

every
CYBERSECURITY GRC PRIVACY

UN GLOBAL COMPACT

CERTIFICADA ISO 27001 SEGURANÇA DA INFORMAÇÃO

CERTIFICADA ISO 27701 PRIVACIDADE DA INFORMAÇÃO

WORKSHOP DE CONSCIENTIZAÇÃO DE PRIVACIDADE DE DADOS

PRODEST- Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo

CONTRATO Nº ° 2024.000027.28203.01

1. Apresentar ao PRODEST noções e conceitos basilares sobre Proteção de Dados

2. Garantir a base de conhecimento necessária para melhoria de processos, visando a conformidade da Organização.

3. Promover uma cultura organizacional de proteção de dados

4. Garantir que o PRODEST esteja em conformidade com a LGPD e demais regulações sobre proteção de dados.

OBJETIVOS DO WORKSHOP

PAUTA

- Introdução: Conceitos Básicos sobre a LGPD
- Linha do Tempo – Marcos Relevantes
- Cenário Antes da LGPD
- Dados Pessoais vs. Dados Sensíveis
- Sigilo, Confidencial e Sensível
- Controlador vs. Operador
- Base Legal na Administração Pública
- Transparência vs. LGPD
- Sanções e Fiscalização



Privacidade

Preservação da vida íntima e privada, assim como seu lar e sua família.

Proteção de Dados Pessoais

Controle, poderes e exercício de limites sobre as informações que lhe dizem respeito.

Segurança da Informação

Conjunto de Práticas para proteção de sistemas e informações, incluindo os dados pessoais.



LINHA DO TEMPO – MARCOS RELEVANTES

SETEMBRO/2018

Publicação da LGPD

Foi publicada a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), que dispõe sobre a proteção de dados pessoais.

JULHO/2019

Criação da ANPD

Foi publicada a Lei 13.853/2019 que criou a Autoridade Nacional de Proteção de Dados.

JULHO/2021

Publicação da Política de Proteção de Dados Pessoais e da Privacidade do ES

(Decreto 4922-R)

AGOSTO/2021

Sanções Administrativas

Entrada em vigor da possibilidade de aplicação de sanções administrativas pela ANPD.

OUTUBRO/2021

Designação dos Membros para compor o Comitê Encarregado Central - CEC

Portaria nº 059-S

Nomeação do Encarregado Interno do PRODEST

Instrução De Serviço Nº 076 P.
Sr. Rodrigo Faustini

AGOSTO/2024

Contratação de Consultoria para apoio na adequação à LGPD

Every Cybersecurity, GRC and Privacy Solution



Código de Defesa do Consumidor (CDC) - Lei nº 8.078/1990



Lei do Habeas Data - Lei nº 9.507/1997



Lei de Acesso à Informação (LAI) Lei nº 12.527/2011



Marco Civil da Internet - Lei nº 12.965/2014

Lei Geral de Proteção de Dados Pessoais
Lei nº 13.709/2018

CENÁRIO ANTES DA LGPD



Dados Pessoais:

Informação relacionada a pessoa natural identificada ou identificável. Exemplos: nome, CPF, conta bancária, endereço, telefone, estado civil etc.



Dados Pessoais Sensíveis:

Dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.



Sigiloso

Informações cuja a divulgação pode comprometer a segurança do Estado ou de pessoas.



Confidencial

Informações cujo acesso deve ser restrito por questões de interesse institucional, comercial ou de relacionamento.



