment Calculator

TLP:CLEAR

3D VIEW



Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Risk Treatment

- Define risk response actions
- Prioritize actions based on risk scores

Communication and documentation

- Document risks in both technical and executive formats
- Present risks to stakeholders and board

Monitoring

- Review: Context, Threats & vulnerabilities, Risk scenarios, Risk acceptance criteria

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope

- Understand the company, the business, and the system under assessment

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Failure
Destruction
Loss
Malfunction
Theft
Interruption
and others...

Information Security Risk Management

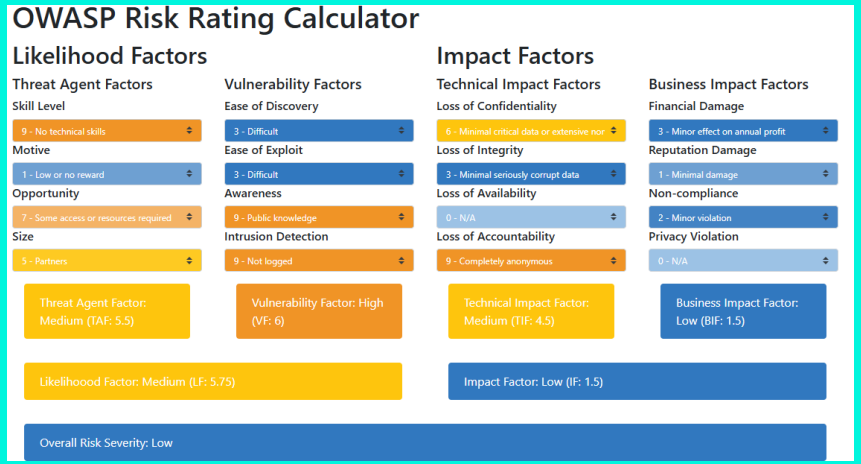
Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Failure
Destruction
Loss
Malfunction
Theft
Interruption
and others...



Information Security Risk Management

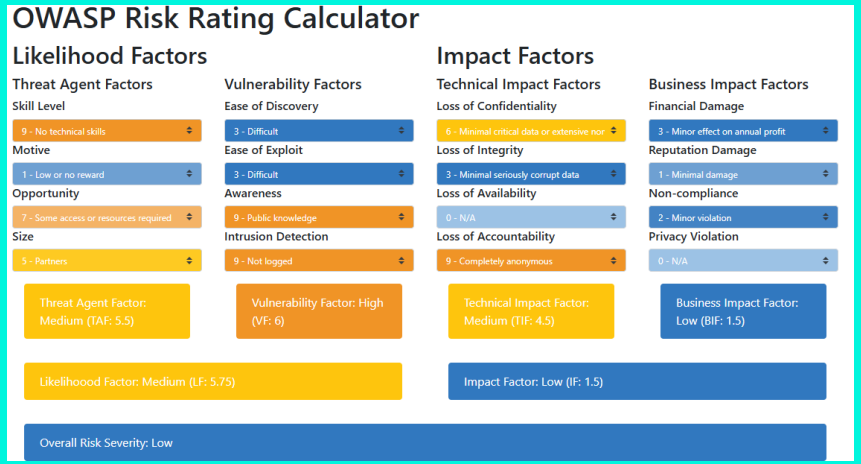
Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Failure
Destruction
Loss
Malfunction
Theft
Interruption
and others...



1. Avoid
2. Mitigate
3. Transfer
4. Accept

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Risk Treatment

- Define risk response actions
- Prioritize actions based on risk scores

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Risk Treatment

- Define risk response actions
- Prioritize actions based on risk scores

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

ASSOCIATED RISKS

RISKS SEVERITY

SCORE

Risk Treatment

- Define risk response actions
- Prioritize actions based on risk scores

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Risk Treatment

- Define risk response actions
- Prioritize actions based on risk scores

Communication and documentation

- Document risks in both technical and executive formats
- Present risks to stakeholders and board

