V Semana Estadual de Tecnologia da Informação e Comunicação - TIC

Segurança da Informação

Os impactos da Lei Geral de Proteção de Dados - LGPD na estratégia de segurança da informação

Prodest
Tecnologia da Informação

31 de Maio de 2019

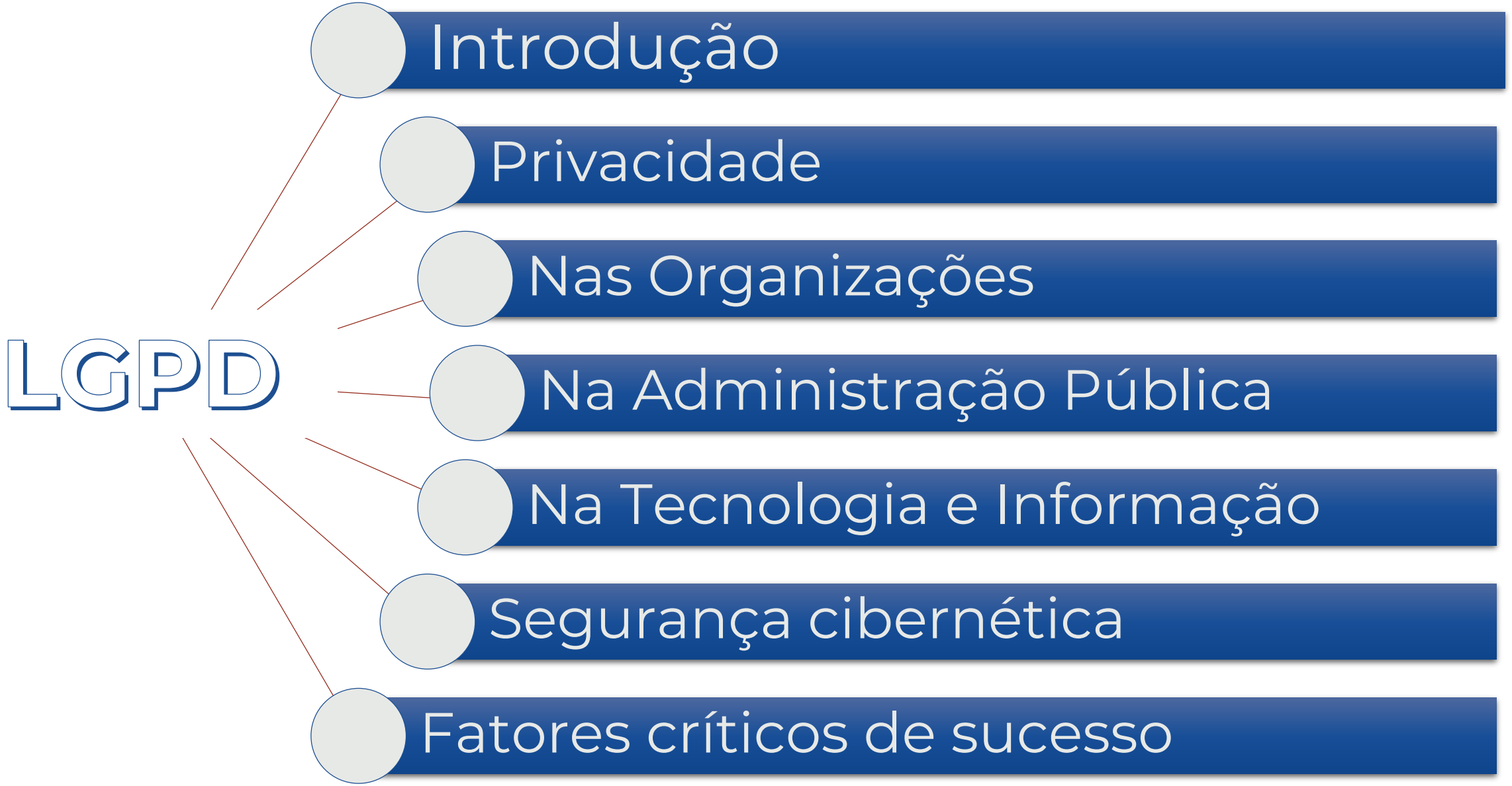
Privacidade e Segurança Cibernética na administração pública

DISCLAMER

Este documento apresenta o nosso entendimento sobre o tema. As informações apresentadas devem ser validadas antes da sua aplicabilidade.

