every
CYBERSECURITY GRC PRIVACY

UN GLOBAL COMPACT

CERTIFICADA ISO 27001 SEGURANÇA DA INFORMAÇÃO

CERTIFICADA ISO 27701 PRIVACIDADE DA INFORMAÇÃO

PROTEÇÃO DE DADOS PESSOAIS: DA TEORIA À PRÁTICA

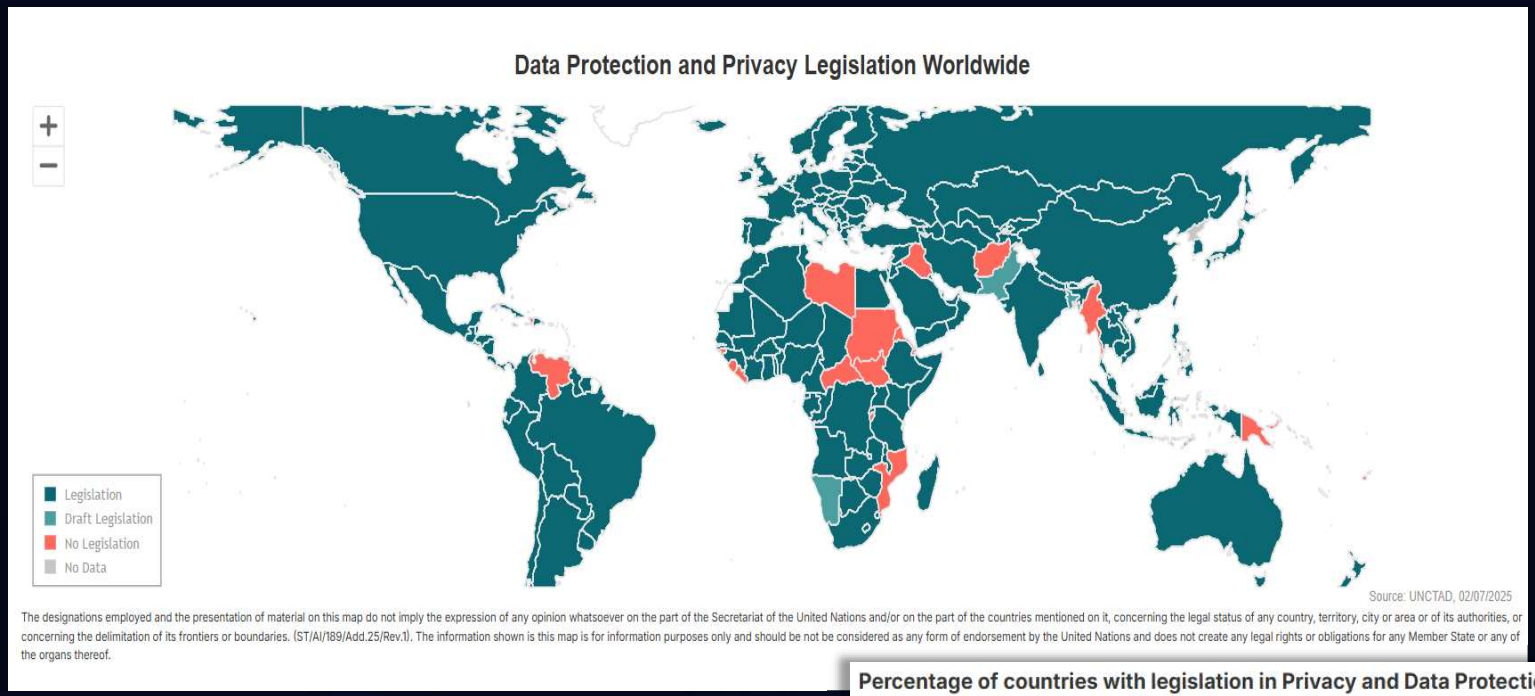
Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo - PRODEST