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Risk Treatment

- Define risk response actions
- Prioritize actions based on risk scores

Communication and documentation

- Document risks in both technical and executive formats
- Present risks to stakeholders and board

Monitoring

- Review: Context, Threats & vulnerabilities, Risk scenarios, Risk acceptance criteria

Information Security Risk Management

Scope and Context

- Interviews, input collection and define the scope
- Understand the company, the business, and the system under assessment

Risk Assessment

- Identify: Assets, threats, vulnerabilities, and risk scenarios
- Analyze: Estimate likelihood, impact, and risk level
- Evaluate: Determine response type for each risk scenario

Risk Treatment

- Define risk response actions
- Prioritize actions based on risk scores

Communication and documentation

- Document risks in both technical and executive formats
- Present risks to stakeholders and board

Monitoring

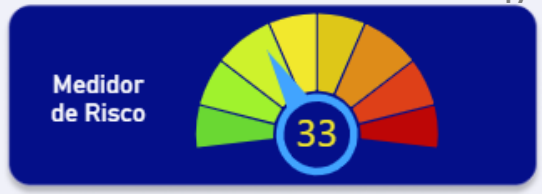
- Review: Context, Threats & vulnerabilities, Risk scenarios, Risk acceptance criteria

Example of application

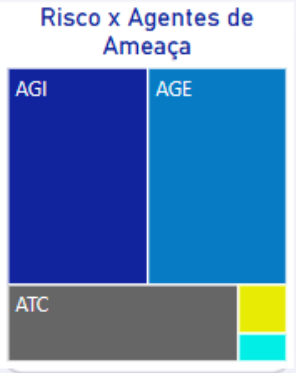
- Riscos
- Plano de Ação
- Informações

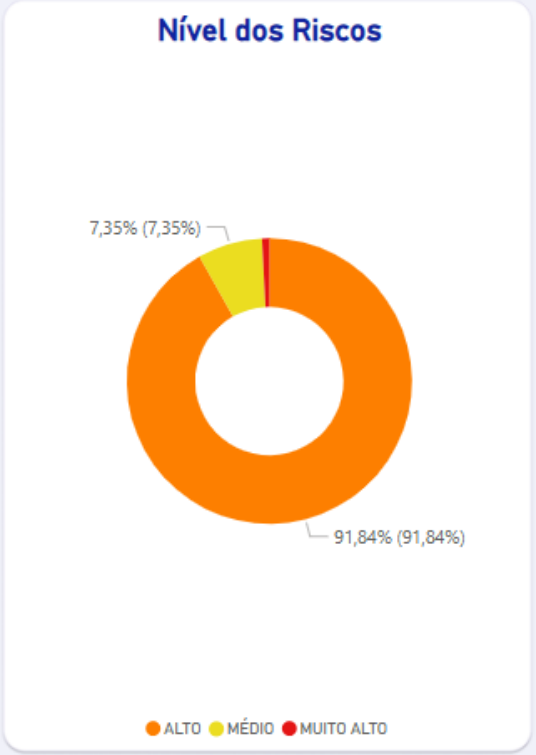
cais
Inteligência em Cibersegurança

Ativos	Vulnerabilidades	Riscos
46	91	245

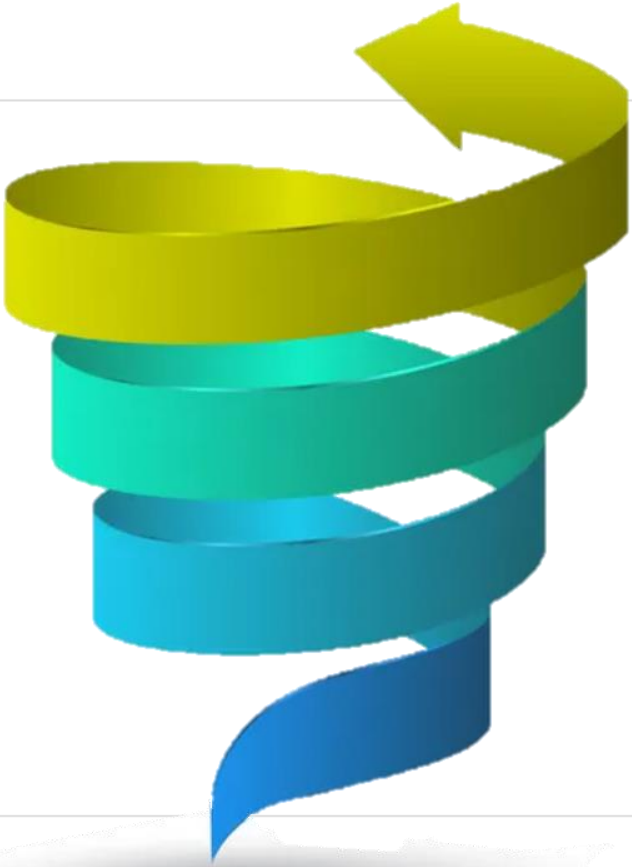


Probabilidade	BAIXO	IMPORTANTE	SIGNIFICATIVO	Total
PROVÁVEL	4	128	89	**221**
OCASIONAL	1	7	13	**21**
FREQUENTE		2	1	**3**
Total	**5**	**137**	**103**	**245**