DADOS PESSOAIS VS DADOS SENSÍVEIS

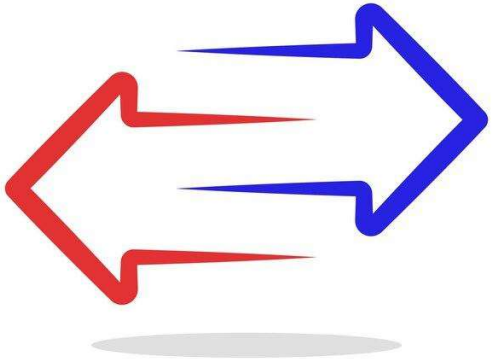
every CYBERSECURITY GRC PRIVACY

	SIGILOSO	CONFIDENCIAL	SENSÍVEL
Definição	Informações protegidas por interesse do Estado, acesso restrito por prazo legal.	Informações com valor estratégico/comercial, protegidas por contrato ou política.	**Dados pessoais que revelam origem racial, opinião política, religião.**
Base legal	Lei nº 12.527/2011 (LAI), Código Penal, Código Militar Lei Estadual nº 9.871/2012 (art. 4º, inciso III).	Normas institucionais, cláusulas contratuais.	**LGPD – art. 5º, inciso II e art. 11.**
Princípio básico	Garantir que a informação seja mantida em segredo e só seja divulgada com autorização.	As informações serão "tratadas" apenas por pessoas para as quais o acesso foi concedido.	**Por risco de preconceito ou discriminação, esses dados exigem proteção especial.**
Exemplo	Infraestrutura de rede crítica, senhas, investigações policiais. Declarações fiscais, informações bancárias.	Código-fonte de sistemas, configurações técnicas exclusivas. Cláusulas de confidencialidade em contratos	**Dados biométricos, acesso ao sistema via reconhecimento facial.**



CONTROLADOR

Pessoa natural ou jurídica, de direito público ou privado, que toma as principais decisões sobre como o dado pessoal será tratado.





OPERADOR

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

CONTROLADOR VS OPERADOR

ARMAZENAMENTO SOB DEMANDA (COLOCATION)

SOLICITAÇÃO DO ÓRGÃO

Órgão requisitante solicita por chamado a criação de ambiente para armazenamento.



PRODEST RECEBE

PRODEST recebe a solicitação e estrutura o espaço em seus servidores



ATUAÇÃO DO PRODEST?

Operador técnico (infraestrutura)



HÁ TRATAMENTO?

O PRODEST não acessa, nem processa os dados.

Apenas Armazena



Há responsabilidade perante a LGPD?



EXEMPLOS PRÁTICOS DO PRODEST

CRIAÇÃO DE SISTEMA E ARMAZENAMENTO PARA OUTRO ÓRGÃO

SOLICITAÇÃO DO ÓRGÃO

Órgão solicita criação e manutenção de sistema



1º - ATUAÇÃO DO PRODEST

GESIT desenvolve, implanta, atualiza e gerencia o sistema.



2º - ATUAÇÃO DO PRODEST

Dados são hospedados no banco de dados do PRODEST



HÁ TRATAMENTO?

PRODEST (via GESIT) tem acesso e faz a gestão técnica, **mas não define a finalidade dos dados**.





EXEMPLOS PRÁTICOS DO PRODEST

ACESSO CIDADÃO

ATIVIDADE	1ªL ATUAÇÃO	2ª ATUAÇÃO	AGENTES ENVOLVIDOS
Desenvolvido e mantido pelo PRODEST.	PRODEST gerencia tecnicamente e armazena os dados	PRODEST define finalidades e critérios de acesso.	PRODEST











EXEMPLOS PRÁTICOS DO PRODEST

SISTEMA DE CONTROLE DE ACESSO (EMPRESA TERCEIRIZADA)

DEMANDA

Contratação de empresa privada que fornece sistema, catracas, leitores biométricos.



GERENCIAMENTO DOS DADOS

Dados são armazenados em servidor do PRODEST, porém gerenciados pela empresa terceirizada.



ATUAÇÃO DO PRODEST

PRODEST dá as diretrizes, define a finalidade de uso.



ATUAÇÃO DA TERCEIRIZADA

Empresa contratada atua sob ordem do PRODEST.





EXEMPLOS PRÁTICOS DO PRODEST



Controlador e operador NÃO representam posições teóricas, mas RESPONSABILIDADES.

A definição desses papeis auxiliará o PRODEST numa atuação segura e eficiente.