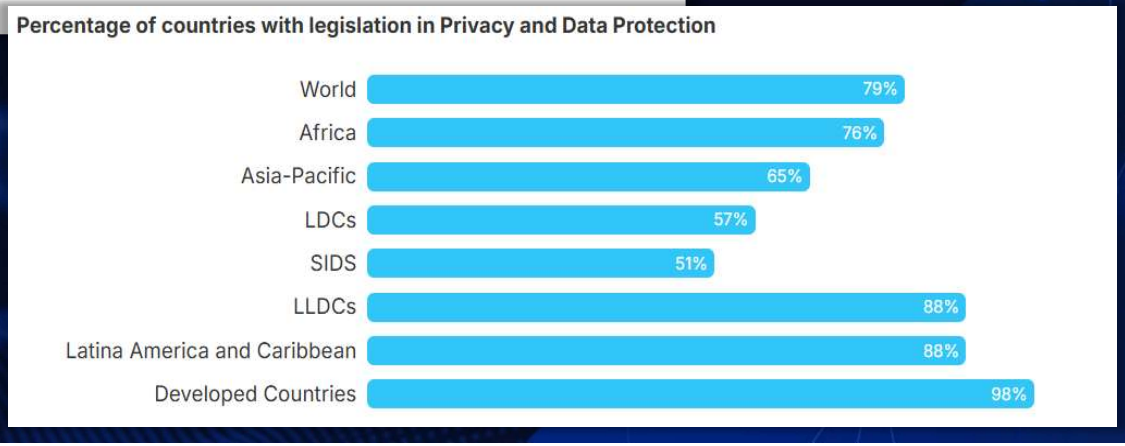
Contrato: 2024.000027.28203.01

AGENDA

1. PANORAMA SOBRE A PRIVACIDADE DA INFORMAÇÃO
2. CONTEXTUALIZAÇÃO COM PRODEST
3. CONCEITOS BÁSICOS
4. APLICABILIDADE CONCRETA
5. NOTÍCIAS ATUAIS
6. PRÓXIMOS PASSOS

PROGRESSO MUNDIAL





PRIVACIDADE DA INFORMAÇÃO NO BRASIL

Marcos Regulatórios

ANTES DO ADVENTO DA LGPD

Marco Civil da Internet

Cód. Defesa do Consumidor

Lei de Acesso à Informação

08/07/2019

Criação da ANPD

Autoridade Nacional de Proteção de Dados (ANPD)

14/08/2020

Entrada em Vigor

Lei Geral de Proteção de Dados Pessoais (LGPD)

01/08/2021

Entrada em Vigor das Sanções Administrativas aplicáveis pela ANPD

10/02/2022

Emenda Constitucional nº 115

Direito Fundamental

Política Estadual de Proteção de Dados Pessoais e da Privacidade
Decreto Estadual nº 4.922- R/2021

Art. 1º Fica instituída a Política Estadual de Proteção de Dados Pessoais e da Privacidade (PEPDP) em consonância com a agosto de 2018, Lei Geral de Pro ao direito fundamental à autode

§ 1º As disposições desta P eletrônico ou físico e vinculam t que tenham personalidade juríd

§ 2º As empresas públicas, a com personalidade jurídica de di dados pessoais e da privacid conselhos de administração ou c Geral de Proteção de Dados.

Art. 4º São diretrizes desta Política Estadual de Proteção de Dados Pessoais e Privacidade:

I - estabelecimento de regras de boas práticas pelos agentes de tratamento observando, para tanto, a natureza, o es dos riscos e dos benefícios decorrentes d

II - levantamento dos dados pessoais

III - mapeamento dos fluxos dos da do Poder Executivo Estadual;

IV - alinhamento à Política Estadua Espírito Santo (PESI);

V - revisão e adequação dos contrato Poder Executivo Estadual à Lei Geral de P

VI - instituição de medidas de propo dados, privacidade, segurança da infor harmonia entre a Lei Geral de Proteção d LAI.

Art. 8º Os dados pessoais tratados no âmbito do Poder Executivo Estadual deverão:

I - ser mantido em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e acesso das informações pelo público em geral, quando for o caso;

II - ser compartilhados somente em razão do atendimento das finalidades específicas de execução de políticas públicas e atribuições legais pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais que orientam a execução desta Política.

Parágrafo único. Fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres quando o compartilhamento de dados ocorrer entre os órgãos, autarquias e fundações do Poder Executivo Estadual, observados os princípios e diretrizes desta Política e as demais normas da LGPD.

QUAL O LIMITE DOS DIREITOS À PROTEÇÃO DE DADOS PESSOAIS?



POR QUE DEVEMOS NOS PREOCUPAR?

RANKING MUNDIAL

PODER 360

Brasil lidera ranking mundial com 7 bi de dados vazados na internet

Levantamento da NordVPN mostra que dos 94 bilhões de cookies expostos na dark web, 7 bilhões são de usuários brasileiros

PODER360
4.jun.2025 (quarta-feira) - 13h55

O Brasil ocupa a 1ª posição entre os países com maior volume de dados de internet vazados no mundo, segundo levantamento divulgado pela NordVPN na 3ª feira (27.mai.2025).

Os usuários brasileiros são os principais afetados por este problema de segurança digital, que expõe informações pessoais e pode resultar em fraudes, roubo de identidade e invasões de contas online.

