

Gestão de Riscos e Compliance com a LGPD



*Lei Geral de Proteção de Dados





Cesar Monteiro

Professor de Pós-Graduação na Universidade Mackenzie, Mestre em Administração do Desenvolvimento de Negócios no Mackenzie. Mestre em ISO 20000 pelo Exin e Pós-Graduado em Análise de Sistemas pela FAAP. Tradutor do ITIL para o Brasil é DPO, ITIL 4 Managing Professional e ITIL 4 Strategic Leader. É o responsável pelo desenvolvimento de cursos e gestão das consultorias na IT Partners.

Leandro Macedo

Professor de Pós Graduação na Fundação de Getúlio Vargas de Brasília, Titular em Gestão de TI na Universidade Católica de Brasília, Graduado em Administração Pública pela AEUDF. Membro da ISACA, ABPMP, PMI e ASEGI.

DPO e Auditor Lider. É Especialista em Gestão de Riscos além de ter participado em inúmeros projetos de implementações de ISO 20000 e ISO 270001.



O que é a Lei Geral de Proteção de Dados?

A **LGPD** tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

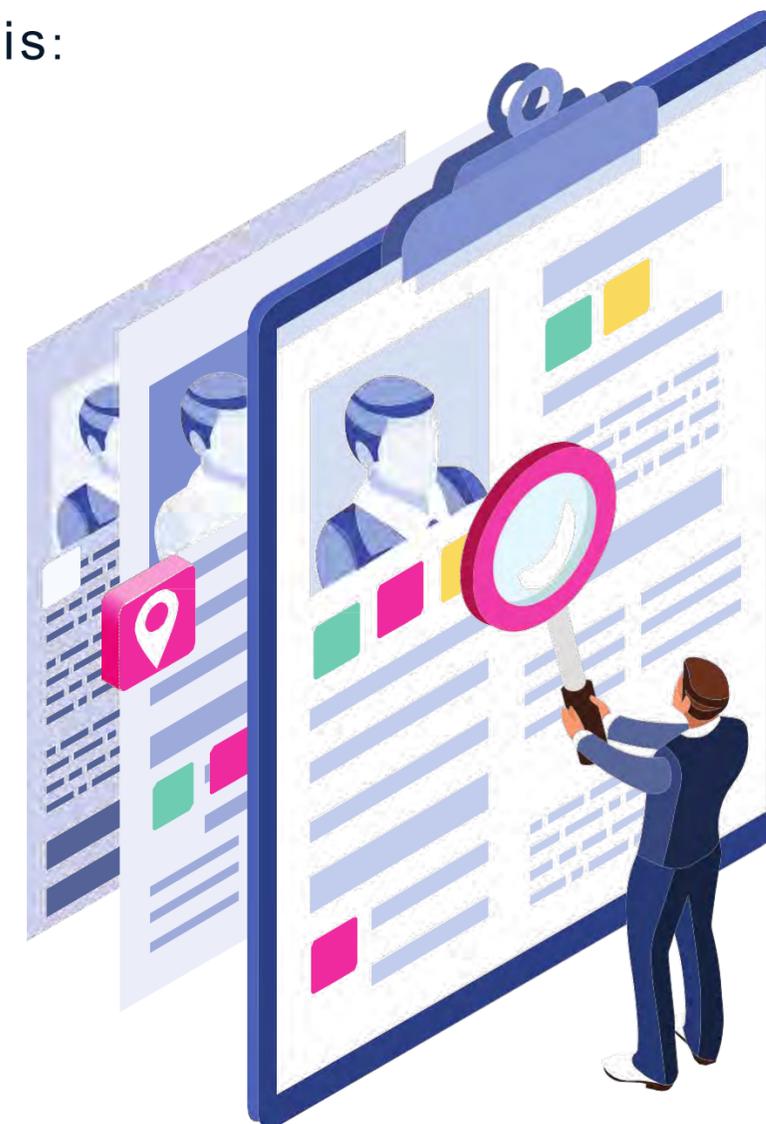
A lei define o que são dados pessoais e explica que alguns deles estão sujeitos a cuidados ainda mais específicos, como os dados pessoais sensíveis e dados pessoais sobre crianças e adolescentes. Esclarece ainda que todos os dados tratados, tanto no meio físico quanto no digital, estão sujeitos à regulação.



O QUE SÃO DADOS PESSOAIS?

Dados Pessoais (art. 5º, I) são os dados que permitem identificar uma pessoa ou torná-la identificável. São exemplos de dados pessoais:

- Nome
- Endereço
- Números Únicos Identificáveis (RG, CPF, CNH)
- Geolocalização
- Hábitos de Consumo
- Exames Médicos
- Dados referentes à saúde
- Biometria
- Perfil Cultural



O objetivo da LGPD é promover:



- Proteção à privacidade;
- Liberdade de expressão, informação, comunicação e opinião;
- Inviolabilidade da intimidade, honra e da imagem;
- Desenvolvimento econômico, tecnológico e inovação;
- Livre iniciativa, livre concorrência e a defesa do consumidor;
- Direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania.

QUAIS OS BENEFÍCIOS ESPERADOS DA LGPD?

1. Mais segurança em geral
2. Melhor regulamentação do mercado
3. Melhor relacionamento entre empresa e consumidor
4. Transparência
5. Melhor organização e gerenciamento de dados



PUNICÕES PREVISTAS PELA LEI:

As empresas que violarem a nova lei estarão sujeitas à aplicação de advertências, multas, bloqueios e eliminações de dados. As multas podem chegar a 2% do faturamento da organização, com um limite de R\$ 50 milhões por infração.

Empresas que estiverem plenamente adequadas à legislação contarão com vantagem competitiva em relação às demais empresas.



PASSOS PARA IMPLANTAR ALGPD NA SUA EMPRESA:

1

Estudo da LGPD e demais leis que regulamentam o negócio;



2.

Mapear a entrada e o tratamento dos dados;



3.

Analisar os riscos do tratamento e elaborar o Relatório de Impacto;



4.

Criar o plano de ação para se adequar à Lei com ajuda de especialistas.



PASSOS PARA IMPLANTAR ALGPD NA SUA EMPRESA:

1

Estudo da LGPD e demais leis que regulamentam o negócio;



2.

Mapear a entrada e o tratamento dos dados;



3.

Analisar os riscos do tratamento e elaborar o Relatório de Impacto;



4.

Criar o plano de ação para se adequar à Lei com ajuda de especialistas.