ENCERRAMENTO DO TÓPICO

BASES LEGAIS

- Mediante consentimento de titular
- Para cumprimento de obrigação legal
- Para execução de políticas públicas
- Para realização de estudos por órgão de pesquisa
- Para a execução de contrato
- Para exercício regular de direitos (Investigação judicial)
- Para proteção da vida
- Para tutela de saúde
- Para atender aos interesses legítimos do controlador ou de terceiros
- Para a proteção do crédito

FINALIDADE	BASE LEGAL
Publicação de informações sobre remuneração de servidores públicos	Cumprimento de obrigação legal ou regulatória (Art. 7º, II)
Utilização de dados biométricos para acesso ao GOV.BR	Prevenção à fraudes (Art. 11, II, g)
Coleta de dados pessoais sensíveis para comunicação de ocorrência	Cumprimento de obrigação legal ou regulatória (Art. 11, II, a)
Inscrição em evento de formação, como palestras	Consentimento (art. 7º, I)

TRANSPARÊNCIA x PRIVACIDADE



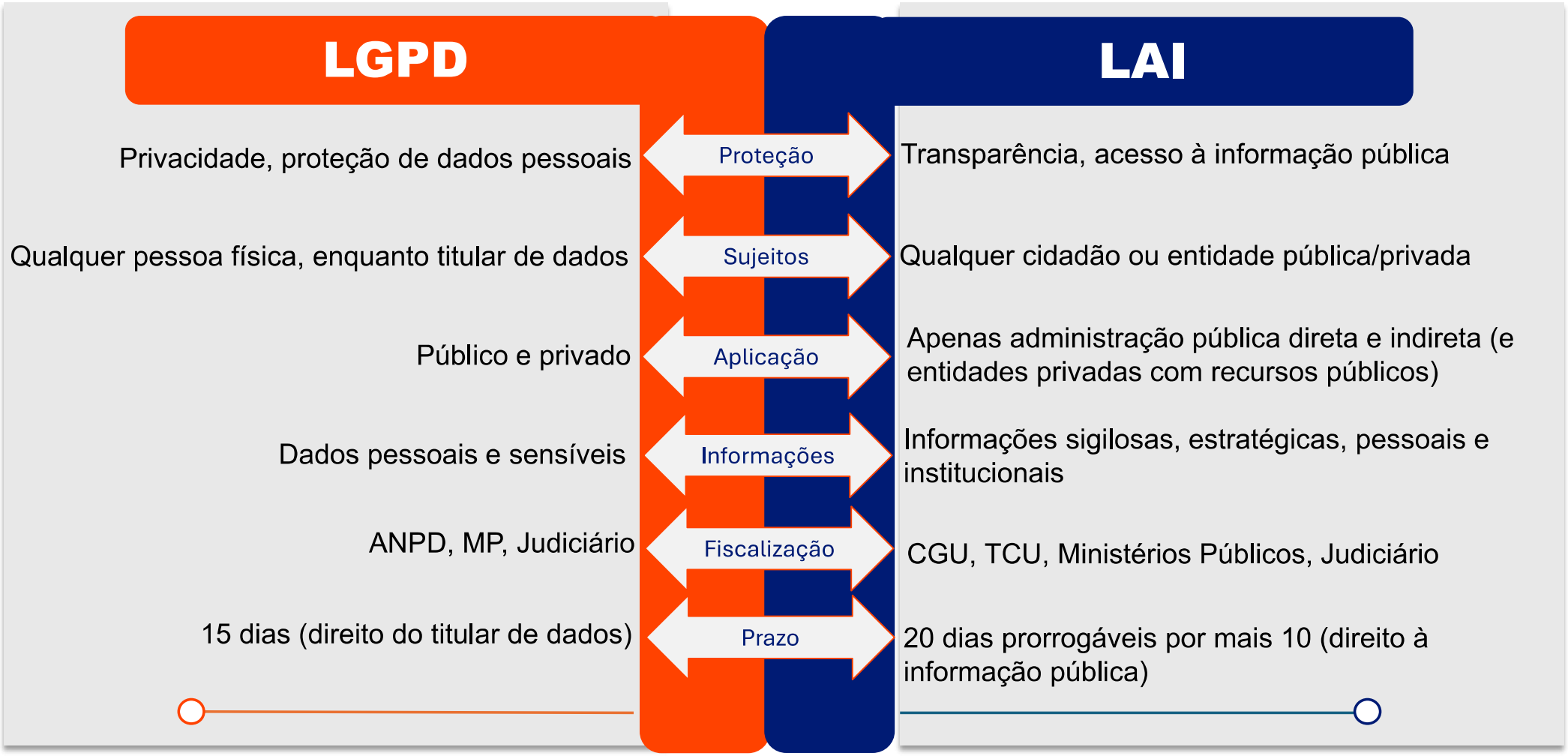
Complementariedade e harmonia entre as legislações.