Fonte: www.poder360.com.br/poder-tech/brasil-lidera-ranking-mundial

MAIOR VAZAMENTO JÁ REGISTRADO

exame.

Home > Tecnologia

Vazamento de senhas: ataque hacker expõe 16 bilhões de credenciais do Google, Apple e Facebook

FBI emitiu um alerta pedindo cautela com mensagens de texto suspeitas que contenham links

Um **megavazamento de dados** expôs 16 bilhões de credenciais de login, vinculadas a grandes empresas de tecnologia e serviços governamentais. A descoberta foi divulgada por pesquisadores da **Cybernews**, site especializado em segurança cibernética, e confirmada pela agência *Reuters*. Este pode ser considerado o maior vazamento de dados já registrado.

Publicado em 20 de junho de 2025

Fonte: Vazamento de senhas: ataque hacker expõe 16 bilhões de credenciais do Google, Apple e Facebook | Exame

DECISÕES JUDICIAIS - LGPD

Tribunais brasileiros dobram menções à LGPD em decisões em um ano

Estudo aponta consolidação da lei e utilização contínua com o Código de Defesa do Consumidor



Tribunais brasileiros dobram menções à LGPD em decisões em um ano | CNN Brasil

AUDITORIA DO TCU – ACÓRDÃO 1372/2025

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria aponta falhas na aplicação da LGPD por organizações federais

Fiscalização do TCU avaliou 387 entes e recomendou melhorias

Por Secom
14/07/2025

Auditoria do Tribunal de Contas da União (TCU) revelou que quase um terço das organizações federais ainda não implementou **medidas básicas** para cumprir a **Lei Geral de Proteção de Dados** (LGPD). A fiscalização avaliou as providências de adequação de **387 órgãos e entidades federais** a essa lei, indicando aperfeiçoamentos que precisam ser feitos.

Sob relatoria do ministro Walton Alencar Rodrigues, o TC 009.980/2024-5 revelou o **descumprimento de dispositivos da LGPD** por grande parte das organizações auditadas. No acórdão, foram feitas recomendações para melhorias.

Auditoria aponta falhas na aplicação da LGPD por organizações federais – Notícias | Portal TCU

DIMENSÕES - TCU ACÓRDÃO 1372/2025

TRIBUNAL DE CONTAS DA UNIÃO

387
ORGANIZAÇÕES FEDERAIS FISCALIZADAS

- Liderança
- Preparação
- Estrutura para Condução da Iniciativa de Adequação
- Capacitação
- Contexto Organizacional

- Conformidade do Tratamento
- Compartilhamento de Dados Pessoais
- Violação de Dados Pessoais
- Medidas e Controles de Proteção de Dados Pessoais Implementados
- Direitos dos Titulares
- Medidas de Proteção

Auditoria aponta falhas na aplicação da LGPD por organizações federais – Notícias | Portal TCU

SUBDIMENSÕES DO ACÓRDÃO 1372/2025

TRIBUNAL DE CONTAS DA UNIÃO

Capacitação	Conformidade do Tratamento	Direito dos Titulares	Compartilhamento dos Dados	Medidas de Proteção
Plano de capacitação dos colaboradores em proteção de dados pessoais	Registro e inventário de dados pessoais	Implementação dos mecanismos para atender os direitos dos titulares de dados	Inventário de dados pessoais compartilhados	Gestão dos riscos identificados
Plano de capacitação	Elaboração de Relatório de Impacto à Proteção de Dados Pessoais	Elaboração de Política de Privacidade	Adequação do compartilhamento de dados com as bases legais da LGPD	Aplicação da metodologia Privacy by Desing e Privacy by Default
	Implementação de controles para mitigar riscos identificados	Implementação de canal específico para atender os direitos dos titulares de dados	Mapeamento dos agentes de tratamento nos processos que envolvem compartilhamento de dados	Implementação de anonimização como proteção dos dados pessoais
	Coleta dos dados pessoais estritamente necessários	Implementação de gestão das solicitações dos titulares de dados	Implementação de Política de Transferência Internacional	Elaboração de plano de ação contínuo para implementar atividades de conformidade

Auditoria aponta falhas na aplicação da LGPD por organizações federais – Notícias | Portal TCU



ATENÇÃO!