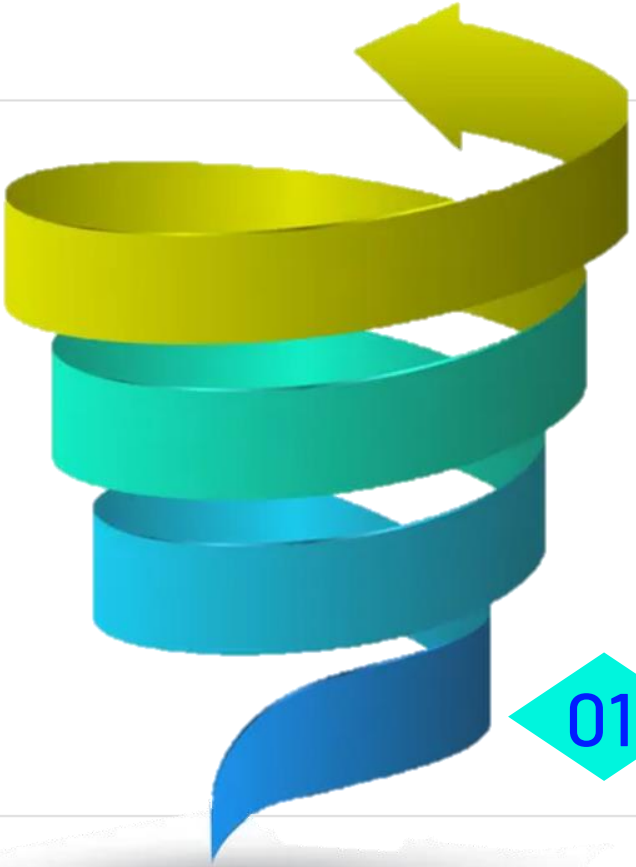


Upward spiral



Methodology Design

Upward spiral



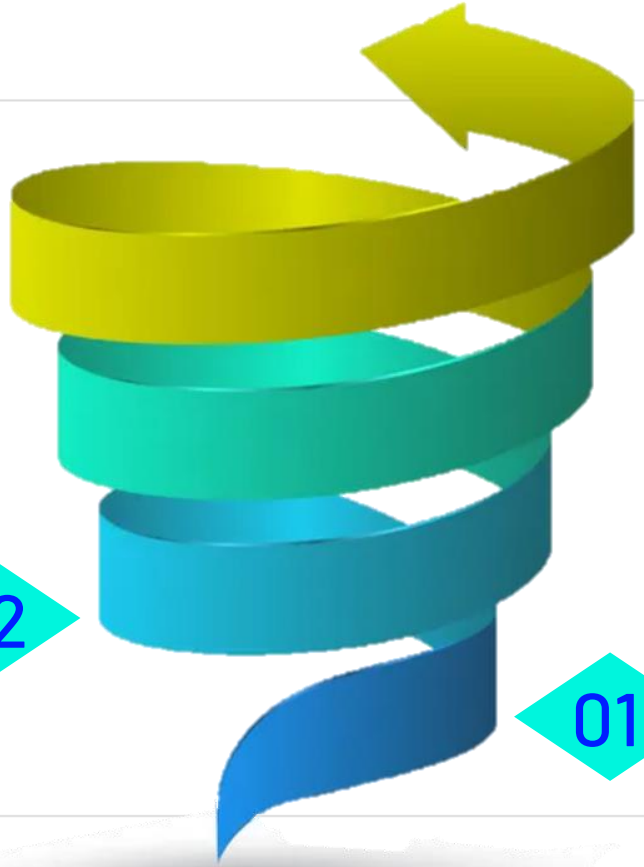
01

PILOT - LIneA (RNP ecosystem) and LNCC (e-Science)

Methodology Design

RNP

Upward spiral



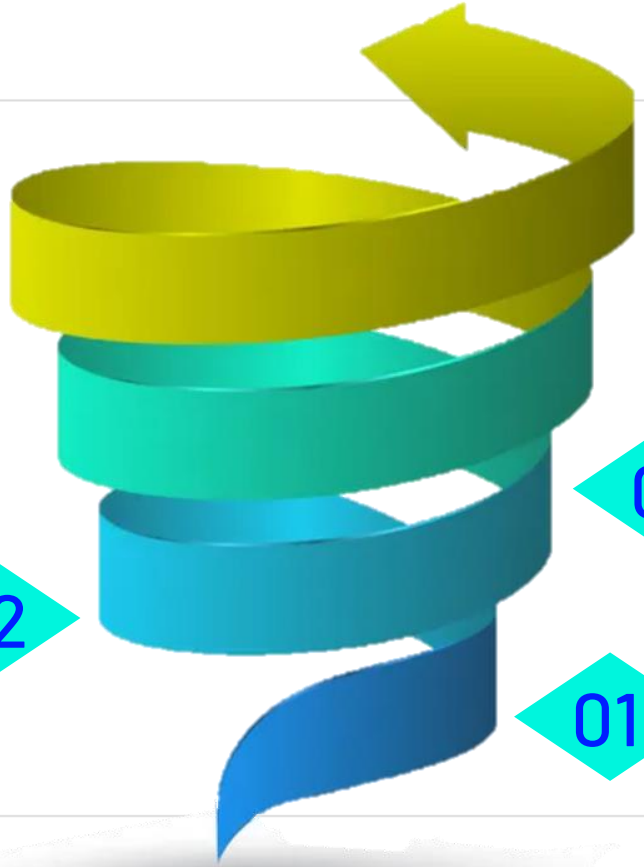