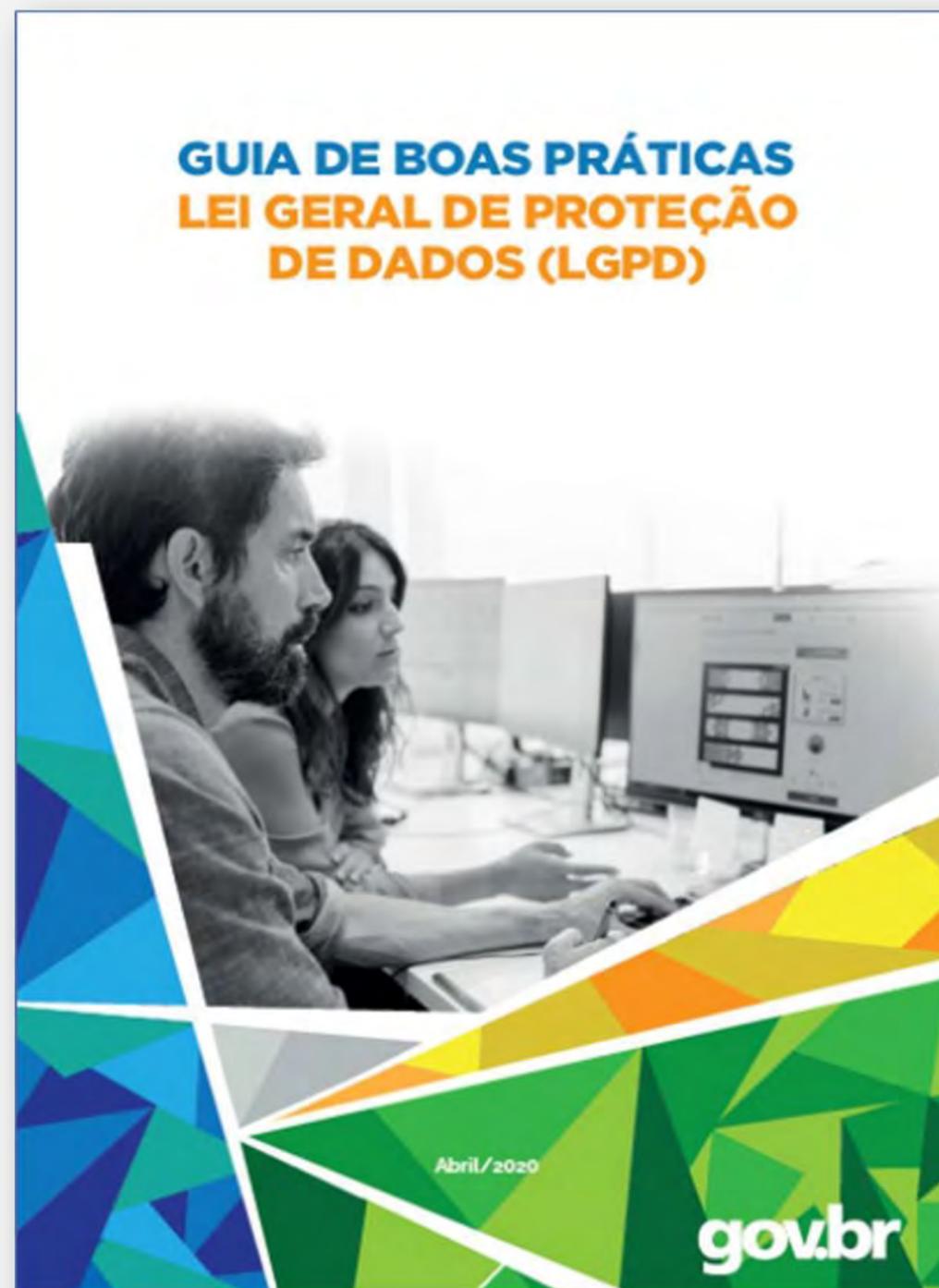


QUIZ !

Avaliação de Riscos de Segurança e Privacidade



Referência



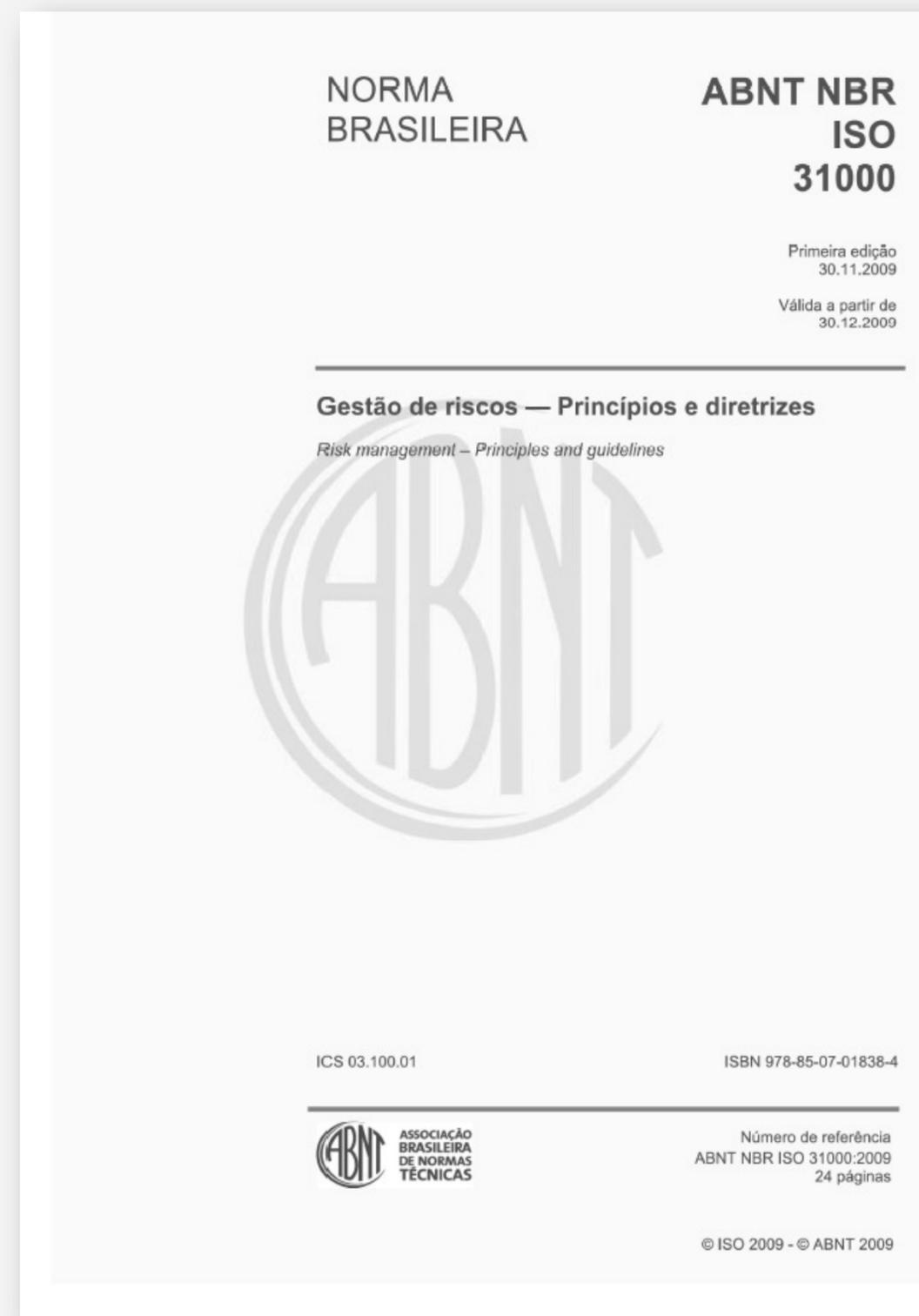
Avaliação de Riscos de Segurança e Privacidade



