

Gestão de Riscos e Proteção de Dados Pessoais

Palestrante: Léo Farias



Gestão de Riscos



- **A LGPD e o risco.**
- **O que é risco?**
- **Como posso gerir riscos?**

Risco

“Risco é o efeito da incerteza nos objetivos. Risco é normalmente expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades.

Um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças.

Objetivos podem possuir diferentes aspectos e categorias, e podem ser aplicados em diferentes níveis.”

- ABNT NBR ISO/IEC 27005:2023

Alto risco

“Conceito utilizado em diferentes contextos, como, por exemplo:

- estabelecer regulação assimétrica para agentes de pequeno porte;*
- deflagrar a necessidade de comunicação de incidente de segurança; e*
- apoiar a definição da dosimetria da sanção administrativa.”*

- Miriam Wimmer, Diretora da ANPD



ASSOCIAÇÃO
BRASILEIRA
DE NORMAS
TÉCNICAS

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



**Center for
Internet Security®**

Creating Confidence in the Connected World.™



UK Government

gov.br

The Orange Book

Management of Risk – Principles and Concepts

GUIA ORIENTATIVO

TRATAMENTO DE DADOS
PESSOAIS DE ALTO RISCO

Em elaboração

Minuta - Estudo preliminar

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

This publication contains comprehensive updates to the Risk Management Framework. The updates include an alignment with the constructs in the NIST Cybersecurity Framework; the integration of privacy risk management processes; an alignment with system life cycle security engineering processes; and the incorporation of supply chain risk management processes. Organizations can use the frameworks and processes in a complementary manner within the RMF to effectively manage security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. Revision 2 includes a set of organization-wide RMF tasks that are designed to prepare information system owners to conduct system-level risk management activities. The intent is to increase the effectiveness, efficiency, and cost-effectiveness of the RMF by establishing a closer connection to the organization's missions and business functions and improving the communications among senior leaders, managers, and operational personnel.

JOINT TASK FORCE

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-372>

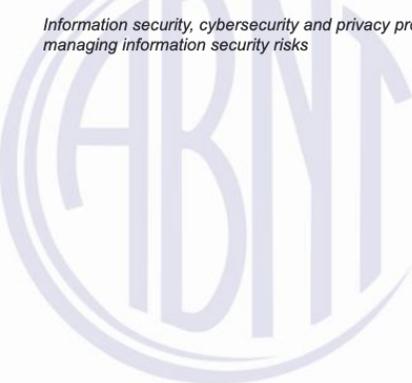
NORMA
BRASILEIRA

ABNT NBR
ISO/IEC
27005

Quarta edição
30.05.2023

Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação

Information security, cybersecurity and privacy protection — Guidance on managing information security risks



CIS Risk Assessment Method (RAM)