02 Feedbacks from security and corporate risks teams

01 PILOT - LIneA (RNP ecosystem) and LNCC (e-Science)

Methodology Design

RNP

Upward spiral



03 Case Study – Point of Presence from Rio de Janeiro

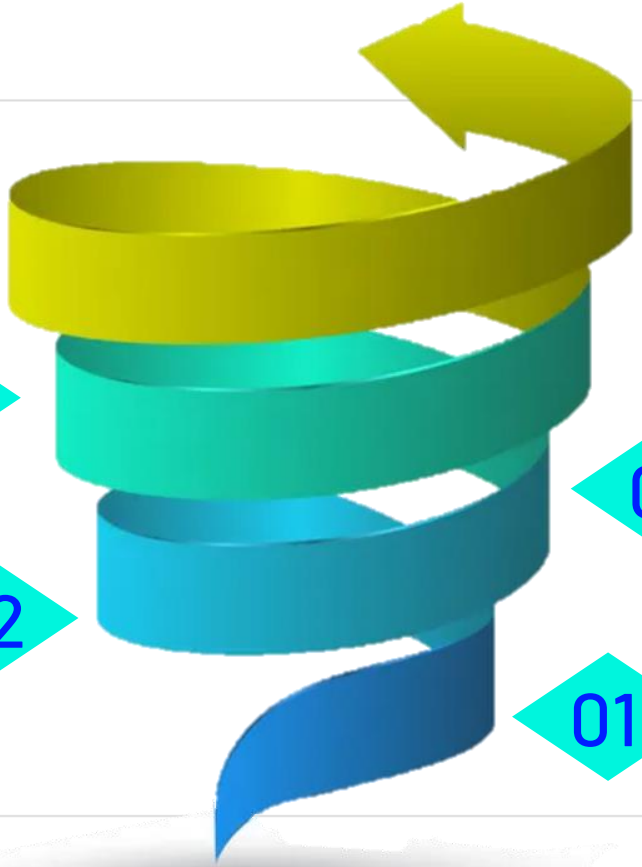
02 Feedbacks from security and corporate risks teams

