cais Inteligência em Cibersegurança RNP

# Segurança da Informação: além das ferramentas, uma questão de estratégia

Renan Silva – CAIS/RNP

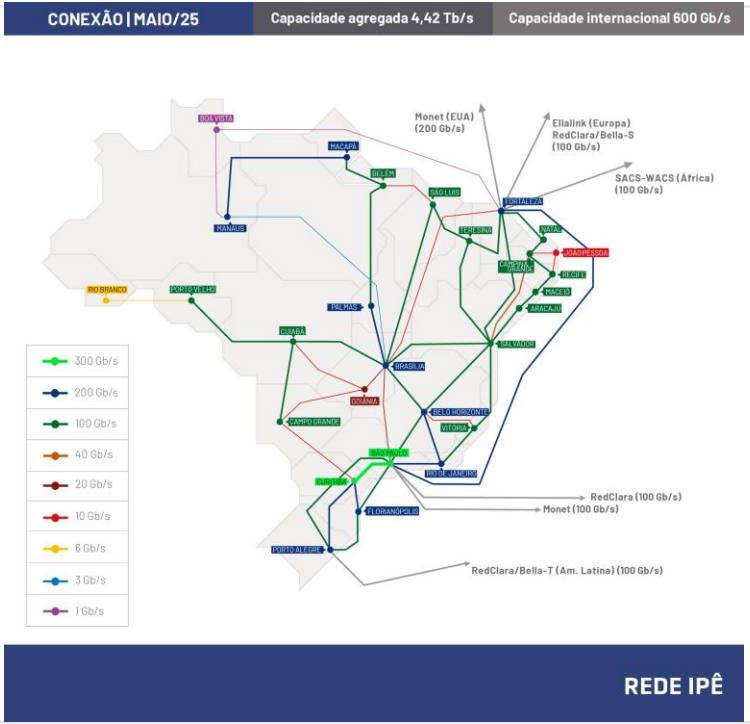
TLP: CLEAR

# Agenda

- Estar em conformidade com normas e frameworks não garantem segurança estratégica;
- Ferramentas só geram resultado quando fazem parte de uma estratégia;
- Por onde podemos começar.

# RNP – Rede Nacional de Ensino e Pesquisa

- Internet de alta capacidade, serviços personalizados e promoção de projetos de inovação.
- Beneficiamos 4 milhões de alunos, professores e pesquisadores brasileiros.
- Pioneiros, ao trazer uma rede de internet para o Brasil e a primeira rede de fibra ótica na América Latina em 2005.
- Apoiamos com tecnologia e serviços mais de 1800 universidades, institutos educacionais e culturais, agências de pesquisa, hospitais de ensino, parques e polos tecnológicos.




TLP: CLEAR

# CAIS – Inteligência em Cibersegurança

cais

Promover e impulsionar o desenvolvimento e uso seguro de CT&I (ciência, tecnologia e inovação)

RNP

TLP: CLEAR

# CONFORMIDADE X SEGURANÇA

TLP: CLEAR

# Padrões, normas, frameworks e regulações


Fonte: https://drata.com/grc-central/security-frameworks

# Segurança por conformidade

**Cloud Security Alliance**

*"Uma abordagem centrada na conformidade geralmente enfatiza a documentação e o cumprimento de requisitos em detrimento da mitigação proativa de ameaças.*

*Isso pode levar a um modelo de segurança estático que pode não se adaptar rapidamente às ameaças emergentes, deixando as organizações vulneráveis, apesar de estarem "em conformidade"."*

Fonte: https://cloudsecurityalliance.org/blog/2025/08/27/risk-based-vs-compliance-based-security-why-one-size-doesn-t-fit-all#

RNP

# 5 principais problemas ao implementar ISO/IEC 27001


Fonte: Evaluation of ISO/IEC 27001 Framework Implementation for Information Security in Organizations: A Systematic Literature Review (Universitas Sebelas April)