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

SANÇÕES PREVISTAS NA LGPD

Advertência

Notificação com indicações de prazos para adoção de medidas corretivas

Publicização

Divulgação da infração nos canais oficiais ou de grande circulação

Bloqueio

Suspensão de uso dos dados pessoais referentes à infração

Eliminação

Destruição dos dados pessoais referentes à infração

Suspensão

Interrupção temporária do funcionamento do banco de dados ou da atividade de tratamento

Proibição

Vedação ao exercício da atividade relacionada ao tratamento de dados

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS APLICADA AO PRODEST

DA TEORIA À PRÁTICA



CONTEXTO DO PRODEST

Trata massivamente dados pessoais para execução das atividades finalísticas.

Compartilha dados pessoais com outros órgãos públicos.

Realiza o processamento de dados pessoas em sistemas digitais.

Representa uma referência em tecnologia para o Estado do Espírito Santo.

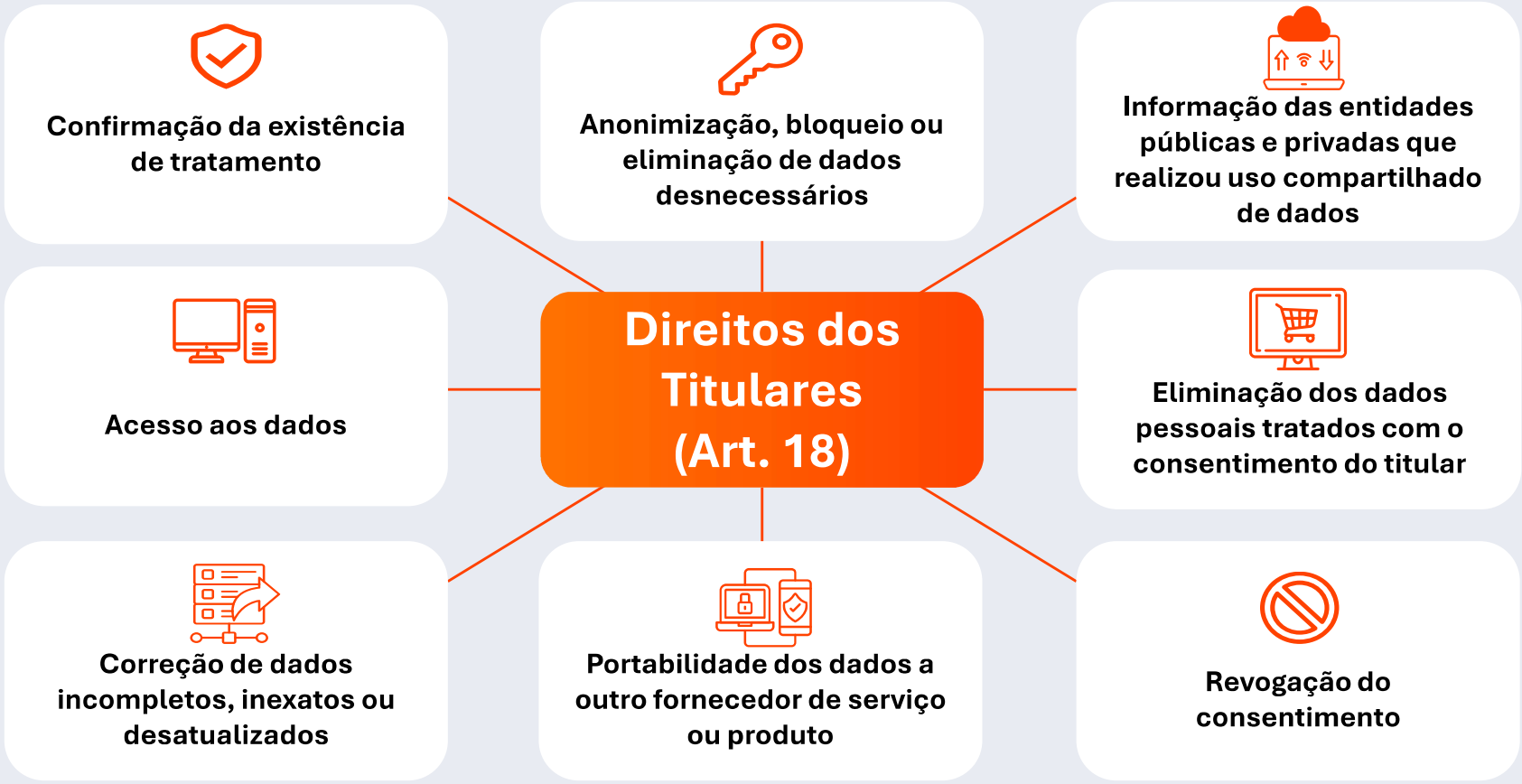


IMPACTO POSITIVO

LGPD:
restritiva ou permissiva?