Referência



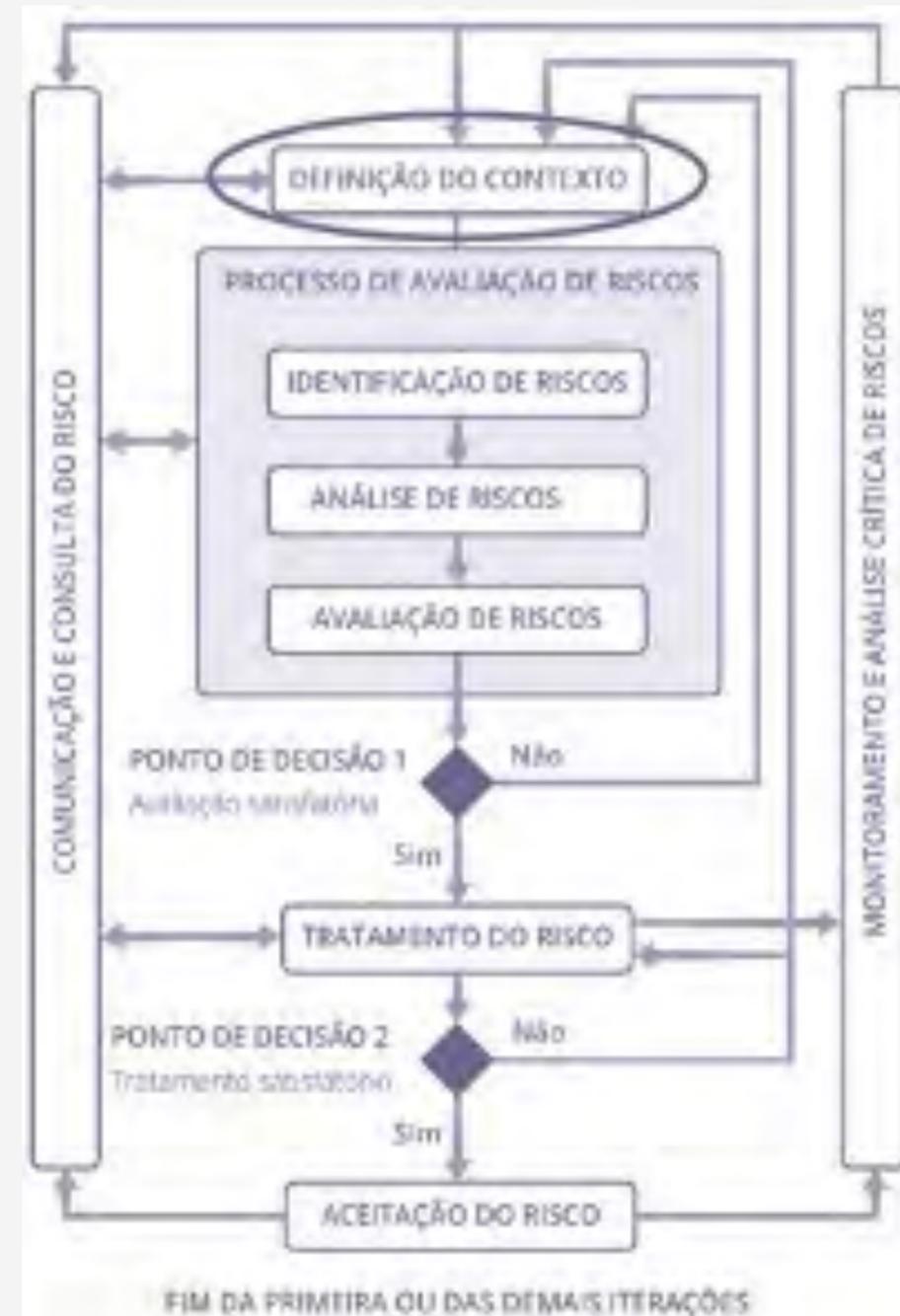
Curso ISO31000



Avaliação de Riscos de Segurança e Privacidade



Alinhamento de expectativas Definição do Contexto

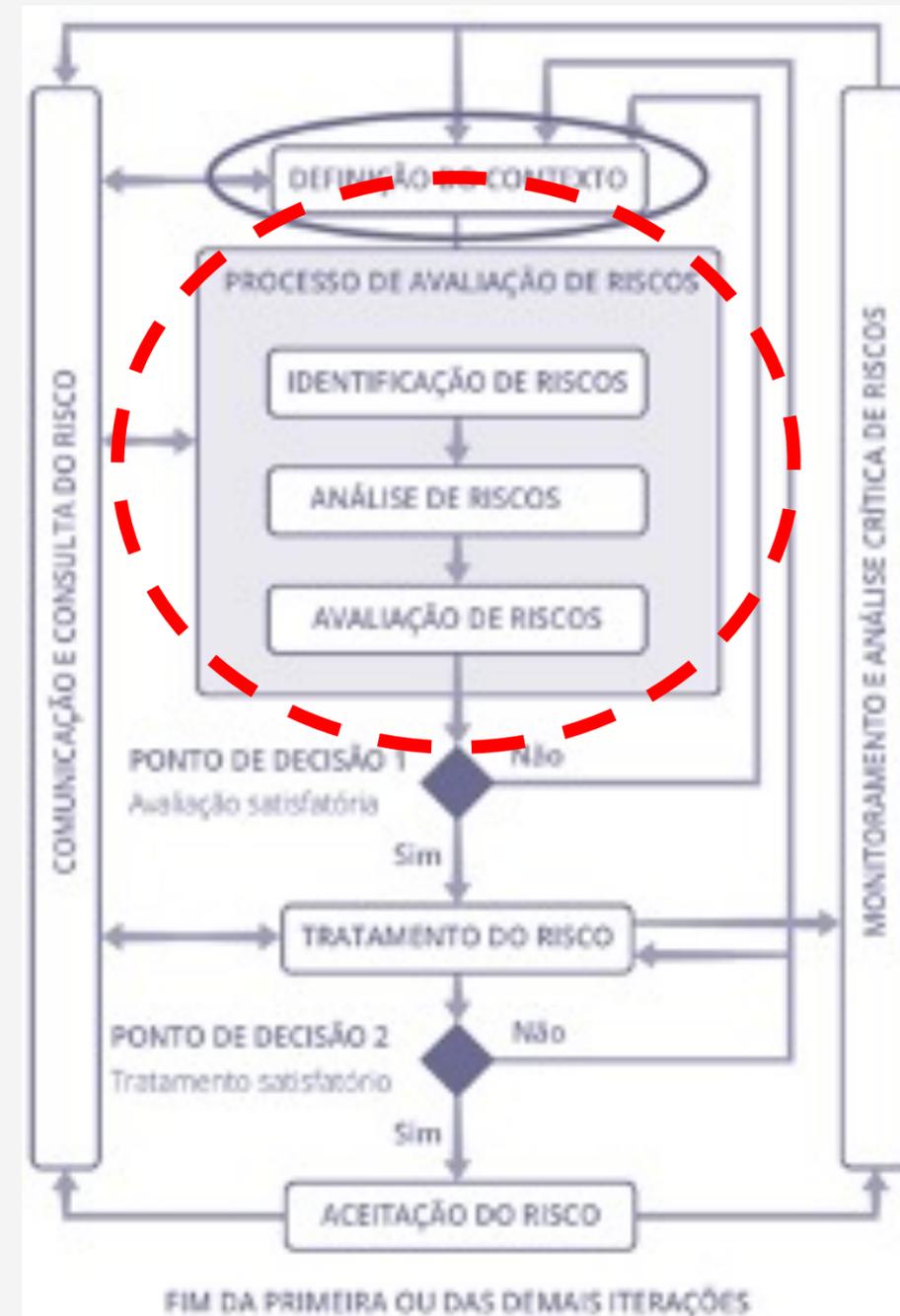


Processo de Gestão de Riscos – (ABNT NBR ISO/IEC 31000:2018)