LGPD (Lei nº 13.709/2018)
Proteção de dados pessoais;
Regula o tratamento de dados pessoais seguro e responsável.

LAI (Lei nº 12.527/2011)
Acesso à informação pública;
Garante a transparência da atuação do Estado.

CONVERGÊNCIAS E DIFERENÇAS

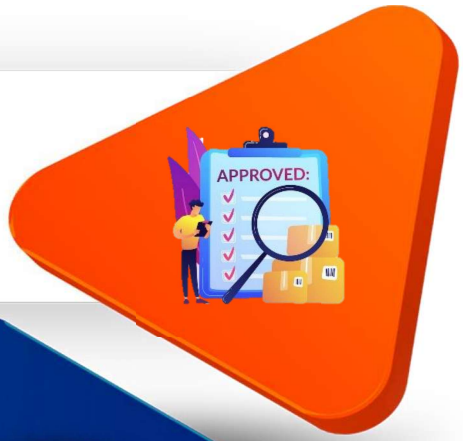
CRITÉRIO	LAI (Lei nº 12.527/2011)	LGPD (Lei nº 13.709/2018)
Abrangência	Direito público; Incide sobre todos os entes públicos.	Direito público e privado; Incide sobre os entes públicos e privados.
Tipo de Acesso	Coletivo; Qualquer cidadão pode solicitar informações de interesse público.	Individual; Solicitação restrita aos titulares de dados pessoais.
Controle de Acesso	O ente público pode indeferir na ausência de interesse público. Cabe recurso.	O titular tem direito ao acesso; Indeferimento pode ser questionado na ANPD ou judicialmente.
Tratamento de Dados	Foco na disponibilização de informações públicas; menos ênfase em segurança de dados.	Enfatiza a proteção de dados pessoais, com requisitos de segurança e privacidade.
Sanções	Prevê sanções administrativas e disciplinares para servidores públicos.	Prevê sanções administrativas expressas para as hipóteses de violação.


LGPD
LAI
Privacidade, proteção de dados pessoais
Proteção
Transparência, acesso à informação pública
Qualquer pessoa física, enquanto titular de dados
Sujeitos
Qualquer cidadão ou entidade pública/privada
Público e privado
Aplicação
Apenas administração pública direta e indireta (e entidades privadas com recursos públicos)
Dados pessoais e sensíveis
Informações
Informações sigilosas, estratégicas, pessoais e institucionais
ANPD, MP, Judiciário
Fiscalização
CGU, TCU, Ministérios Públicos, Judiciário
15 dias (direito do titular de dados)
Prazo
20 dias prorrogáveis por mais 10 (direito à informação pública)

Dica para Gestores

“A LAI e a LGPD não são leis concorrentes e devem ser harmonizadas de acordo com o caso concreto. Uma protege o coletivo pelo acesso à informação; a outra protege o indivíduo pela privacidade.

Avaliação do Pedido:
Analisar se a solicitação é de interesse público (LAI) ou pessoal (LGPD).



Transparência e Privacidade:
Buscar a harmonia entre a divulgação de informações públicas e a proteção de dados pessoais, de acordo com o caso concreto.



Proteção de Dados Pessoais:
A aplicação da LAI não impede a proteção de dados pessoais sensíveis.





Advertência

Advertência com indicações de prazos para adoção de medidas corretivas



Publicização

Publicização da infração nos canais oficiais ou de grande circulação



Bloqueio

Bloqueio dos dados pessoais referentes à infração



Eliminação

Eliminação dos dados pessoais referentes à infração



Suspensão

Suspensão do funcionamento do banco de dados ou da atividade de tratamento



Proibição

Proibição do exercício da atividade relacionada ao tratamento de dados

LGPD: SANÇÕES

DECISÕES JUDICIAIS SOBRE PROTEÇÃO DE DADOS PESSOAIS



A entrega dos dados à administração não implica dizer que eles deverão ser expostos ao público em geral, cabendo àquela, já com as informações em mãos, adotar as cautelas necessárias para dar concretude ao artigo 5º, inciso LXXIX, da Constituição, e à LGPD, ou seja, tais normas não proíbem a coleta dos dados, mas asseguram que os entes político-administrativos deverão respeitar o tratamento nelas conferido.