- Conceitos inéditos
- Empoderamento do titular de dados
- Princípios específicos
- Autodeterminação informativa
- Peculiaridades para o poder público
- Responsabilidades e sanções
- Bases legais e legitimadoras do tratamento de dados

DIREITOS DOS TITULARES DE DADOS PESSOAIS - LGPD



CONCEITOS IMPORTANTES



Dados Pessoais

Informação da 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.



Grupo Vulnerável

Dados pessoais relacionados a menores de idade, idosos, pessoas com deficiência, e outros, a depender do contexto.

CONCEITO NA PRÁTICA

APLICABILIDADE

CATEGORIA	EXEMPLOS DE DOCUMENTOS	POSSÍVEIS VIOLAÇÕES
Identificação pessoal	RG, CPF, passaporte, título de eleitor, CNH, carteira de trabalho	Uso para fraude, falsidade ideológica, roubo de identidade, exposição de dados biométricos.
Saúde	Prontuários médicos, exames, relatórios psicológicos, histórico de tratamentos	Discriminação, estigma social, violação de dados sensíveis.
Financeiro	Extratos bancários, declarações de IR, faturas de cartão, contratos de empréstimos	Fraude financeira, extorsão, roubo de identidade
Profissional e Educacional	Histórico escolar, avaliações de desempenho, dossiês funcionais, processos disciplinares	Danos à reputação, discriminação profissional ou acadêmica
Judicial/administrativo	Processos de família, criminais, denúncias com identificação de vítimas/testemunhas	Exposição de vítimas, constrangimento, retaliação

E-DOCS: CLASSIFICAÇÃO ADEQUADA DA INFORMAÇÃO

No E-Docs, usuários podem classificar documentos como:



1. **Público:** visível para todos que tenham acesso ao processo.
2. **Organizacional:** restrito a uma unidade/órgão.
3. **Sigiloso:** acesso apenas para pessoas designadas.

E-DOCS: CLASSIFICAÇÃO DA INFORMAÇÃO

O QUE É?

Atribuição do nível de restrição ou sigilo de acesso aos documentos com dados pessoais.

OBJETIVO

Evitar que dados pessoais ou sensíveis fiquem acessíveis a pessoas que não precisam deles para desempenhar suas funções.

CRITÉRIO

Finalidade Específica
+
Necessidade
+
Adequação

E-DOCS: SIGILO E CONFIDENCIALIDADE

Classificação da Informação



*A necessidade de classificação de uma peça, encaminhamento ou processo como "**sigiloso**" não está relacionada apenas ao tipo de dados pessoais contidos neles (por exemplo, se é CPF, nome etc.) e nem à **forma** de tratamento desses dados pessoais, mas **à natureza** do conteúdo e se a exposição a quem não precisar ter acesso a eles (quando sob classificação pública/organizacional) vier a **comprometer a intimidade, privacidade, honra, imagem ou segurança de uma ou mais pessoas, ou expô-las ao constrangimento**.*

Rodrigo Faustini

LGPD: ATORES IMPORTANTES



Titular

Pessoa natural (física) a quem se referem os dados pessoais tratados.

Exemplos: cidadãos, servidores públicos.



Controlador

Pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões essenciais do tratamento de dados pessoais.



Operador

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



ANPD

Autoridade Nacional de Proteção de Dados Pessoais é uma Autarquia responsável por regular, fiscalizar e sancionar os destinatários da LGPD.



Encarregado

Responsável por atuar como um canal de comunicação entre a organização, os titulares dos dados e a ANPD.

ENCARREGADO DE DADOS
Decreto Estadual nº 4.922- R/2021

COMITÊ ENCARREGADO CENTRAL

- Colegiado estadual que orienta os Encarregados Internos dos órgãos;
- Coordenação dos Encarregados Internos;
- Estabelece diretrizes e padrões a serem seguidos pelos Encarregados Internos;
- Recebe a comunicação de incidentes dos órgãos, informando-os à ANPD;
- Composição: SEG, SEGER, PGE, SECONT e PRODEST.

ENCARREGADO INTERNO

- Vinculado à alta direção e se reporta ao CEC e à ANPD;
- Orientar todos os setores da organização à luz da proteção de dados pessoais;
- Estruturar o Programa de Privacidade e Proteção de Dados Pessoais da organização;
- Monitorar a implementação da adequação institucional à LGPD.

AGENTES DE TRATAMENTO

Controladoria Singular

Apenas um controlador define os elementos essenciais do tratamento de dados pessoais.