Avaliação de Riscos de Segurança e Privacidade



Alinhamento de expectativas Análise / Avaliação



Avaliação de Riscos de Segurança e Privacidade



Alinhamento de expectativas Análise / Avaliação

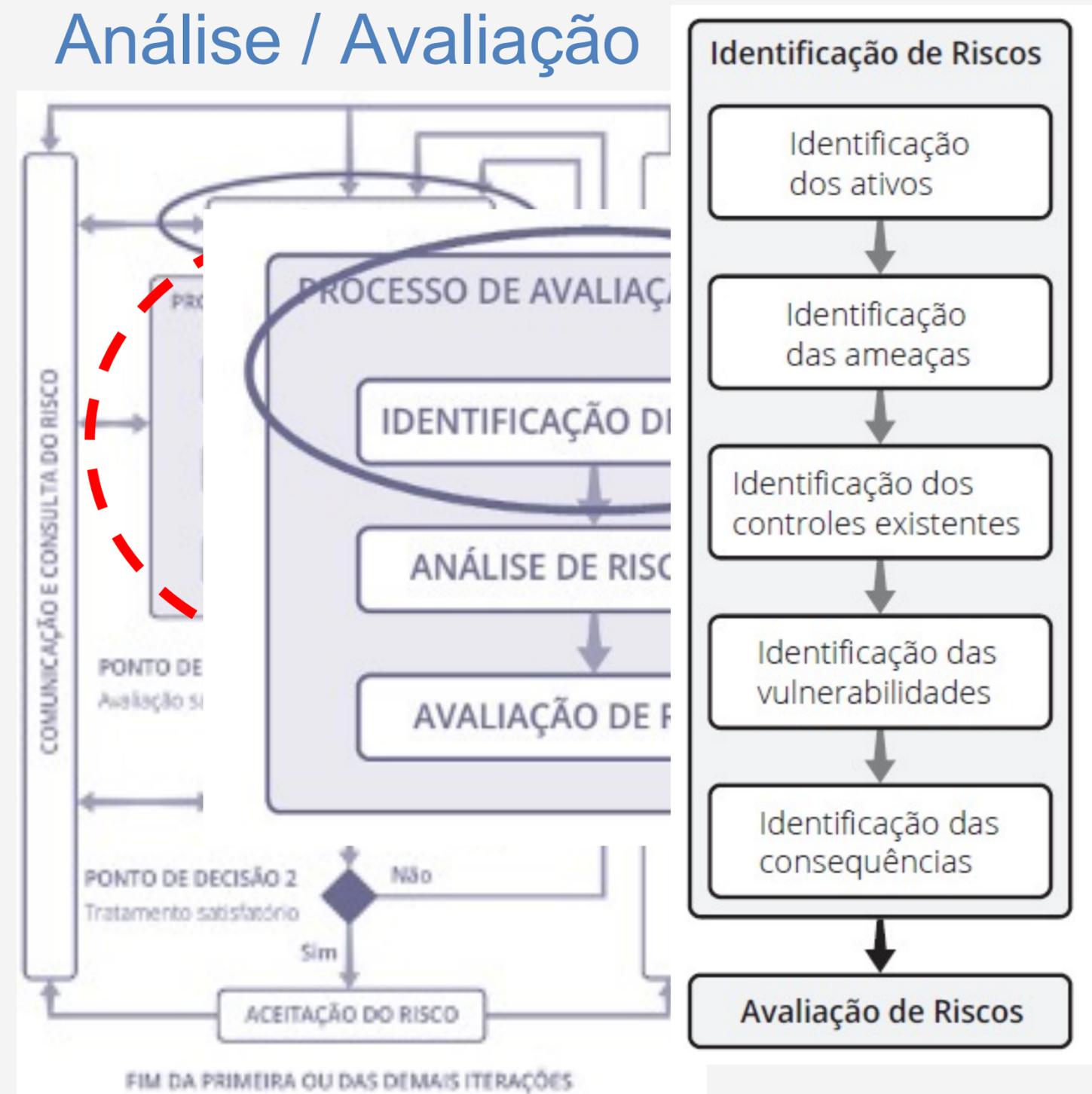


Processo de Gestão de Riscos – (ABNT NBR ISO/IEC 31000:2018)

Avaliação de Riscos de Segurança e Privacidade



Alinhamento de expectativas Análise / Avaliação



Avaliação de Riscos de Segurança e Privacidade



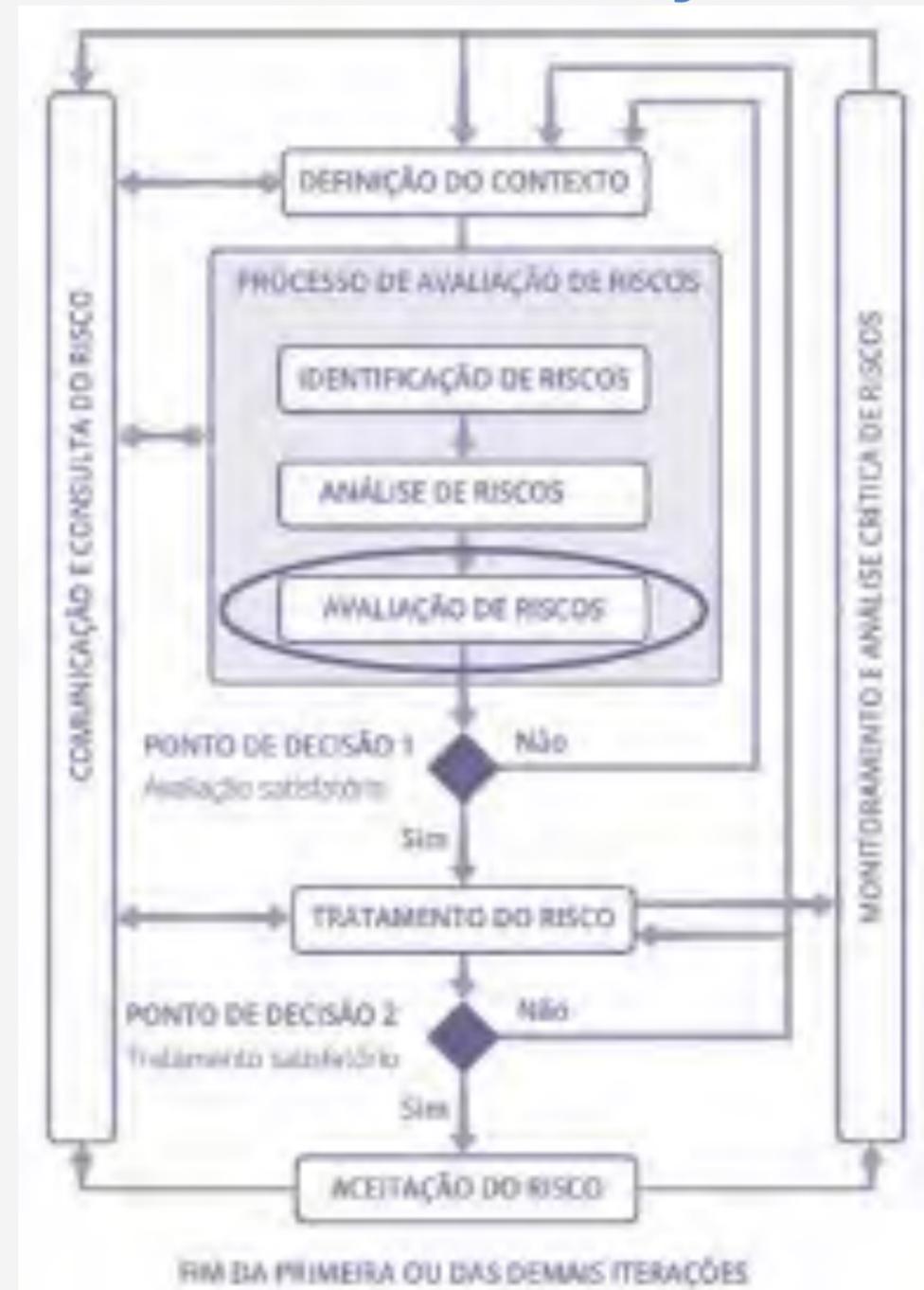
Alinhamento de expectativas Análise / Avaliação