RNP

# PADRÕES E NORMAS SÃO IMPORTANTES E ÚTEIS QUANDO BEM IMPEMENTADAS

RNP

TLP: CLEAR

# COMO ABORDAMOS O USO DE FERRAMENTAS?

# COMO É A SEGURANÇA DO SEU AMBIENTE?

RNP

TLP: CLEAR

# Ferramentas vs Estratégia

***Sam Olyaei -***
*Cybersecurity VP*
*(Gartner)*

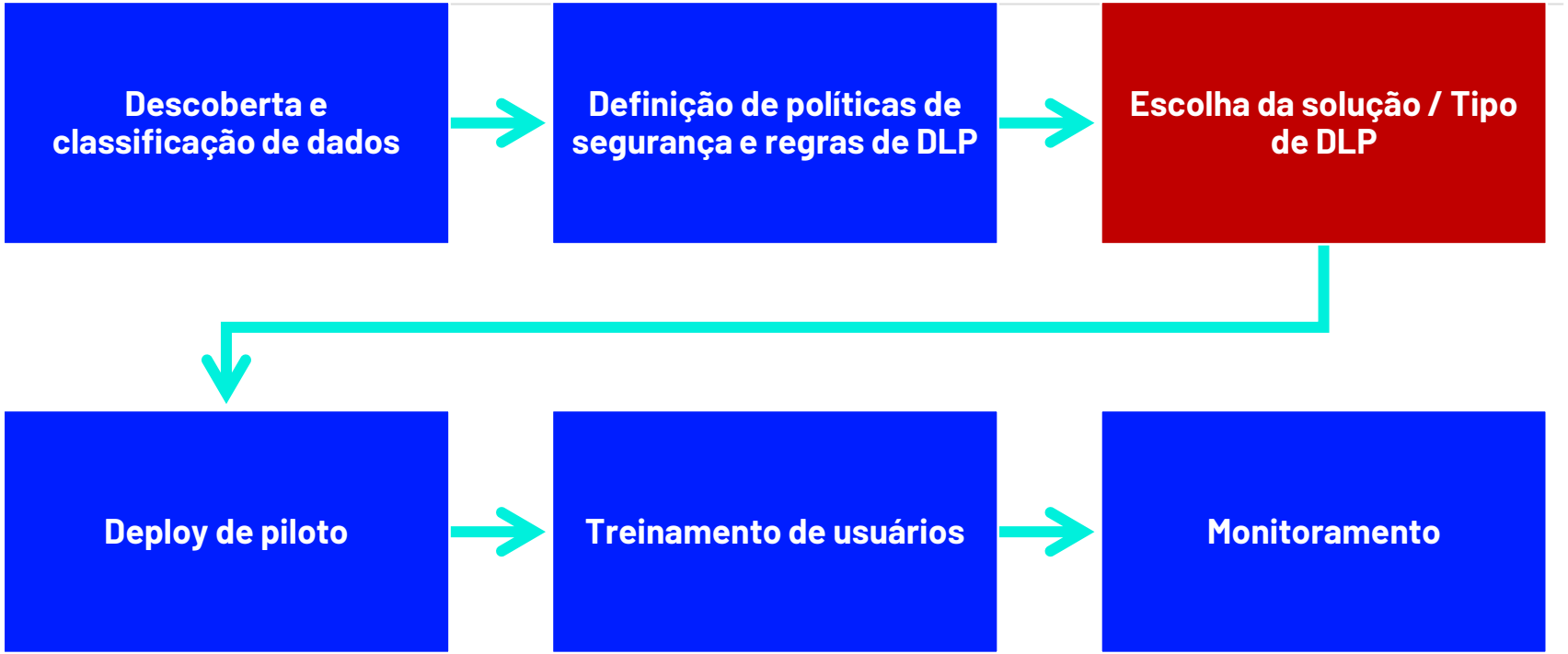
"CISOs frequentemente escolhem ferramentas inadequadas porque não partem de uma estratégia clara.

Em vez de definir primeiro os processos e as pessoas necessárias, tentam resolver tudo com tecnologia.

Muitas vezes, o problema exige contratar alguém ou amadurecer um processo — não comprar mais uma ferramenta.