Controladoria Conjunta

Dois ou mais controladores tomam decisões comuns ou convergentes sobre as finalidades e elementos essenciais do tratamento.

Suboperador

Contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador.
É equiparado ao operador.

CICLO DE VIDA DOS DADOS PESSOAIS



TRATAMENTO DE DADOS PESSOAIS

OPERAÇÕES DE TRATAMENTO	CONCEITOS
COLETA	Obter os dados pessoais pela primeira vez, de forma física ou digital
PRODUÇÃO	Gerar novos dados a partir de outras informações
RECEPÇÃO	Receber dados pessoais que foram enviados por outra pessoa ou sistema
REPRODUÇÃO	Copiar ou duplicar os dados
ACESSO	Consultar ou visualizar os dados

TRATAMENTO DE DADOS PESSOAIS

OPERAÇÕES DE TRATAMENTO	CONCEITOS
TRANSMISSÃO	Enviar os dados pessoais de um ponto a outro
PROCESSAMENTO	Organizar ou trabalhar os dados pessoais para gerar informações ou resultados
MODIFICAÇÃO	Alterar ou atualizar os dados pessoais
COMUNICAÇÃO	Passar os dados pessoais a alguém autorizado
ARMAZENAMENTO	Guardar os dados pessoais em meio físico ou digital

TRATAMENTO DE DADOS PESSOAIS

COMPARTILHAMENTO	⟷	Disponibilização de dados para diversas aplicações, usuários ou organizações, com finalidades distintas.
USO COMPARTILHADO	⟷	Duas ou mais organizações tratam dados pessoais de forma compartilhada, a partir de finalidades específicas alinhadas.
TRANSFERÊNCIA	⟷	Movimentação dos dados pessoais de um local para outro.

CASOS CONCRETOS – MAPEAMENTO DE PROCESSOS

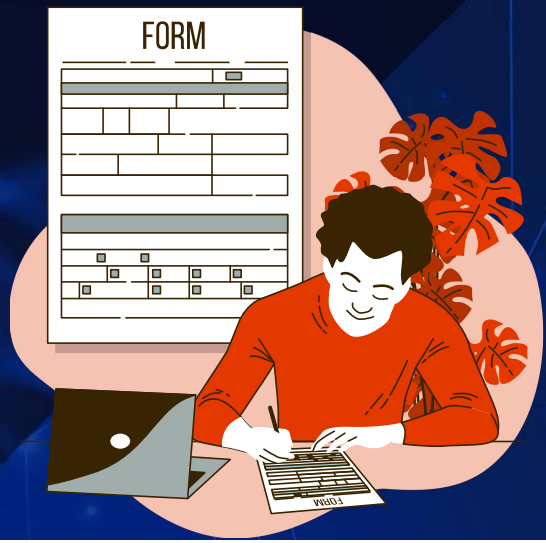
CADASTRO DE VISITANTES

DADOS PESSOAIS LEGITIMAMENTE COLETADOS

- **Nome completo e CPF:** Para identificar a pessoa com segurança.
- **Reconhecimento facial:** Para agilizar futuras entradas e garantir que a pessoa que sai é a mesma que entrou.
- **Número de telefone:** Para entrar em contato em caso de emergência.

DADOS PESSOAIS EXCESSIVAMENTE COLETADOS

- Filiação, Endereço, Histórico escolar, Estado Civil, Religião.



CASOS CONCRETOS – MAPEAMENTO DE PROCESSOS

PARECERES JURÍDICOS - ASJUR

Passo 1: O Jurídico recebe um ofício

- A ASJUR recebe um ofício da Procuradoria Geral do Estado (PGE) sobre uma ação trabalhista de um ex-empregado.
- O ofício deve conter, no mínimo, o número do processo judicial e cópia da inicial.

Passo 2: O Jurídico solicita informações no RH

- O parecer jurídico (ASJUR) depende de informações do histórico do empregado.
- A **ASJUR** envia a solicitação de informações ao **GEREH**
- Transmissão dos dados pessoais pela **GEREH**

PRINCÍPIOS DA LGPD

Emissão de Pareceres - ASJUR

Princípio da Finalidade

O tratamento dos dados tem um objetivo claro: **defender a empresa em uma ação judicial**. Toda a cadeia de acesso e transmissão é justificada por essa finalidade.

Princípio da Adequação

O Jurídico e o RH acessam dados de um histórico de emprego, o que é adequado ao caso. Não acessam, por exemplo, dados bancários ou de saúde sem necessidade.

Princípio da Necessidade

Apenas os dados **essenciais** para a defesa na ação devem ser acessados e transmitidos. Não é necessário acessar o histórico pessoal completo do empregado.