Avaliação de Riscos de Segurança e Privacidade

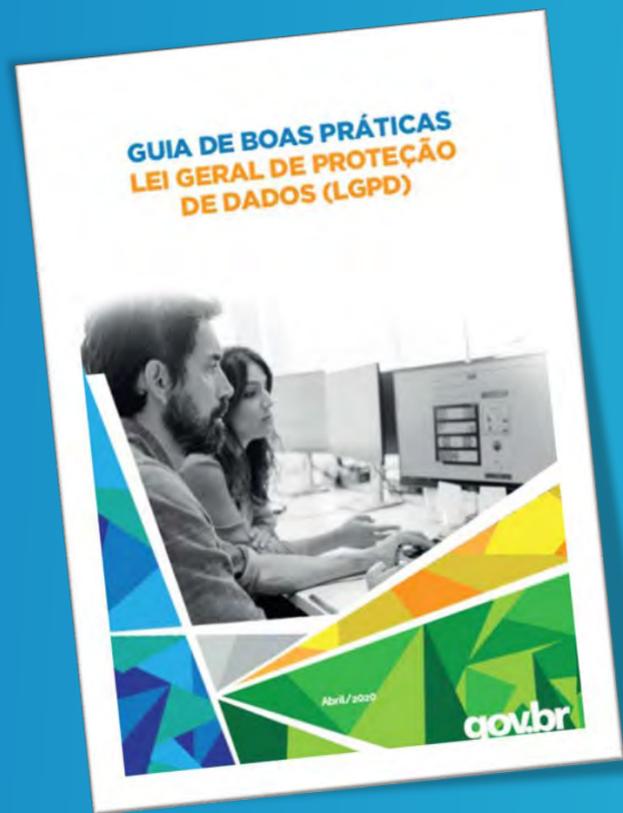


Alinhamento de expectativas Análise / Avaliação



Processo de Gestão de Riscos – (ABNT NBR ISO/IEC 31000:2018)