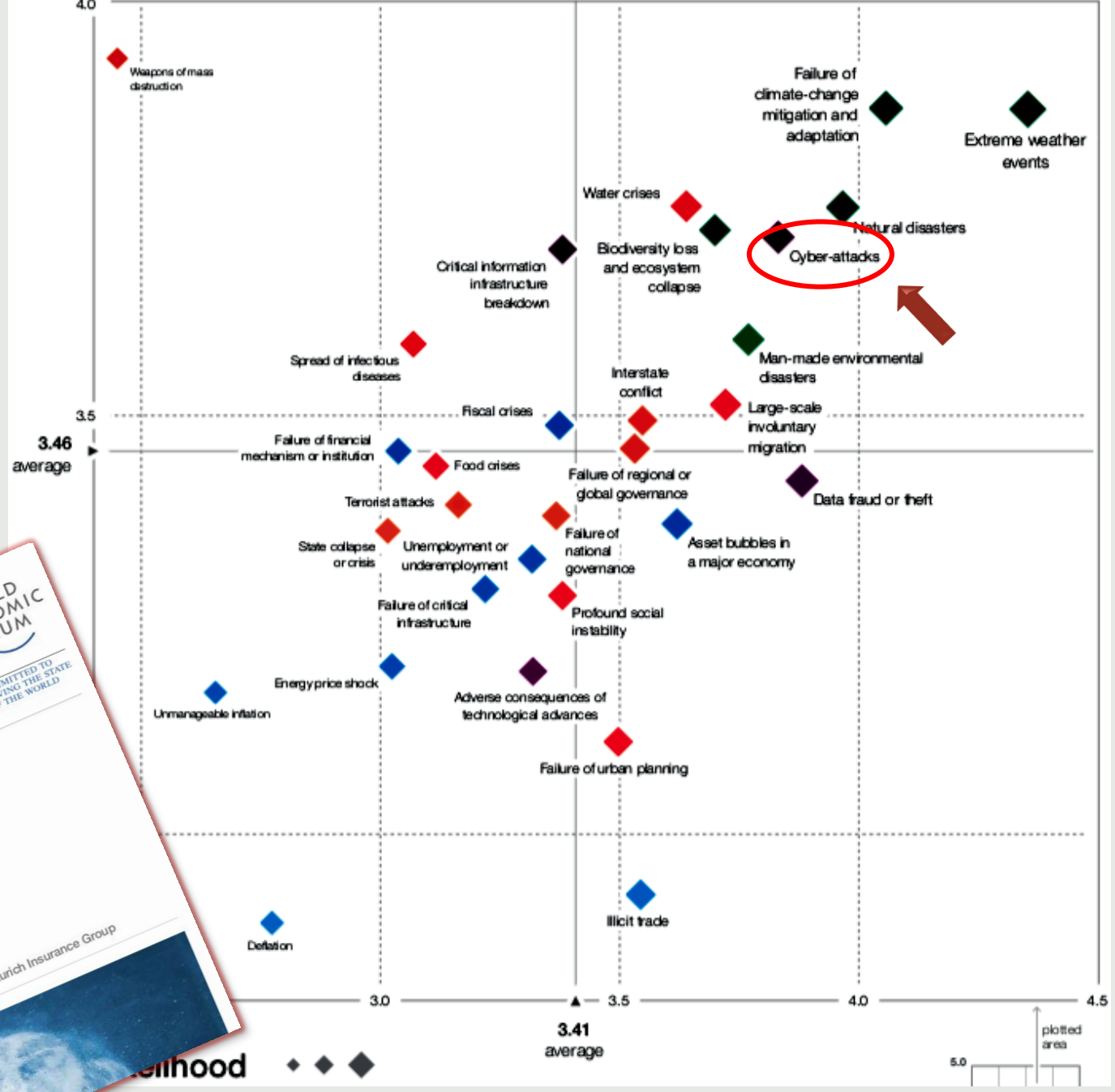
.A AÉRAS não se responsabiliza por perdas, danos ou gastos incorridos por qualquer pessoa decorrente de circulação, publicação, reprodução ou uso não autorizados deste documento.

A AÉRAS não assegura nem assegurará o sucesso da implementação das recomendações, nem assegura ou assegurará que tal se verifique em qualquer prazo, nem responderá por eventuais oportunidades que deixem de ser identificadas, apresentadas ou exploradas, independentemente dos motivos ou das razões para tais ocorrências.



GLOBAL RISK REPORT 2019

Conforme o The Global Risks Report 2019 do Fórum Econômico Mundial, os desastres naturais e os ataques cibernéticos representam os maiores perigos globais em 2019.



http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

AÉRAS

TIPOS DE DADOS PESSOAIS

Informações básicas:

- Crenças, pensamentos, fidelidade política, etc.
- Credenciais (autenticação)
- Preferências e interesses

Informações históricas:

- Experiências de vida individuais
- Eventos relevantes
- Padrões que permitam inferências

Informações financeiras:

- Contas, status financeiro
- Propriedades, estruturas
- Transações e padrões
- Histórico de crédito

Informações adicionais:

- Identificadores únicos Etnia
- Preferências sexuais
- Padrões de comportamento
- Idade, saúde, localização, etc.
- Saúde médica
- Dados físicos

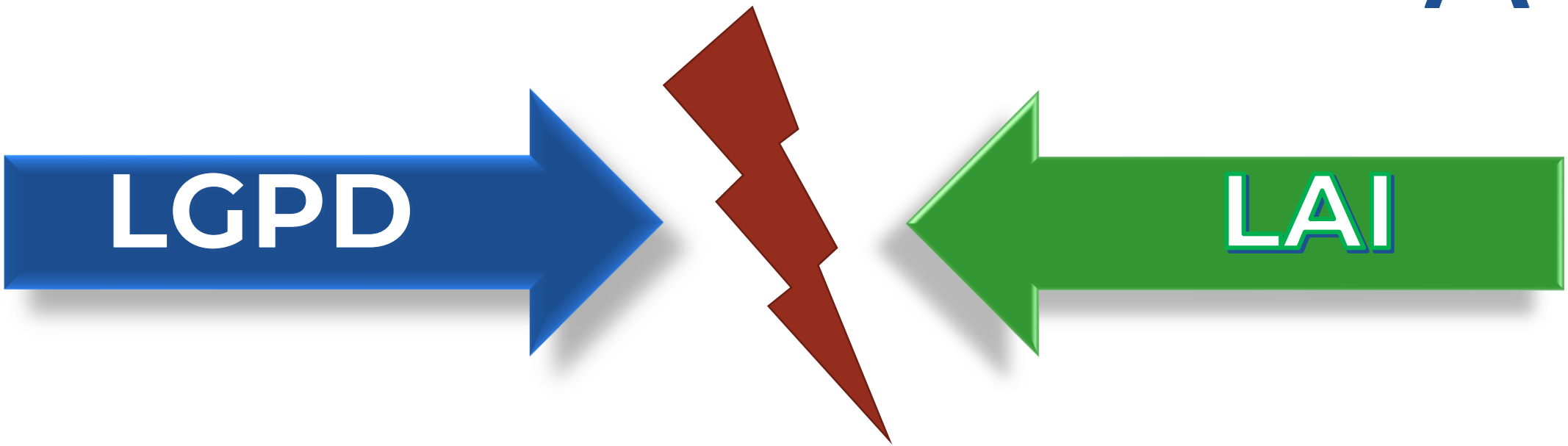
:Informações sociais

- Profissão, carreira
- Registros criminais
- Vida pública
- Família e relacionamentos
- Redes sociais
- Comunicações Privadas

Dados em tempo real

- Rastreamento dependente de dispositivo
- Informações de contato
- Base de localização
- Comportamento (ex: utilização de padrões)

@2018 – Tradução não oficial com base em: Implementing the General Data Protection Regulation – Figure 11—Types of Personal Data (Overview)



“É inegável que o caráter de complementariedade das atividades públicas dessas duas pessoas, autoridade de acesso à informação e encarregado, recomenda que sua interação seja próxima e recorrente, dando-se ampla publicidade às deliberações conjuntas, não somente ao controlador....”