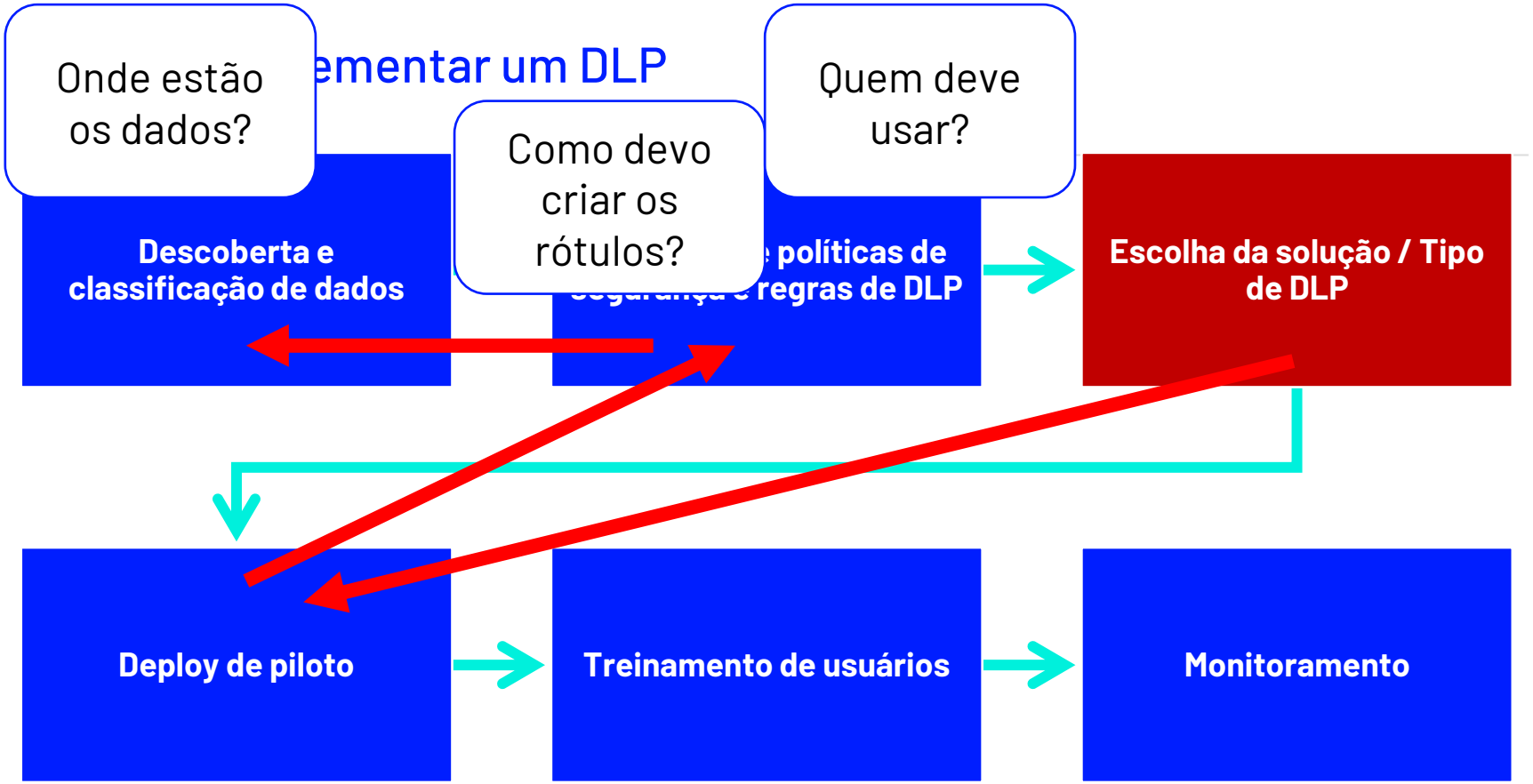
Fonte: https://www.csoonline.com/article/570077/do-you-have-a-security-tools-gap.html

# Ex. Implementar um DLP




RNP

TLP: CLEAR




RNP

TLP: CLEAR

# ONDE A ESTRATÉGIA COMEÇA?

Uma **estratégia de cibersegurança** é um plano abrangente desenvolvido para proteger os sistemas de informação, os dados e as redes de uma organização contra ameaças cibernéticas.