Avaliação de Riscos de Segurança e Privacidade



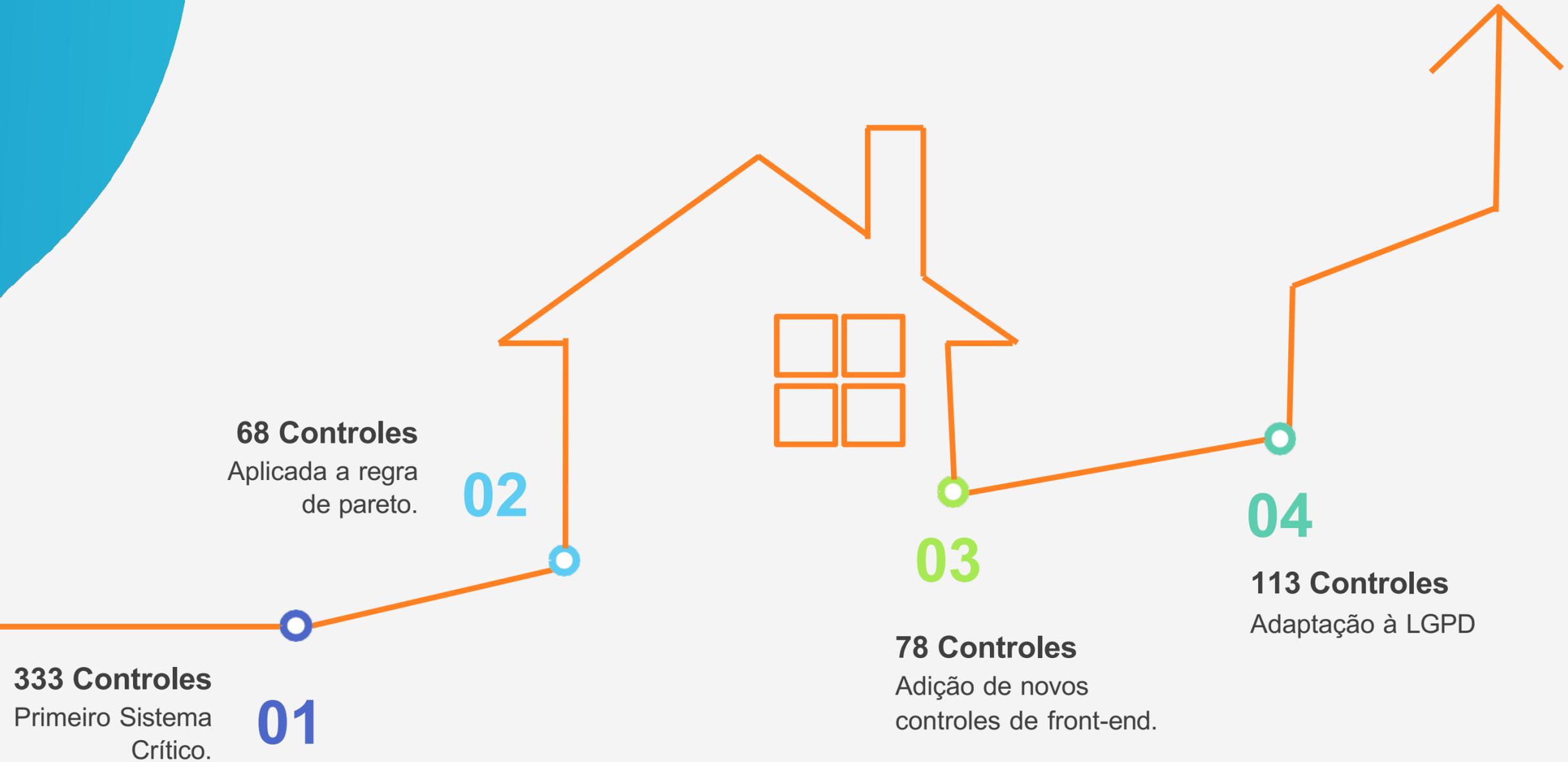
Alinhamento de expectativas Benefícios



Avaliação de Riscos de Segurança e Privacidade



Contexto



Avaliação de Riscos de Segurança e Privacidade



Etapas da Elaboração Dimensões



Avaliação de Riscos de Segurança e Privacidade



36 controles
processos e infraestrutura

Etapas da Elaboração Dimensões

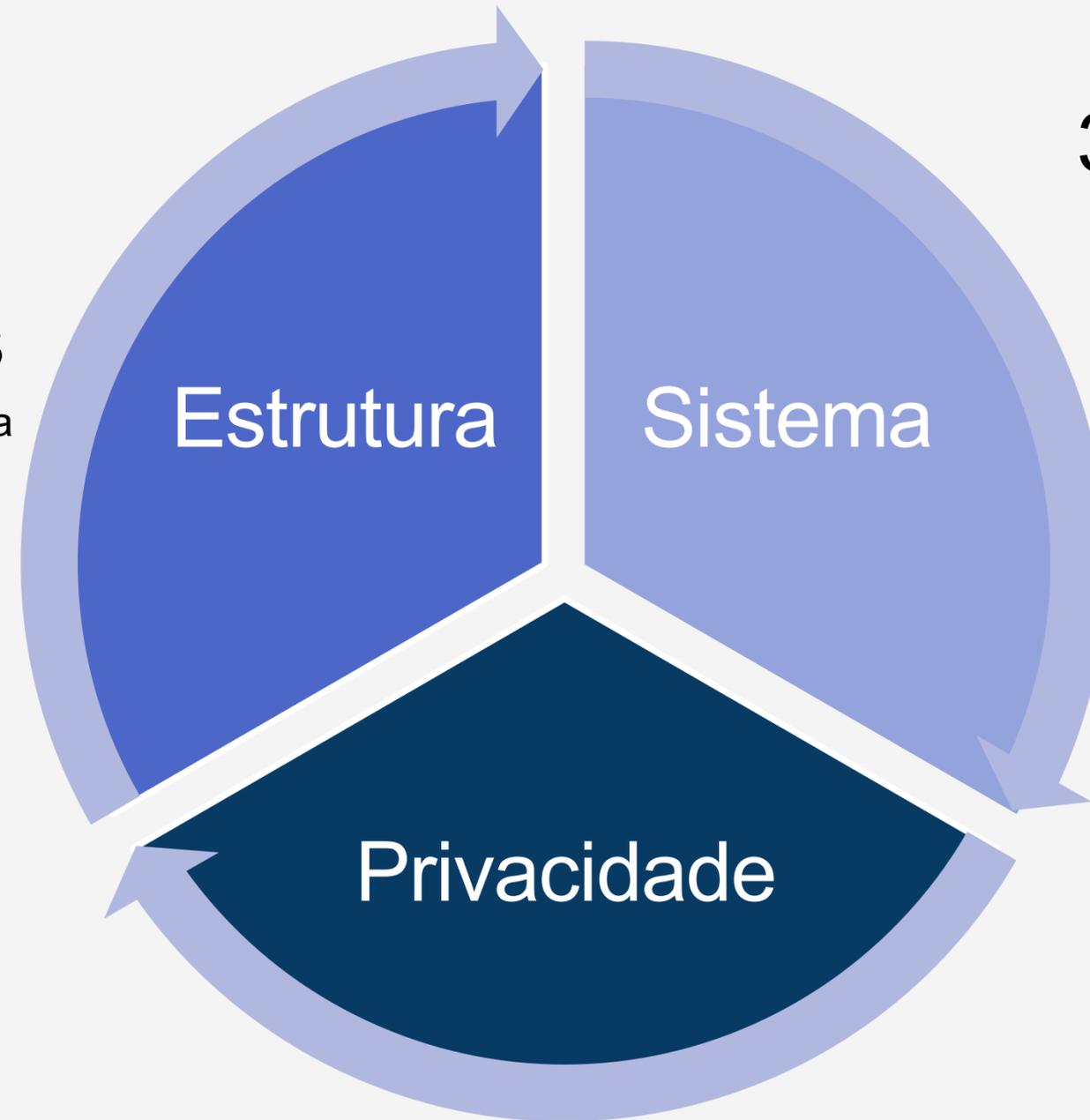


Avaliação de Riscos de Segurança e Privacidade



36 controles
processos e infraestrutura

Etapas da Elaboração Dimensões



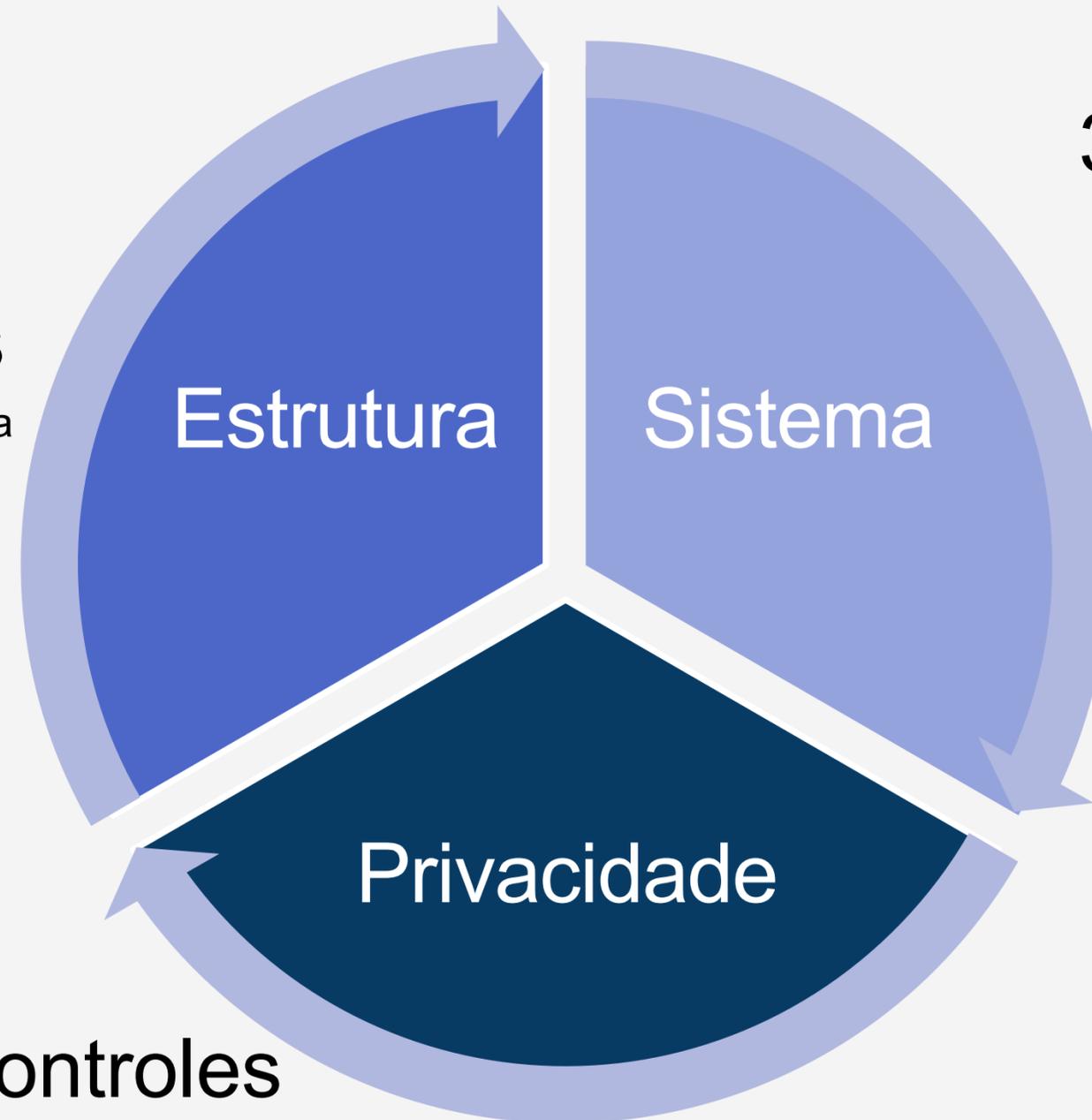
39 controles
Desenvolvimento seguro

Avaliação de Riscos de Segurança e Privacidade



Etapas da Elaboração Dimensões

36 controles
processos e infraestrutura



39 controles
Desenvolvimento seguro

38 controles
Conformidade legal com a LGPD

QUIZ !