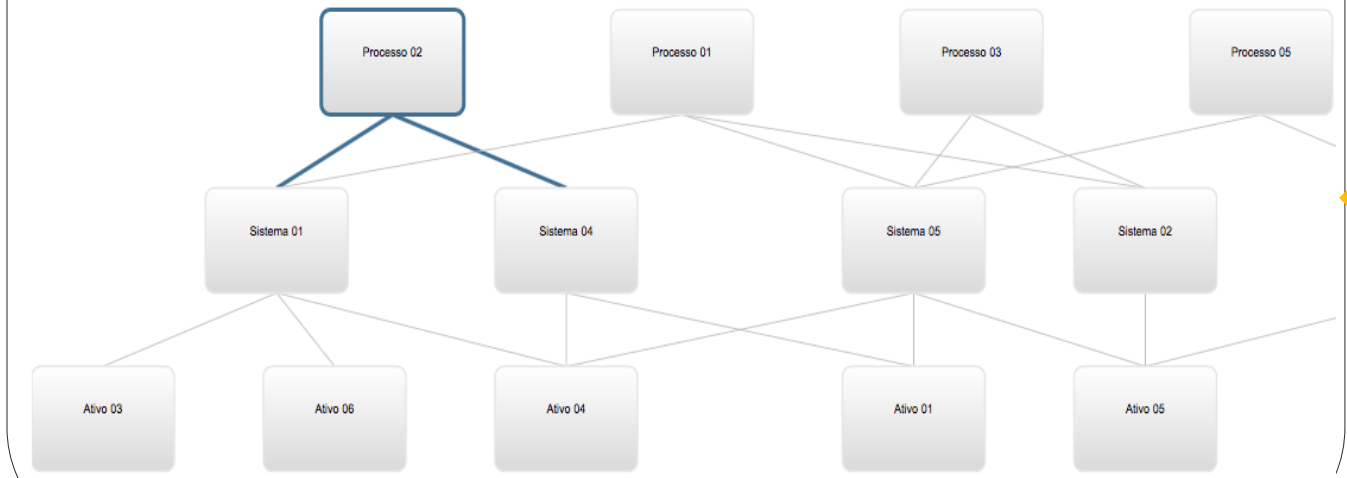
LGPD, Comentada, Thomson Reuters, pag 262 | Art. 23

Exigências legais Governo Federal, Estadual e Municipal

- Agências reguladoras
- MP
- CFM
- Marco Civil da Internet
- Código de defesa do consumidor
- LAI

ORGANIZAÇÃO PÚBLICA OU PRIVADA

OPERAÇÃO



CLIENTE, CONTRIBUINTE, PARTE INTERESSADA e etc.

PARCEIROS, PRESTADORES DE SERVIÇOS e etc.

Exigências legais Governo Federal, Estadual e Municipal

Agências reguladoras

MP

CFM

Marco Civil da Internet

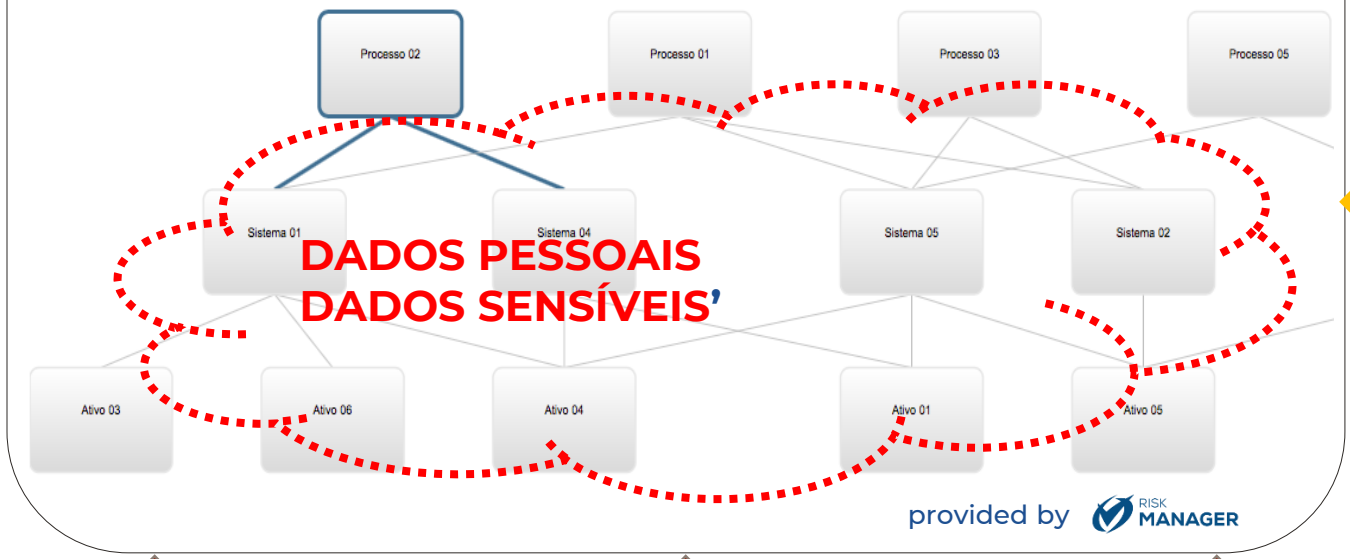
Código de defesa do consumidor

LAI

ANPD

ORGANIZAÇÃO PÚBLICA OU PRIVADA

OPERAÇÃO



PARCEIROS, PRESTADORES DE SERVIÇOS e etc.