01 PILOT - LIneA (RNP ecosystem) and LNCC (e-Science)

Methodology Design

RNP

Upward spiral



04 Case Study – CAFe (internal solution)

03 Case Study – Point of Presence from Rio de Janeiro

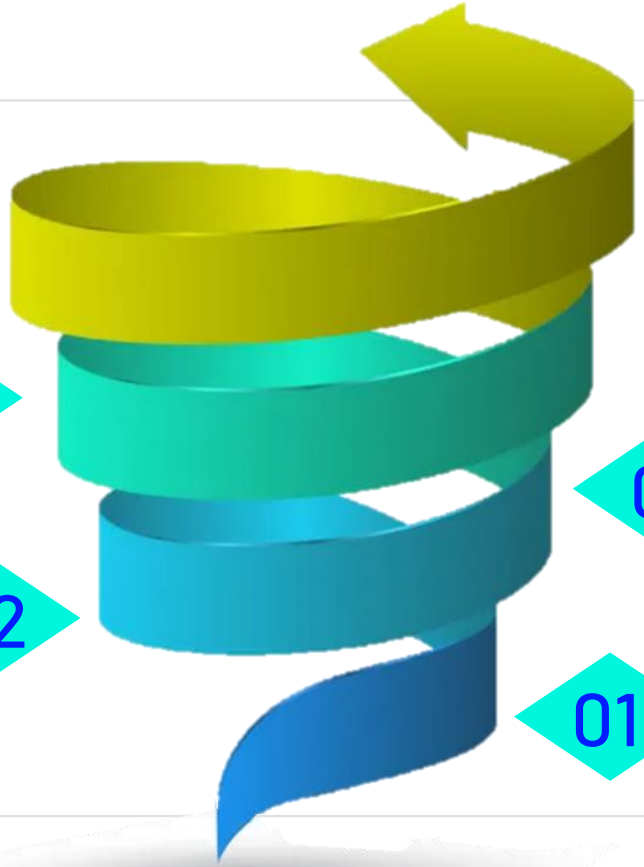
02 Feedbacks from security and corporate risks teams