Avaliação de Riscos de Segurança e Privacidade

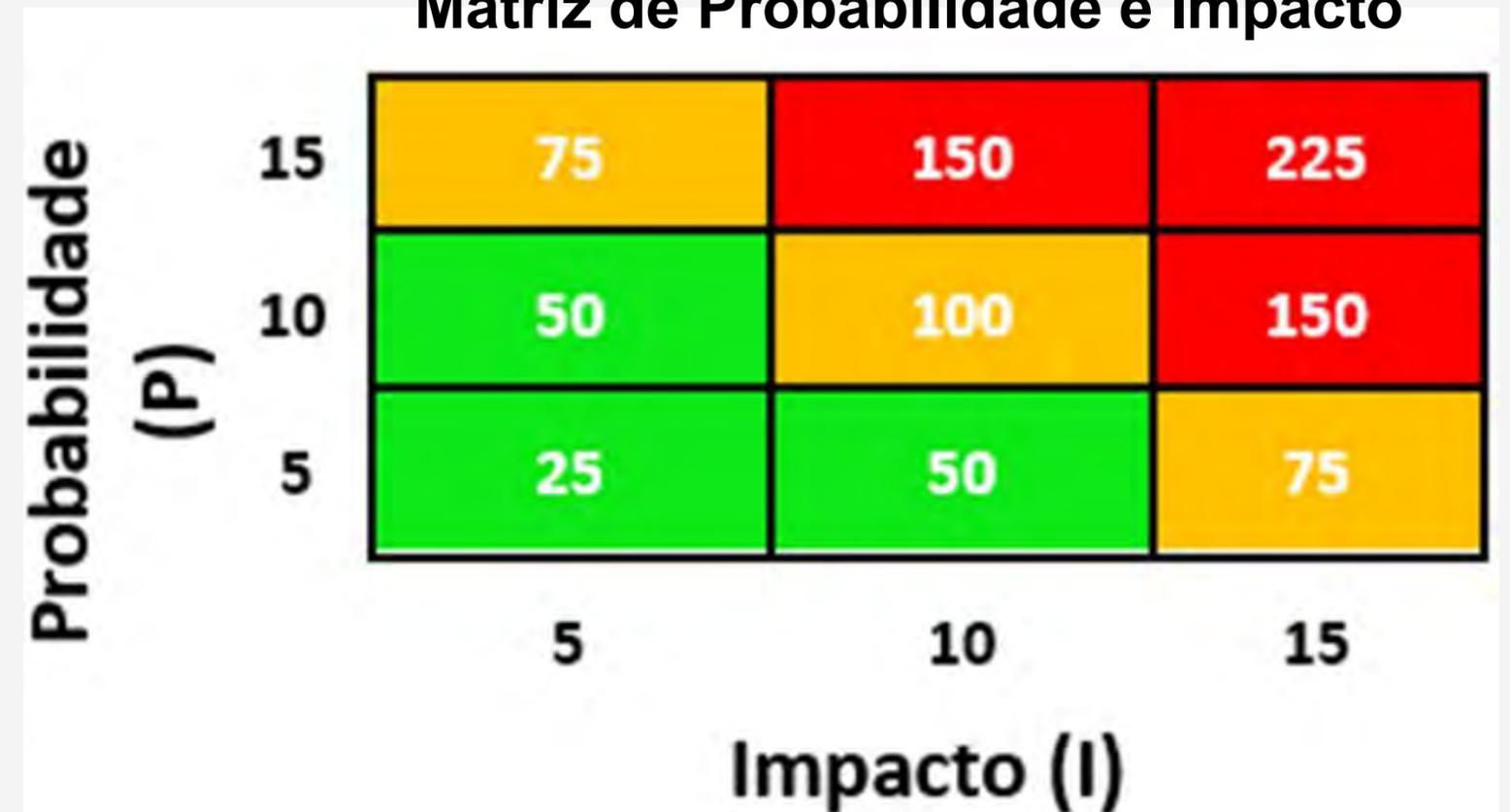


Avaliação de Riscos

Parâmetros escalares

CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

Matriz de Probabilidade e Impacto



Avaliação de Riscos de Segurança e Privacidade



Avaliação de Riscos

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P	I	NÍVEL DE RISCO (P X I)
R01	Acesso não autorizado.	10	15	150
R02	Modificação não autorizada.	10	15	150
R03	Perda	5	15	75
R04	Roubo	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
....
...
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

Riscos e nível de risco (diagnóstico inicial)

Legenda: P – Probabilidade; I – Impacto.

Avaliação de Riscos de Segurança e Privacidade

Avaliação de Riscos

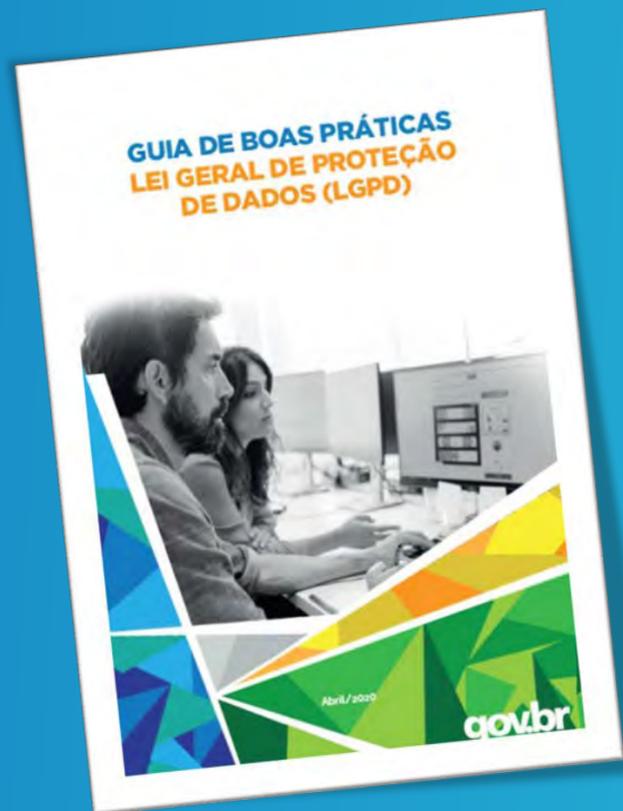
RISCO	MEDIDA(S)	EFEITO SOBRE RISCO	RISCO RESIDUAL			MEDIDA(S) APROVADA(S)
			P	I	(P X I)	
R01 Acesso não autorizado.	1. Controle de acesso Lógico.	Reduzir	5	10	50	Sim
	2. Desenvolvimento seguro.					
	3. Segurança em Redes.					

Exemplos de medidas aplicadas para reduzir o risco



Legenda: P – Probabilidade; I – Impacto.

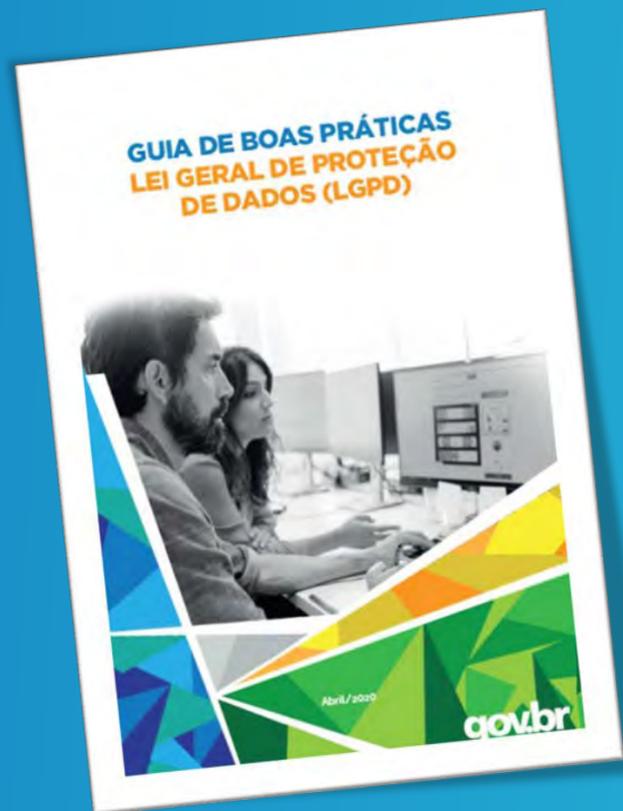
Avaliação de Riscos de Segurança e Privacidade



Contabilização da proporcionalidade entre riscos e benefícios **IT PARTNERS**

- Embora a LGPD não forneça orientação sobre como avaliar e atribuir peso aos vários riscos e danos no contexto dos requisitos da AIPD, ele prevê que qualquer avaliação deve levar em consideração a proporcionalidade entre risco/dano e os propósitos, interesses ou benefícios que estão sendo perseguidos.
- Assim, o mesmo risco pode ser pontuado de forma diferente quando comparado a um benefício baixo ou um benefício alto.