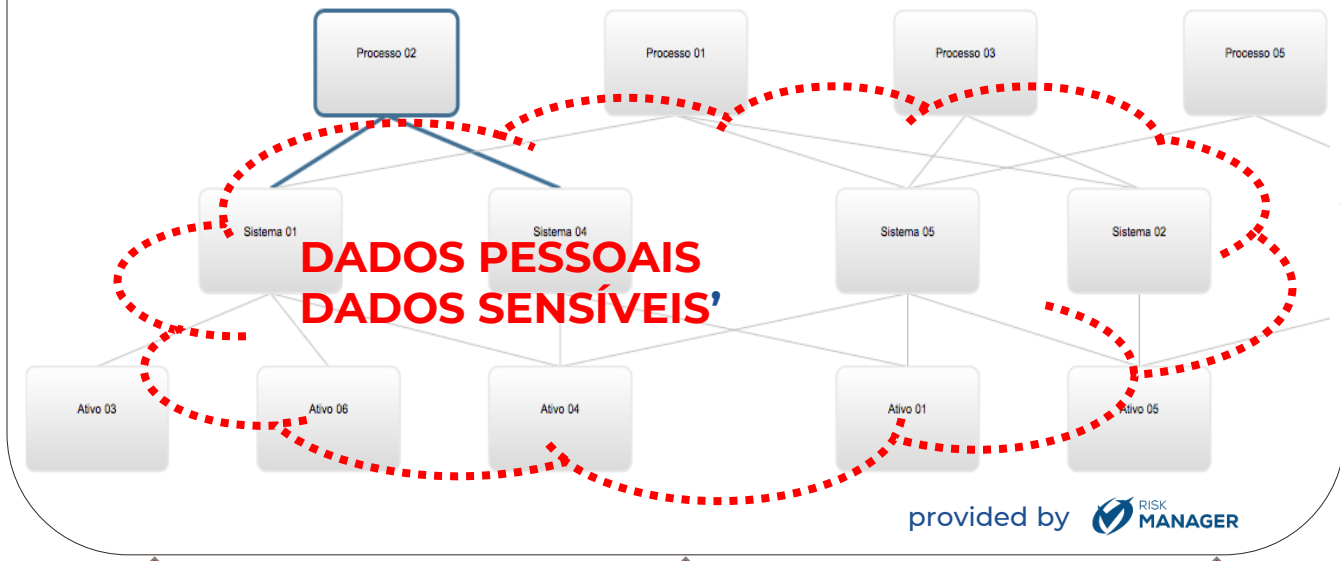
CLIENTE, CONTRIBUINTE, PARTE INTERESSADA e etc.

Exigências legais Governo Federal, Estadual e Municipal

- Agências reguladoras
- MP
- CFM
- Marco Civil da Internet
- Código de defesa do consumidor
- LAI
- **ANPD**

ORGANIZAÇÃO PÚBLICA OU PRIVADA

OPERAÇÃO



PARCEIROS, PRESTADORES DE SERVIÇOS e etc.

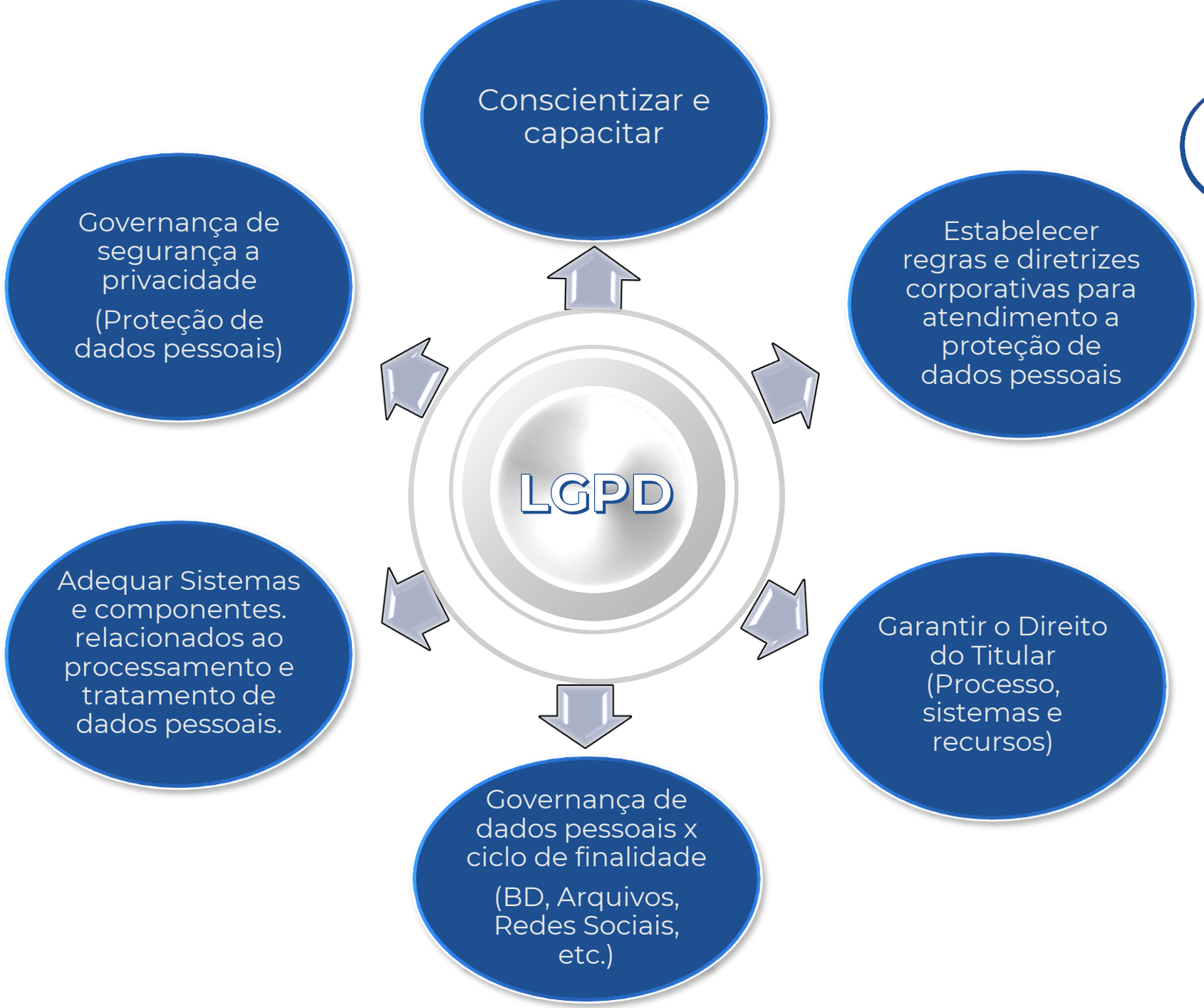
CLIENTE, CONTRIBUINTE, PARTE INTERESSADA e etc.