01 PILOT - LIneA (RNP ecosystem) and LNCC (e-Science)

Methodology Design

RNP

Upward spiral



05 Feedbacks from leadership

04 Case Study – CAFe (internal solution)

03 Case Study – Point of Presence from Rio de Janeiro

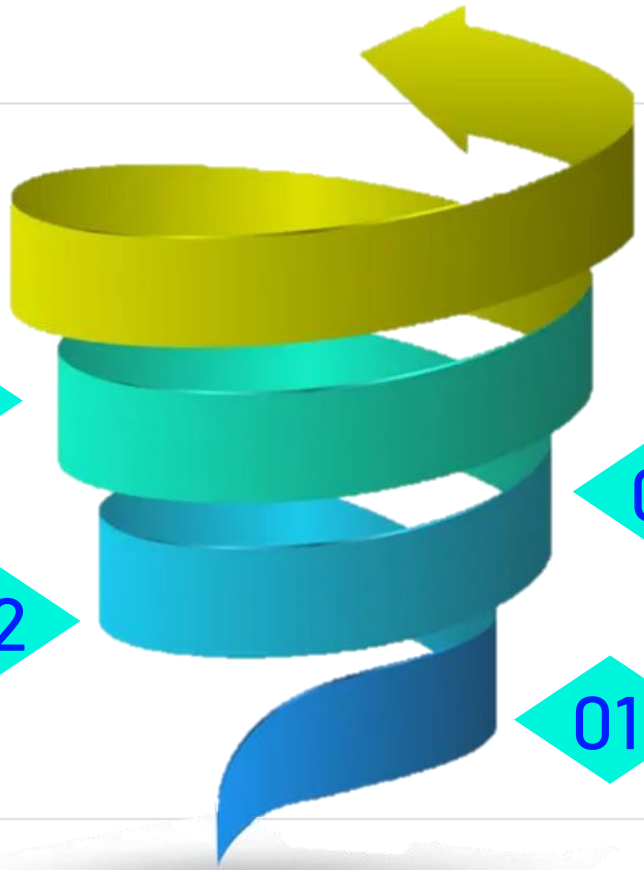
02 Feedbacks from security and corporate risks teams

01 PILOT - LIneA (RNP ecosystem) and LNCC (e-Science)

Methodology Design

RNP

Upward spiral



06 Applications and risk management

05 Feedbacks from leadership

04 Case Study – CAFe (internal solution)

03 Case Study – Point of Presence from Rio de Janeiro

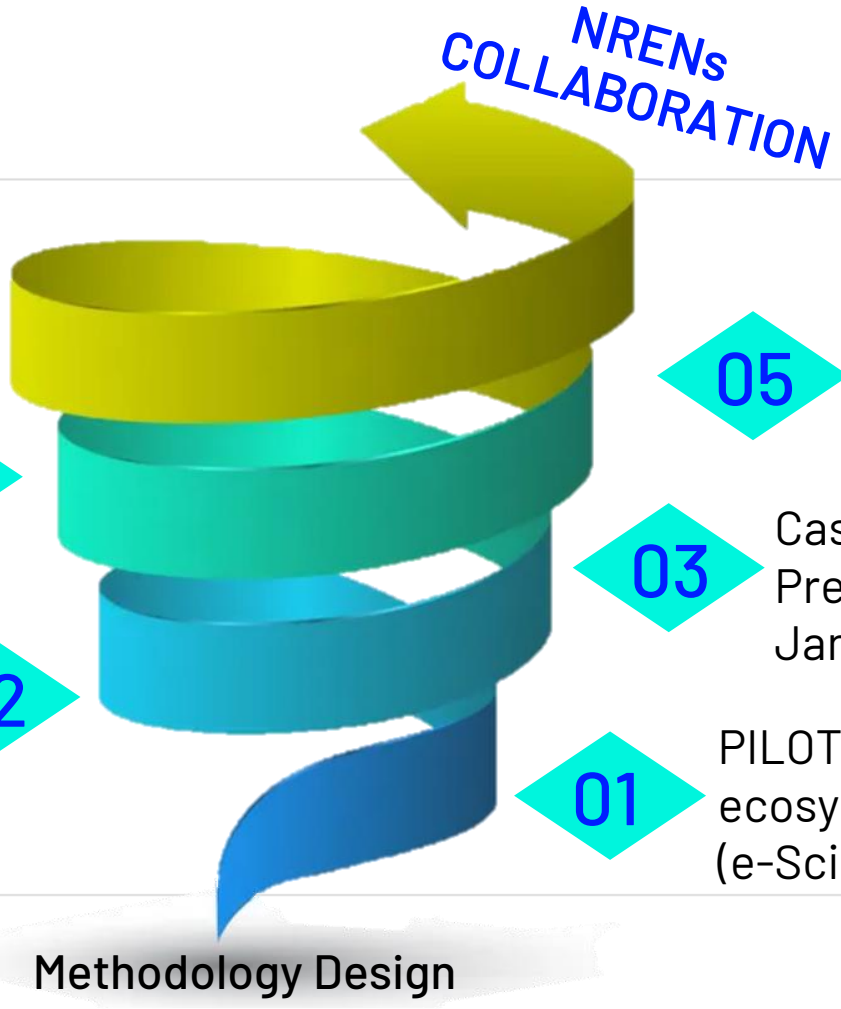
02 Feedbacks from security and corporate risks teams