Avaliação de Riscos de Segurança e Privacidade



Contabilização da proporcionalidade entre riscos e benefícios **IT PARTNERS**

- Os benefícios devem ser considerados no início da avaliação de risco, pois estão relacionados à finalidade do processamento.
- Os benefícios e propósitos do processamento devem ser levados em consideração ao conceber mitigações para evitar a redução desnecessária dos benefícios ou o enfraquecimento dos propósitos.

Avaliação de Riscos de Segurança e Privacidade



Selecionando as mitigações

- As organizações devem considerar uma ampla gama de medidas de mitigação de risco, desde pseudonimização, minimização de dados e medidas de segurança, até vários mecanismos de governança ou supervisão de dados.
- As medidas de mitigação apropriadas dependem do contexto, levando em consideração os riscos envolvidos, o custo de implementação e a eficácia dessas medidas, seu impacto nos propósitos, a transparência e os elementos de um processamento justo.

Avaliação de Riscos de Segurança e Privacidade



Mitigação de Riscos, não eliminação

- A mitigação do risco não significa a eliminação do risco, mas a redução do risco na maior extensão razoável, dados os benefícios desejados e parâmetros econômicos e tecnológicos razoáveis.
- As organizações terão que tomar uma decisão fundamentada e comprovada sobre prosseguir com o processamento, levando em consideração a “proporcionalidade” em relação às finalidades e/ou benefícios.

QUAIS OS BENEFÍCIOS DA GESTÃO DE RISCOS?

1. Redução das surpresas operacionais e prejuízos.
2. Identificação de oportunidades de crescimento e melhorias.
3. Racionalização do capital estabelecendo uma ordem de prioridades de investimento.
4. Definição de objetivos.
5. Papéis e responsabilidades definidos
6. Integração entre Segurança e a Gestão



Conclusões

Se implementada com flexibilidade suficiente, a abordagem baseada em risco desempenhará um papel vital para garantir que a LGPD permaneça neutro em tecnologia e à prova de futuro e, portanto, capaz de fornecer proteção efetiva de dados de privacidade a indivíduos a longo prazo.

Conclusões

Em vez de criar regras e obrigações de tamanho único que em breve podem ficar desatualizadas, a abordagem baseada em risco fornece um processo com resultados que podem mudar com o contexto e se adaptar às mudanças nas tecnologias e práticas de negócios.



Conclusões

A abordagem baseada em risco será mais eficaz tanto do ponto de vista da proteção dos direitos fundamentais quanto do ponto de vista comercial, se houver um diálogo aberto e contínuo entre organizações, ANPD, leis e formuladores de políticas sobre as tecnologias e práticas de negócios em constante evolução, bem como as necessidades e expectativas dos indivíduos e da sociedade.

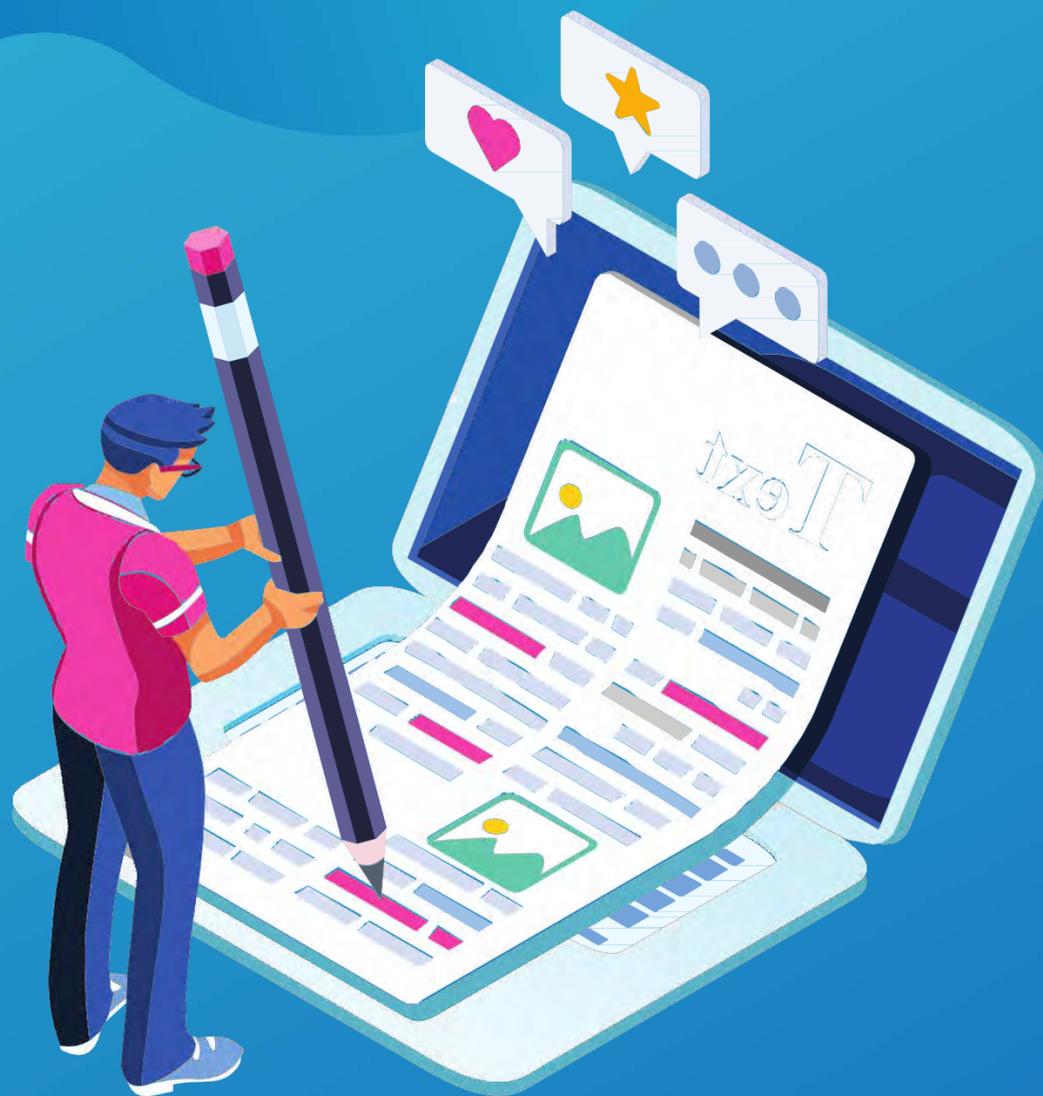
QUIZ !

Curso: Gestão de Riscos de Privacidade e Segurança da Informação - LGPD

De 16 a 20 de maio -das 18:30 as 22:30

Aprenda a:

- Realizar análise de riscos de SI
- Aplicar a metodologia
- Propor controles e
- Integrar a GRC com privacidade
- Voucher de 30% de desconto!



Obrigado!

Perguntas finais



Será enviada cópia da apresentação e vouchers no e-mail de agradecimento.