DIREITO A PRIVACIDADE

PROTEÇÃO DE DADOS PESSOAIS

LGPD

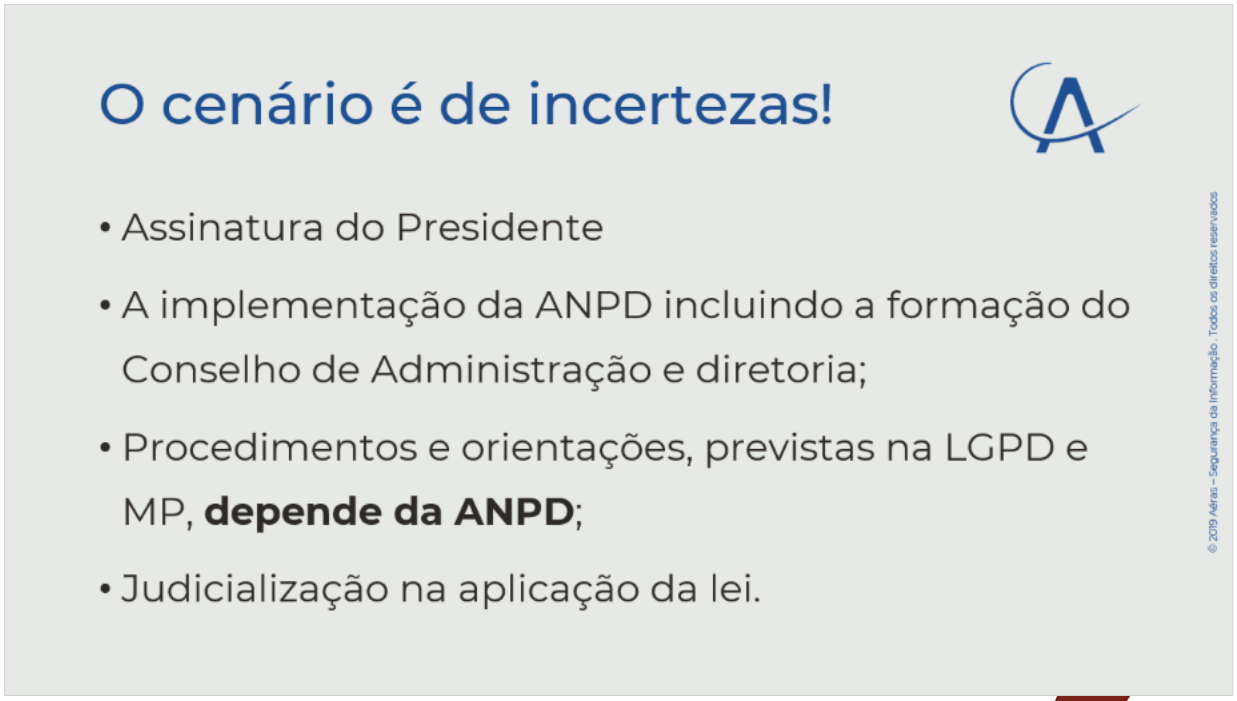
- DISPOSIÇÕES PRELIMINARES
- DIREITOS DO TITULAR E TRATAMENTO DE DADOS PESSOAIS
- SEGURANÇA E BOAS PRÁTICAS
- AGENTES DE TRATAMENTO DE DADOS PESSOAIS



O cenário é de incertezas!

- Assinatura do Presidente
- A implementação da ANPD incluindo a formação do Conselho de Administração e diretoria;
- Procedimentos e orientações, previstas na LGPD e MP, **depende da ANPD**;
- Judicialização na aplicação da lei.

O cenário é de incertezas!