Version 2.1

Core Document

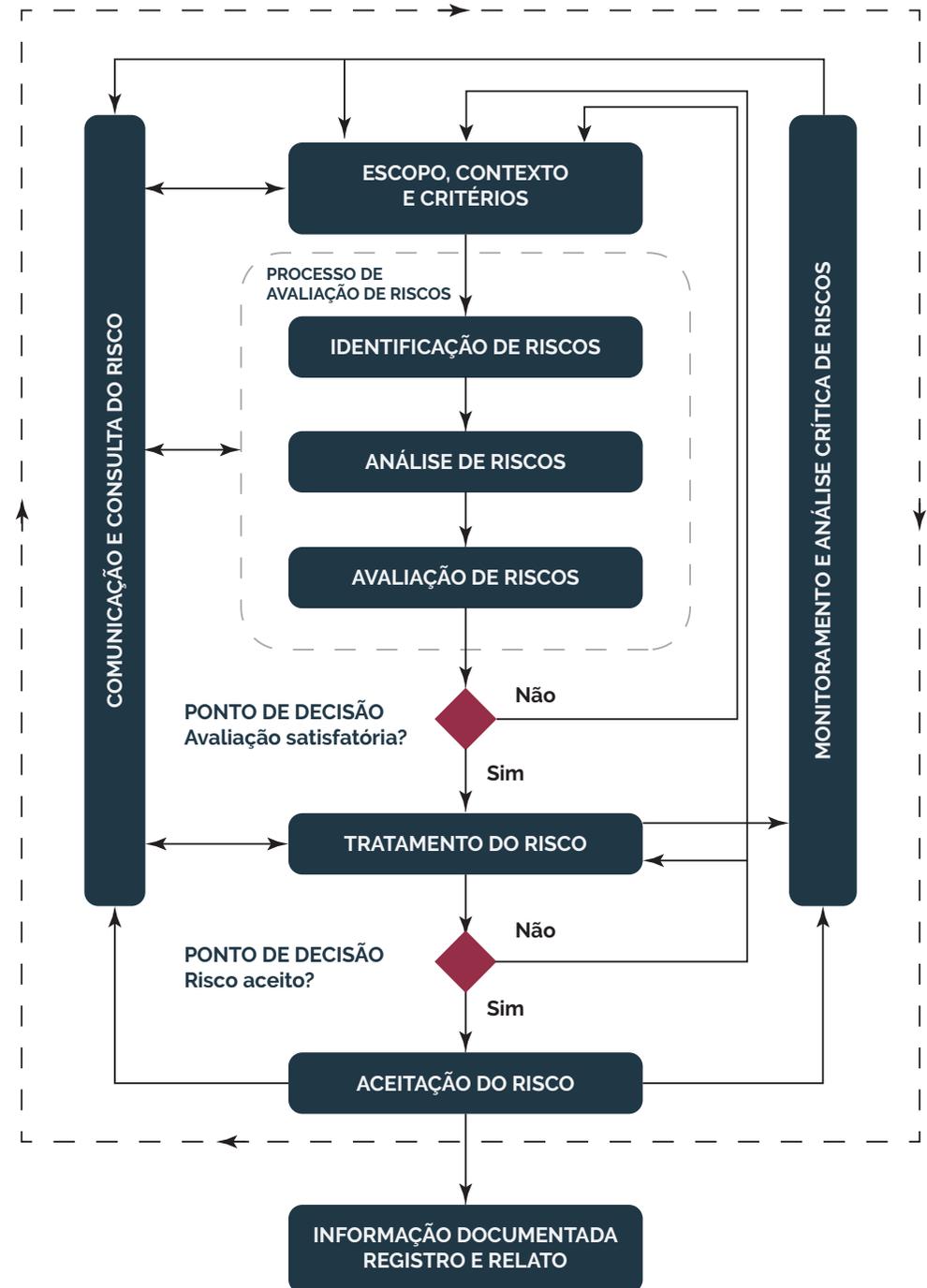
Guia de Avaliação de Riscos de
Segurança e Privacidade

LEI GERAL DE PROTEÇÃO DE
DADOS PESSOAIS (LGPD)

Versão 1.0
Brasília, Novembro de 2020

Gestão de Riscos

- Integração com a governança;
- Todos têm responsabilidade;
- Consideração do comportamento humano e cultural;
- O processo de gestão de riscos é frequentemente apresentado como sequencial;
- Monitoramento e análise crítica precisam ser parte integrante da implementação do tratamento de riscos;
- O relato é parte integrante da governança da organização.





Sistema de
Gestão de Riscos

Governança
Organizacional



Sistema de
Gestão de
Segurança da
Informação



Governança
SegInfo

Sistema de
Gestão de
Privacidade da
Informação



Sistema da
Qualidade



Sistema de
Gestão de
Continuidade
de Negócios

Governança
TI

Normas Essencias para Gestão de Riscos

- ABNT NBR ISO/IEC 27557:2023 - Segurança da Informação, segurança cibernética e proteção da privacidade — Aplicação da ABNT NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional;
- ABNT NBR ISO/IEC 27005:2023 - Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação;
- ABNT NBR IEC 31010:2021 - Gestão de riscos - Técnicas para o processo de avaliação de riscos;
- ABNT NBR ISO 31022:2020 - Gestão de riscos — Diretrizes para a gestão de riscos legais;
- ABNT NBR 16337:2020 - Gerenciamento de riscos em projetos — Princípios e diretrizes gerais;
- ABNT NBR ISO/IEC 23894:2023 - Tecnologia da informação — Inteligência artificial — Orientações sobre gestão de riscos.



in

[linkedin.com/in/leocfarias](https://www.linkedin.com/in/leocfarias)



<https://www.acpdbrasil.com>



[@leofarias.learning](https://www.instagram.com/leofarias.learning)