01 PILOT - LIneA (RNP ecosystem) and LNCC (e-Science)

Methodology Design

RNP

Upward spiral



06 Applications and risk management

05 Feedbacks from leadership

04 Case Study – CAFe (internal solution)

03 Case Study – Point of Presence from Rio de Janeiro

02 Feedbacks from security and corporate risks teams

01 PILOT - LIneA (RNP ecosystem) and LNCC (e-Science)

RNP

Lessons Learned

- **Risk management is continuous** – Always ask: "What's changed? What new risks emerged?"

Lessons Learned

- **Risk management is continuous** – Always ask: "What's changed? What new risks emerged?"
- **Collaboration is non-negotiable** – Cybersecurity is everyone's responsibility.

Lessons Learned

- **Risk management is continuous** – Always ask: "What's changed? What new risks emerged?"
- **Collaboration is non-negotiable** – Cybersecurity is everyone's responsibility.
- **Celebrate wins** – Even small risk mitigations deserve recognition.

Lessons Learned

- **Risk management is continuous** – Always ask: "What's changed? What new risks emerged?"
- **Collaboration is non-negotiable** – Cybersecurity is everyone's responsibility.
- **Celebrate wins** – Even small risk mitigations deserve recognition.
- **Start small, scale smart** – Begin with limited scopes; expand as maturity grows.

Lessons Learned

- **Risk management is continuous** – Always ask: "What's changed? What new risks emerged?"
- **Collaboration is non-negotiable** – Cybersecurity is everyone's responsibility.
- **Celebrate wins** – Even small risk mitigations deserve recognition.
- **Start small, scale smart** – Begin with limited scopes; expand as maturity grows.
- **Communicate directly** – No intermediaries. Clarity drives buy-in.

Lessons Learned

- **Risk management is continuous** – Always ask: "What's changed? What new risks emerged?"
- **Collaboration is non-negotiable** – Cybersecurity is everyone's responsibility.
- **Celebrate wins** – Even small risk mitigations deserve recognition.
- **Start small, scale smart** – Begin with limited scopes; expand as maturity grows.
- **Communicate directly** – No intermediaries. Clarity drives buy-in.
- **Expect (and overcome) resistance** – Discomfort means you're changing the status quo.

Lessons Learned

- **Risk management is continuous** – Always ask: "What's changed? What new risks emerged?"
- **Collaboration is non-negotiable** – Cybersecurity is everyone's responsibility.
- **Celebrate wins** – Even small risk mitigations deserve recognition.
- **Start small, scale smart** – Begin with limited scopes; expand as maturity grows.
- **Communicate directly** – No intermediaries. Clarity drives buy-in.
- **Expect (and overcome) resistance** – Discomfort means you're changing the status quo.
- **When in doubt, assume the worst** – Err on the side of caution in assessments.

Lessons Learned

- **Risk management is continuous** – Always ask: "What's changed? What new risks emerged?"
- **Collaboration is non-negotiable** – Cybersecurity is everyone's responsibility.
- **Celebrate wins** – Even small risk mitigations deserve recognition.
- **Start small, scale smart** – Begin with limited scopes; expand as maturity grows.
- **Communicate directly** – No intermediaries. Clarity drives buy-in.
- **Expect (and overcome) resistance** – Discomfort means you're changing the status quo.
- **When in doubt, assume the worst** – Err on the side of caution in assessments.
- **Culture eats strategy** – With practice, risk-thinking becomes second nature.

RNP

A risk-based strategy isn’t just protection – it’s the art of **making uncertainty work for you**.

That's not just security – **that's working smarter** with focus

In the end, cybersecurity is about enabling the great mission of the academic community: to do science, to improve the world, and to improve people's lives.

We can't let security challenges get in the way of that mission.

THANK YOU!

ingrid.barbosa@rnp.br

humberto.forsan@rnp.br