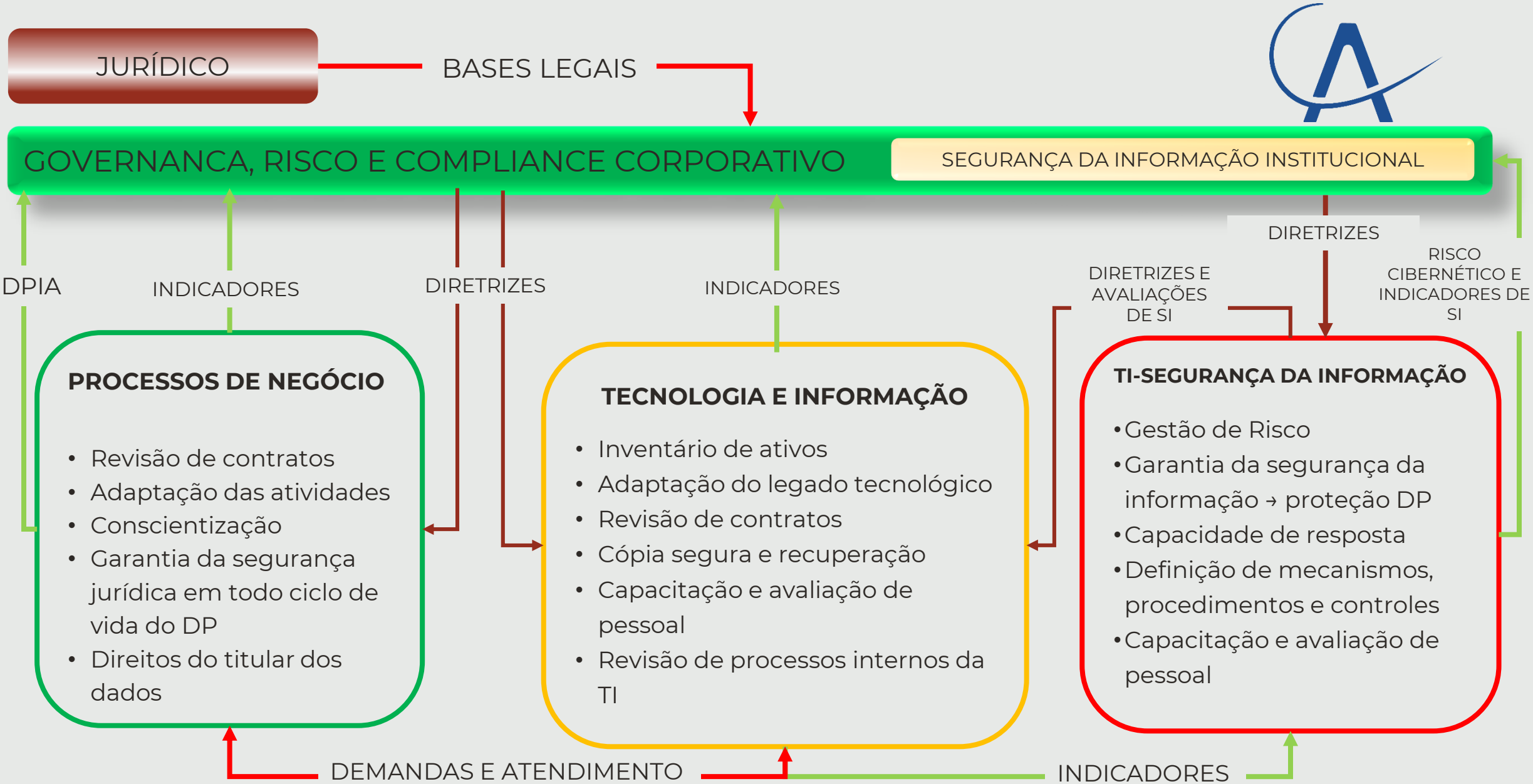


A incapacidade de operacionalizar e fiscalizar da ANPD pode justificar o não fazer nada até que esteja tudo bem definido.

O cenário é de certezas!

- MP´s 869/2018 e 870/2019 foram aprovadas nas duas casas. **Acredita-se** que o Presidente irá sancionar, **sem vetos**.
- A implementação da ANPD será facilitada, nos **dois primeiros anos**, por convocação de funcionários públicos de outros órgãos pelo Presidente da Republica para compor os quadros da ANPD;
- No primeiro momento **deve ocorrer uma força tarefa** para publicar os Procedimentos e orientações, previstas na LGPD e MP;
- A **fiscalização por outros órgãos** (MP) pode influenciar, cada vez mais, a **redução** do não fazer nada;
- Judicialização na aplicação da lei.

ORGANIZAÇÃO – Âmbito da LGPD



METAS E OBJETIVOS

FASES

provided by RISK MANAGER

ESCOPO¹

¹Lei N° 13.709, 14 agostos 2018 de proteção de dados pessoais
²Autoridade Nacional de Proteção de Dados

DIRETRIZES GERAIS

- Utilizar as melhores práticas e frameworks;
- Promover ações para garantir a evolução da maturidade da governança e gestão de segurança da informação;
- Obter uma visão integrada dos negócios (produtos e serviços) com os ativos cibernéticos;
- Considerar e Garantir a Segurança da Informação e Segurança cibernética na evolução dos produtos e serviços;
- Ações e investimento com base em riscos de proteção a privacidade, segurança da informação e riscos cibernéticos.

PREREQUISITOS ADEQUAÇÃO À LEI Nº 13.709, 14 AGOSTOS 2018 DE PROTEÇÃO DE DADOS PESSOAIS

- **Definir e Publicar** as **Diretrizes Corporativas para adequação à LGPD**, fornecidas pela Governança Corporativa com suporte jurídico;
- **Identificar e gerenciar os Riscos** inerentes do negócio no escopo da LGPD;
- **Inventariar** os processos, sistemas e ativos de informação (tecnológicos ou não);
- **Inventariar** fontes de dados com DP/DS;
- **Construir e manter o fluxo dos processos/atividades/procedimentos** que utilizam no ciclo DP/DS;
- **Conhecer** as tecnologias utilizadas;
- **Gerenciar** eficientemente a relação de **parceiros** e **prestadores de serviços** e os respectivos contratos;
- **Identificar e relacionar as Tecnologias e soluções de Segurança** da Informação com a proteção de DP/DS
- Possuir **Serviços gerenciados** de Segurança da Informação;

VISÃO GERAL DE PROJETO GENÉRICO

DIRETRIZES GERAIS

- Utilizar as melhores práticas e frameworks;
- Promover ações para garantir a evolução da maturidade da governança e gestão de segurança da informação;
- Obter uma visão integrada dos negócios (produtos e serviços) com os ativos cibernéticos;
- Considerar e Garantir a Segurança da Informação e Segurança cibernética na evolução dos produtos e serviços;
- Ações e investimento com base em riscos de proteção a privacidade, segurança da informação e riscos cibernéticos.

PREREQUISITOS ADEQUAÇÃO À LEI Nº 13.709, 14 AGOSTOS 2018 DE PROTEÇÃO DE DADOS PESSOAIS

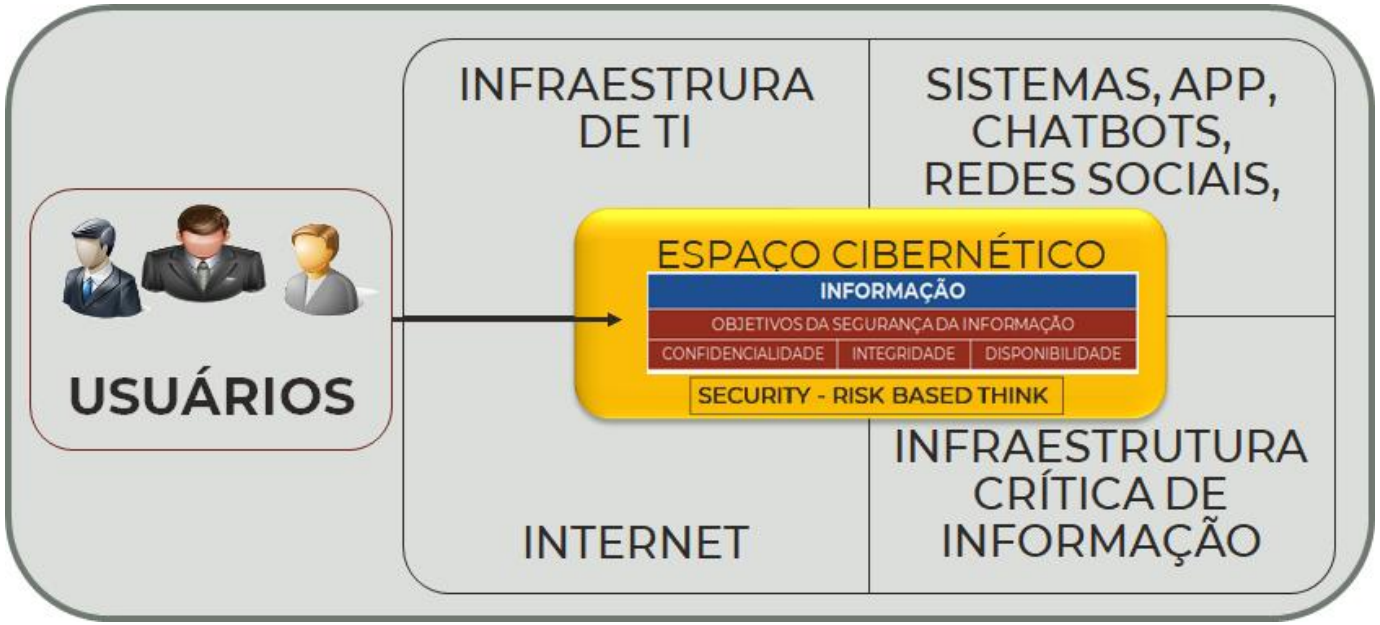
- **Definir e Publicar** as **Diretrizes Corporativas para adequação à LGPD**, fornecidas pela Governança Corporativa com suporte jurídico;
- **Identificar e gerenciar os Riscos** inerentes do negócio no escopo da LGPD;
- **Inventariar** os processos, sistemas e ativos de informação (tecnológicos ou não);
- **Inventariar** fontes de dados com DP/DS;
- **Construir e manter o fluxo dos processos/atividades/procedimentos** que utilizam no ciclo DP/DS;
- **Conhecer** as tecnologias utilizadas;
- **Gerenciar** eficientemente a relação de **parceiros** e **prestadores de serviços** e os respectivos contratos;
- **Identificar e relacionar as Tecnologias e soluções de Segurança** da Informação com a proteção de DP/DS
- Possuir **Serviços gerenciados** de Segurança da Informação;