Princípio da Segurança

A transmissão dos dados entre os setores (ASJUR e GEREH) deve ser feita por meios seguros (sistemas internos, e-mail criptografado, etc.) para evitar vazamentos.

CASOS CONCRETOS – MAPEAMENTO DE PROCESSOS

GESTÃO DE USUÁRIOS

TRATAMENTO DE DADOS PESSOAIS

Coleta: Acontece no momento em que a solicitação é feita no sistema GLPI, quando são coletados o **nome do usuário** e, ocasionalmente, o **número de telefone** e **e-mail corporativo**.

Acesso e Armazenamento: Os dados são acessados para criação do usuário e são armazenados no sistema GLPI e no Active Directory (AD).

Transmissão/Compartilhamento: Acontece quando a solicitação é enviada via GLPI e quando a informação de acesso é integrada ao AD.

Processamento/Utilização: Os dados pessoais são usados para criar, gerir e conceder acesso a bancos de dados. A ação do usuário DBA de executar ações dentro do banco é um tipo de processamento.

Retenção INDEVIDA:

Os dados pessoais não são descartados do Datacenter.

Há retenção por prazo indeterminado.

BASES LEGAIS

- Mediante consentimento do 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

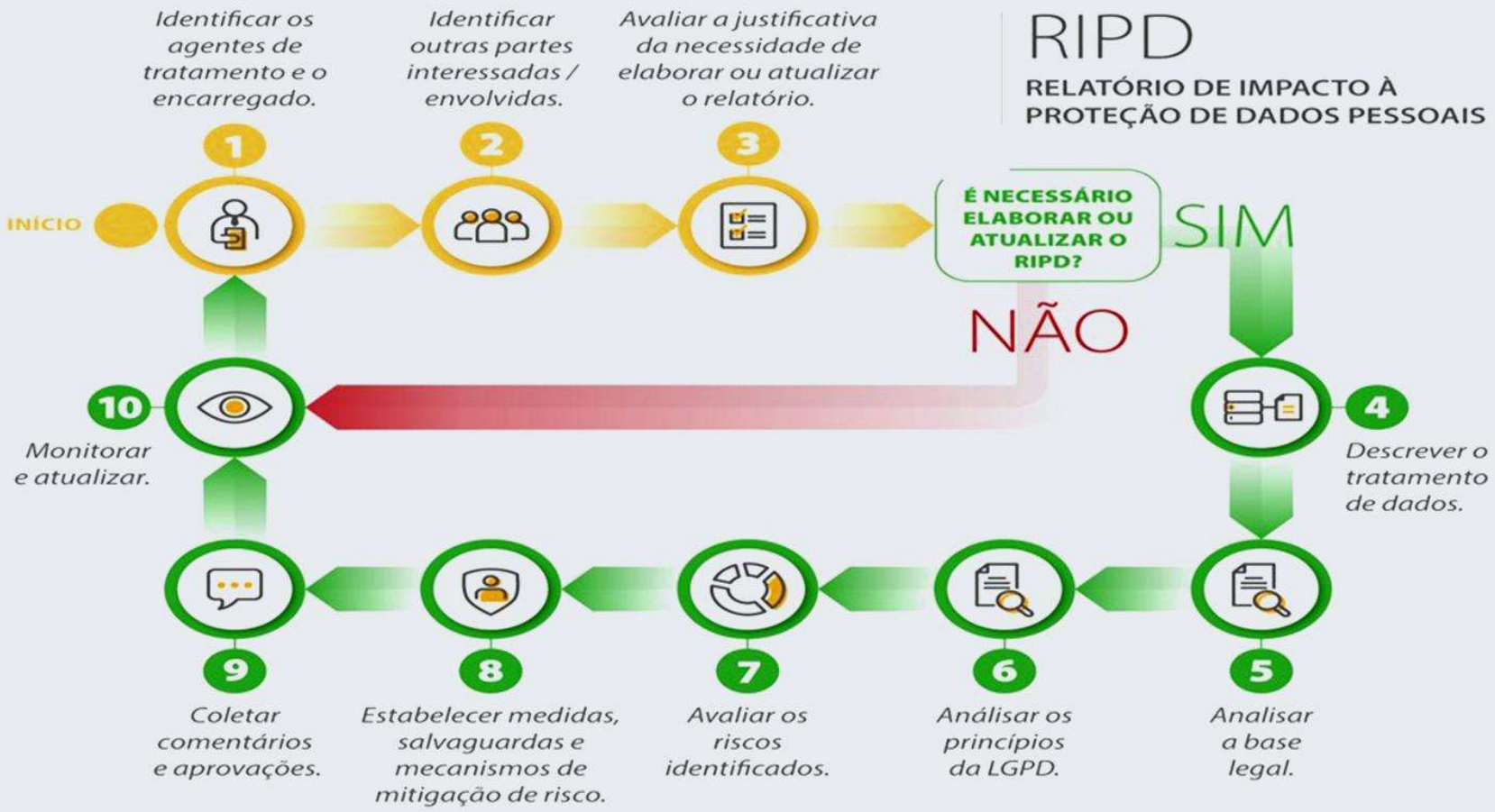
APLICAÇÃO DAS BASES LEGAIS

FINALIDADE	BASE LEGAL
Para a assinatura de contratos com empresas vencedoras de licitações	Cumprimento de obrigação legal ou regulatória (Art. 7º, II) ou para execução de contratos (Art. 7º, V)
Publicação de informações sobre remuneração de servidores públicos	Cumprimento de obrigação legal ou regulatória (Art. 7º, II)
Dados financeiros para pagamento de fornecedores	Para execução de contratos (Art. 7º, V)
Inscrição em evento de formação, como palestras	Consentimento (Art. 7º, I)

PONTOS RELEVANTES NO PROCESSO DE ADEQUAÇÃO À LGPD

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Privacy by Design



RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

POR QUE É NECESSÁRIO?



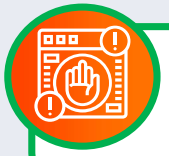
A ausência do RIPD agrava os riscos identificados e as sanções em caso de fiscalização da ANPD.



Aponta as ações de mitigação implementadas ou necessárias à redução dos riscos.



O RIPD identifica como o processo compromete ou coloca em risco os direitos dos titulares.