RMS 55.819

Ministro Gurgel de Faria



A LGPD não exclui a possibilidade da quebra de sigilo. Ao contrário, apresenta regras sobre tal ocorrência, que, no caso, revela-se possível, considerando as espécies de dados, a finalidade da quebra e o contexto em que apresentados.

REsp 1.914.596

Ministro Luis Felipe Salomão



O tratamento indevido de dados pessoais bancários configura defeito na prestação de serviço, notadamente quando tais informações são utilizadas por estelionatário para facilitar a aplicação de golpe em desfavor do consumidor.

REsp 2.077.278

Ministra Nancy Andrighi

- RMS 55819
- REsp 2135783
- AREsp 2130619
- REsp 1914596
- REsp 1914596
- REsp 2077278
- REsp 2092096

Levantamento aponta que LGPD é citada em mais de 14 mil decisões judiciais

Deste total, 10.573 são sentenças da primeira instância da Justiça paulista

Por Laura Ignacio — De São Paulo

16/02/2024 05h03 · Atualizado há 6 dias

LGPD: Penalidades

FISCALIZAÇÕES SOBRE PROTEÇÃO DE DADOS PESSOAIS



TCE-PR audita adequação à LGPD em órgãos de administração e previdência do Estado



Auditoria do TCE fiscaliza aplicação da Lei Geral de Proteção de Dados no RN



TCU fiscaliza implementação dos dispositivos da LGPD — Tribunal Regional Eleitoral da Paraíba

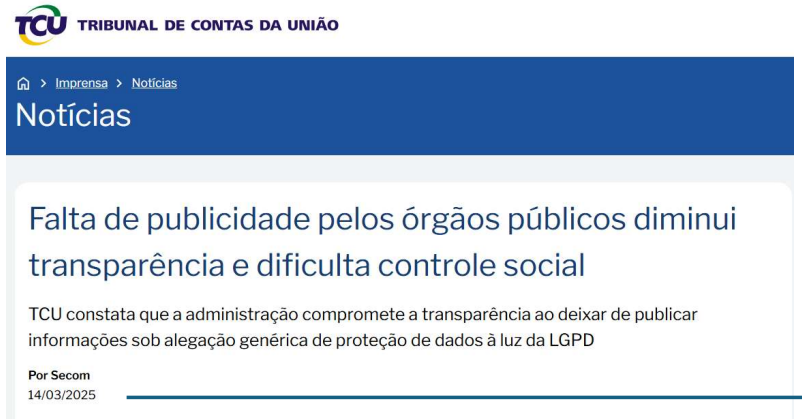
FISCALIZAÇÕES SOBRE PROTEÇÃO DE DADOS PESSOAIS



TCE-PE vai fiscalizar cumprimento da Lei de Proteção de Dados



Tribunal cobra adequação de órgãos estaduais e municipais à LGPD



Falta de publicidade pelos órgãos públicos diminui transparência e dificulta controle social

14/03/2025



TCU constata que a administração compromete a transparência ao deixar de publicar informações sob alegação genérica de proteção de dados à luz da LGPD

ATO DE TERCEIRO

Ataque hacker não exclui responsabilidade por proteção de dados

Danilo Vital

4 de dezembro de 2024, 10h31

Civil

O tratamento de dados pessoais configura-se irregular quando deixa de fornecer a segurança que o titular poderia esperar, consideradas as circunstâncias relevantes do caso.

Ataque hacker não exclui responsabilidade por proteção de dados

ATENÇÃO!

Servidor público que viola a LGPD pode responder por **IMPROBIDADE ADMINISTRATIVA!**



RESPONSABILIDADE DO SERVIDOR

every
CYBERSECURITY GRC PRIVACY