**Ela se alinha aos objetivos gerais do negócio** e garante que a organização possa gerenciar e mitigar de forma eficaz os riscos associados a ataques cibernéticos.

Fonte: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-strategy

RNP

Fonte: Pixabay

RNP

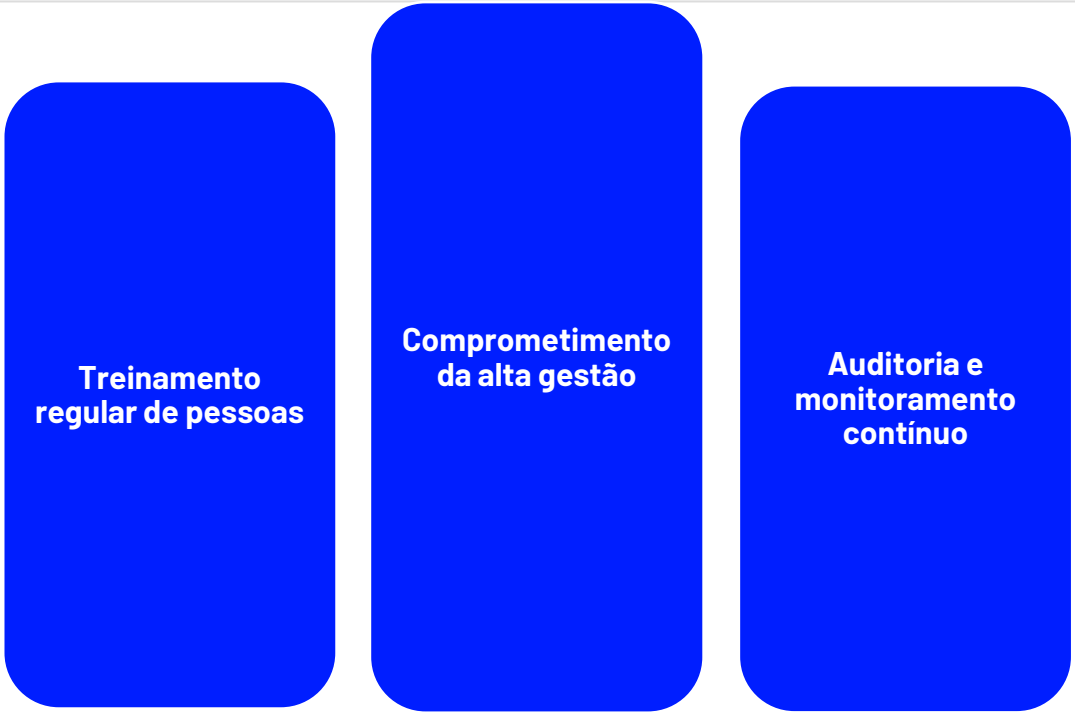
TLP: CLEAR

Fonte: Gerado por IA

RNP

TLP: CLEAR

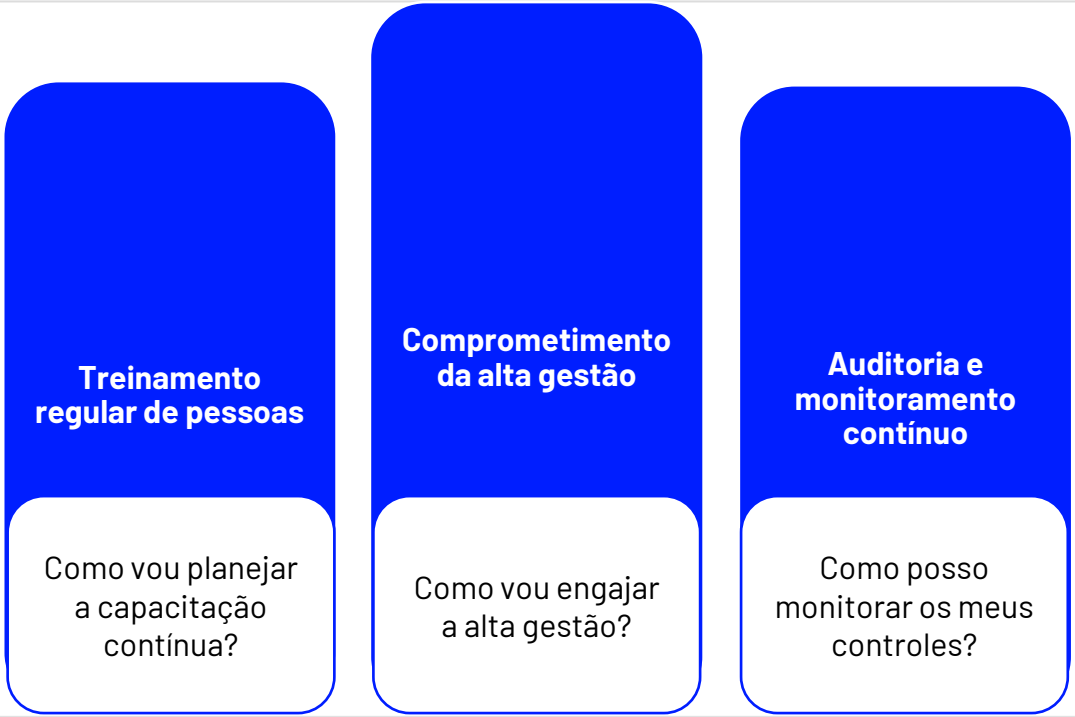
# 3 principais fatores de sucesso ao implementar ISO/IEC 27001




Fonte: Evaluation of ISO/IEC 27001 Framework Implementation for Information Security in Organizations: A Systematic Literature Review (Universitas Sebelas April)

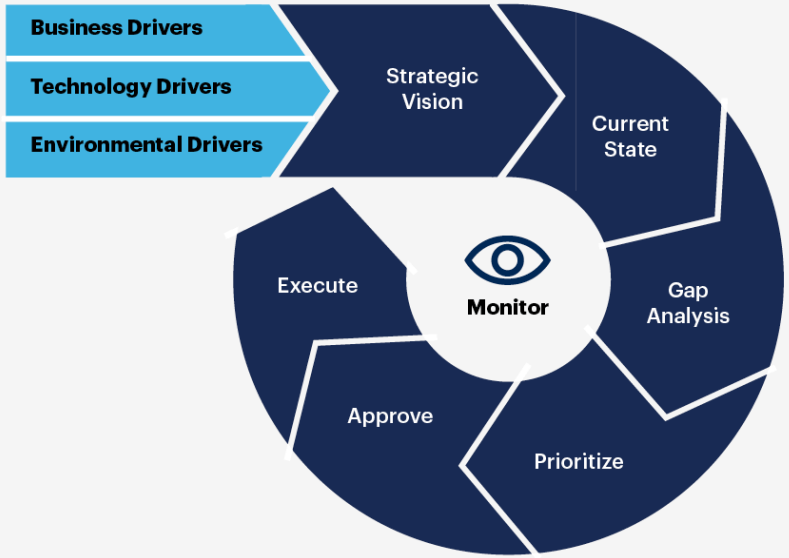
RNP

# 3 principais fatores de sucesso ao implementar ISO/IEC 27001




Fonte: Evaluation of ISO/IEC 27001 Framework Implementation for Information Security in Organizations: A Systematic Literature Review (Universitas Sebelas April)

# Security Strategy Planning Process




Source: Gartner

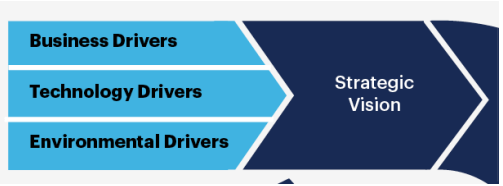

Gartner

Fonte: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-strategy

RNP

TLP: CLEAR

# Direcionadores e visão estratégica




**Direcionadores**

**Negócio:** objetivos de negócio, expansão, compliance, redução de risco.

**Tecnologia:** cloud, modernização, novas arquiteturas e tecnologias.

**Ambiente:** cenário de ameaças, leis, economia, exigências do setor.

Definem por que a estratégia é necessária e quais fatores a direcionam.