Estabelecer o Programa para adequação a LGPD

Plano de ação para demais áreas da Organização

Plano de ação para a TI e Segurança da Informação

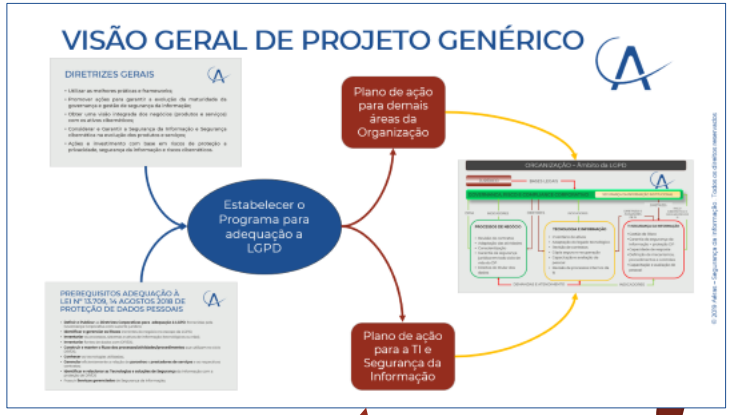
DIAGNÓSTICO & GAPs
Riscos identificados

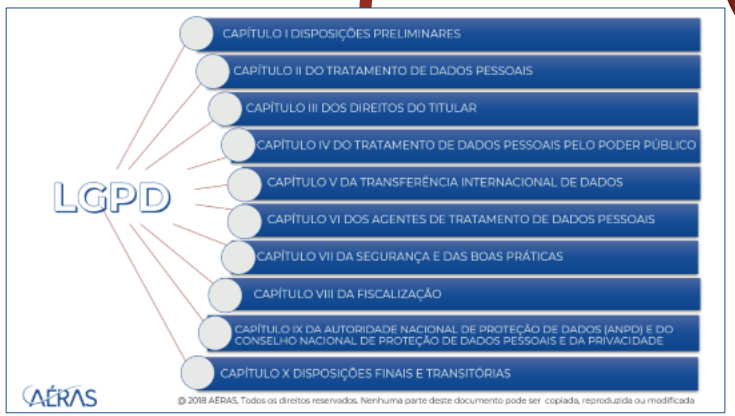


+

DADOS PESSOAIS EM MEIO NÃO DIGITAL

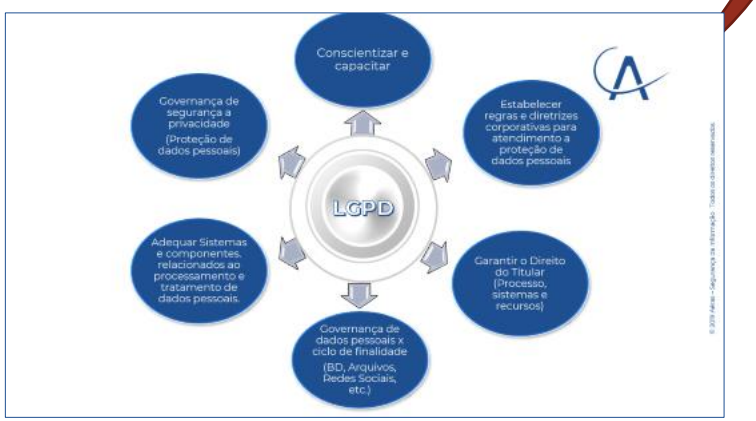
ESPAÇO CIBERNÉTICO : Adaptada a partir da Relação entre a Segurança Cibernética e outros domínios de segurança descrita na norma ISO/IEC 27032:2015 - Tecnologia da Informação Técnicas de segurança - Diretrizes para segurança cibernética Esta Norma fornece diretrizes para melhorar o estado de Segurança Cibernética, traçando os aspectos típicos desta atividade e suas ramificações em outros domínios de segurança.





PROGRAMA DE ADEQUAÇÃO À LGPD

Priorizar baseado em risco (menor investimento para atender os maiores impactos)



Ações de longo prazo

RISCOS

- **Implantação** de soluções sem considerar o risco do negócio relacionado a LGPD
- Não Integração da Governança e gestão da segurança da informação ⬅➡ Governança corporativa. (diretrizes x indicadores)
- Orçamento X Carona ➔ $$$$;
- Ações da TI **sem o alinhamento** com a avaliação do **negócio**;
- **Ausência** de diretrizes formais do negócio para o atendimento à LGPD;

Fatores críticos de sucesso

- ✓ Tempo para elaborar o diagnóstico do negócio;
- ✓ Efetividade do comitê de risco/segurança;
- ✓ Envolvimento de agentes terceirizados;
- ✓ Definição encarregado - DPO;
- ✓ Diretrizes corporativas relacionadas a LGPD para a TI;
- ✓ Comprometimento da Alta direção.