Representa a proatividade em prevenir incidentes com dados pessoais

DIAGNÓSTICO E MAPEAMENTO DE PROCESSOS

- Identificação dos dados pessoais tratados
- Diagnóstico dos riscos à privacidade
- Mapeamento da tramitação dos dados pessoais
- Plano de ação para mitigação dos riscos identificados

O conhecimento antecede a proteção!

ETAPAS IMPLEMENTADAS

GOVERNANÇA
Revisão e elaboração de documentos (RIPD, PIA, LIA, Política de Privacidade)

COOKIES
Política e banner de cookies

CONSENTIMENTO
Procedimentos para coleta e revogação de consentimento (físico ou eletrônico)

DIAGNÓSTICO E MAPEAMENTO
Análise de documentos internos e de conformidade (CIS, NIST, ISOs 27701 e 27001), mapeamentos de processos que tratam dados pessoais (ROPAs)

ANÁLISE DE RISCOS À PRIVACIDADE
Elaboração de metodologia e análise de riscos nos ROPAs

PLANO DE AÇÃO
Elaboração de Planos de Ação para mitigar os **riscos** identificados nos ROPAs

APOIO AO DPO
Assistência e orientação às atividades diárias do Encarregado Interno

AVALIAÇÃO DE FORNECEDORES
Metodologia e checklist para avaliação da adequação de terceiros

O PROGRESSO DA ADEQUAÇÃO À LGPD É TRANSVERSAL!

SOLUÇÕES ESTRATÉGICAS

COMO PROSSEGUIR COM O PROGRAMA DE GOVERNANÇA EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO?

COMO PROMOVER A EFETIVA BLINDAGEM DO AMBIENTE?

PILARES

PRIVACIDADE DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO

PILARES CONVERGENTES E COMPLEMENTARES

Todo Programa de Privacidade e Segurança da Informação envolve necessariamente:



Programa de Governança

PRIVACIDADE DA INFORMAÇÃO

Mapeamento e Diagnóstico
- Mapeamento de Processos
- Registro de Operações
- Descoberta de Dados

Estruturação do Programa
- Gestão de Riscos
- Metodologia Privacy By Desing
- Due Dilligence em Fornecedores

Políticas e Normas
- Aviso de Privacidade
- Políticas de Cookies,
- Transferência Internacional
- Relatório de Impacto à Proteção de Dados Pessoais

Treinamento e Conscientização
- Workshop Customizado
- Capacitação em Privacidade
- Simulações de *Phishing*

Monitoramento Contínuo
- Gap Analysis da ISO 27001 e 27701
- Avaliação de Conformidade de Privacidade

Sua jornada em privacidade continua...

A implementação da LGPD é uma responsabilidade TRANSVERSAL que exige engajamento contínuo.