**Visão Estratégica**

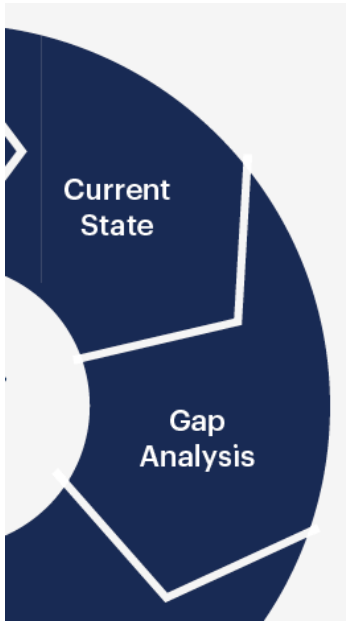
Estabelece onde a organização deseja chegar em maturidade de segurança.

Define princípios, prioridades e o papel da segurança no negócio.

Cria o alinhamento entre segurança e objetivos corporativos.

Fonte: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-strategy

# Estado atual e análise de gaps




**Estado Atual**

Diagnóstico completo da situação atual de segurança.

Avaliação de controles, processos, ferramentas e equipe.

Identificação da maturidade atual.

**Análise de gaps**

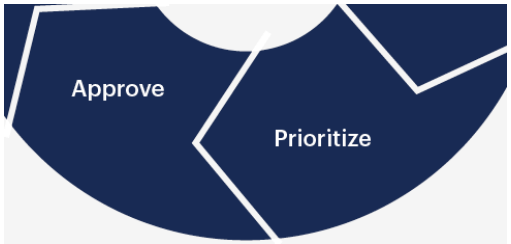
Compara o estado atual com a visão estratégica desejada.

Identifica deficiências, pontos ausentes e oportunidades de melhoria.

Fundamenta as ações necessárias para evolução.

Fonte: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-strategy

# Priorização e aprovação




**Priorização**

Ordena as iniciativas que são prioritárias considerando:

- impacto no negócio e nível de risco
- custo x benefício
- prazos e urgência regulatória
- Vou adotar uma norma e um framework?

**Aprovação**

Apresentação das iniciativas e roadmap à alta gestão.

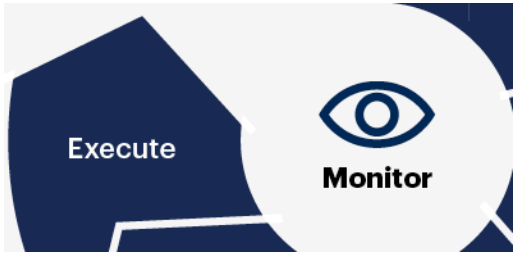
Definição e aprovação de orçamento.

Acordo de responsabilidades, prazos e metas.

Formalização da governança da estratégia.

Fonte: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-strategy

# Executar e monitorar




**Execução**

Implementação dos projetos e controles de segurança.

Criação ou atualização de processos e políticas.

Capacitação da equipe.

Implantação de ferramentas — quando justificadas por estratégia.

**Monitoramento Contínuo**

Acompanhamento de métricas e KPIs de segurança.

Avaliação de riscos e amadurecimento contínuo.

Ajustes no roadmap conforme mudanças no ambiente e no negócio.

Fonte: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-strategy

# Wrap-up

- ✓ Segurança eficaz exige estratégia, não apenas ferramentas.
- ✓ Direcionadores de negócio, tecnologia e ambiente orientam decisões.
- ✓ Análise do estado atual e das lacunas direciona investimentos.
- ✓ Priorização cria um roadmap claro e focado em risco.
- ✓ Aprovação da gestão garante recursos e alinhamento.
- ✓ Execução combina pessoas, processos e tecnologia.
- ✓ Monitoramento contínuo mantém a estratégia e ajuda direcionar melhorias.

# PERGUNTAS?

# OBRIGADO

*renan.silva@rnp.br*