Considerações finais

- Delinear as formas de limitar quantidades e tipos de dados coletados e mantidos - MINIMIZAÇÃO;
- Definir métodos para monitorar mudanças nas leis, regulamentos e práticas de privacidade - CONFORMIDADE;
- Determinar maneiras de limitar o uso que reduzem riscos a uma violação de dados – PRESTAÇÃO DE CONTA;
- Avalie a capacidade das tecnologias para gerenciar e proteger dados – SEGURANÇA E BOAS PRÁTICAS.

ARMADILHAS POTENCIAIS

- Assumir que o **uso pretendido** e o **uso real** são os mesmos;
- Coletar ou manter **mais do que você precisa**;
- **Negligenciar** os Direitos do Titular;
- Não **categorizar** as informações sensíveis;
- Controle ineficaz na transferência de **informações pessoais protegidas (PPI**);
- Ignorar questões relacionadas as diferenças fronteiriças;
- Falta de controle do ciclo de vida do DP (onde, quem usa, como uso, etc);
- Eliminar **PPI** sem destruição completa dos dados do titular;
- Dificuldade de respostas em **tempo hábil às mudanças** dos princípios estabelecidos pela lei;
- Gerenciando **manualmente** do ciclo de vida da informação **complexa**;
- Controle pessoal de terceiros que manipulam ou processam informações do cliente.

A IMPORTÂNCIA DA INTEGRAÇÃO

- *"A gestão de riscos é parte integrante de todas as atividades organizacionais."*

- *"A integração permite que a organização tome decisões que são mais adequadas com a rapidez e potencial interrupção de riscos isolados e com a busca de novas oportunidades."*

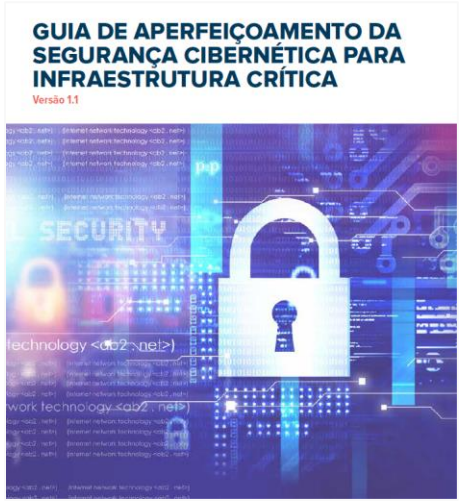
CIS Center for Internet Security®

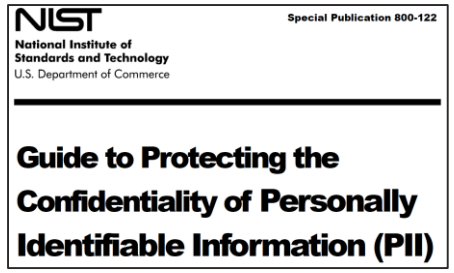
ABNT ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

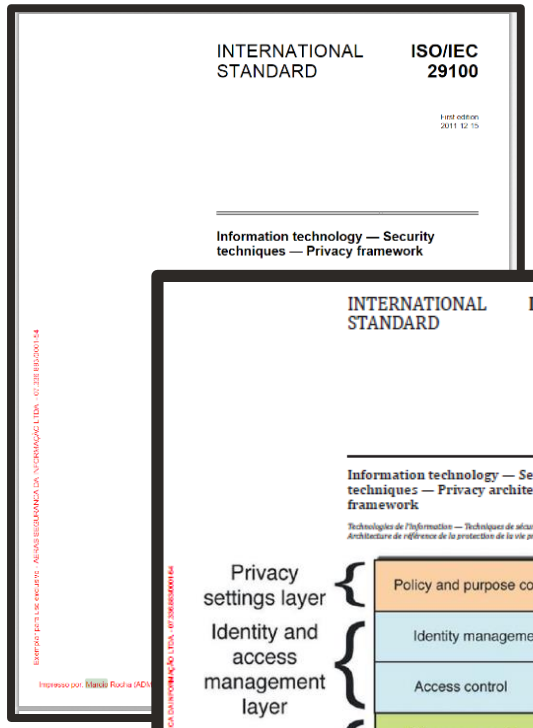
NIST National Institute of Standards and Technology U.S. Department of Commerce

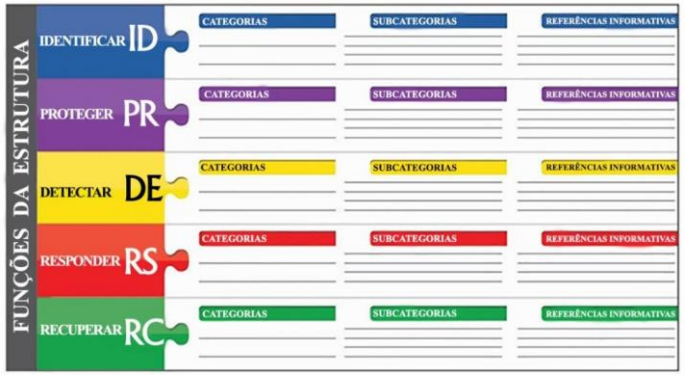
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

COBIT 2019









Components	Consent and choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness transparency and notice	Individual participation and access	Accountbility	nformation security controls	Compliance
Policy and purpose comunication	X	X	X	X			X				X
PII categoraization			X	X	X						
Consent management	X	X	X					X			
Privacy preference management	X	X	X		X		X				

IPD2R

DADOS PESSOAIS

(Onde?, Quem usa?, Como usa?, etc.)

AÉRAS

SEGURANÇA DA INFORMAÇÃO

Obrigado!

MÁRCIO ANTONIO DA ROCHA
marcio@aeras.com.br
mrocha@modulo.com.br
31 984474070

Rua Paraíba 550 - 9°. Andar – Funcionários - Belo Horizonte – MG – 30.130 141
www.aeras.com.br