

Guia 06

Provedor de Internet = B2C

Indústria = B2B

Este guia foi elaborado pelos membros do Grupo de Trabalho de LGPD do Instituto Paranaense de Compliance (IPACOM)

ELABORAÇÃO

Luciliane Ribeiro
Murilo Pastori Roberti

COORDENAÇÃO

Letícia Sugai

Objetivo

- Contato direto com a alta direção e membros do comitê executivo
- Mapeamentos de processos
- Elaboração da matriz de riscos e controles
- Implantação de ferramentas e sistemas de controle
- Desenvolvimento de programas de comunicação e treinamento
- Contato direto com a alta direção e membros do comitê executivo
- Mapeamentos de processos
- Elaboração da matriz de riscos e controles
- Implantação de ferramentas e sistemas de controle
- Desenvolvimento de programas de comunicação e treinamento

Segurança de dados



A **segurança de dados** diz respeito aos **meios de proteção** que uma organização está adotando **para impedir que terceiros não autorizados acessem** os seus dados.

Ela se concentra na proteção de dados contra ataques maliciosos e impede a exploração de dados (violação de dados ou ciberataque).

Inclui controles de acesso, criptografia, segurança de rede, etc.

Privacidade de dados

A **privacidade de dados** se concentra nos **direitos dos indivíduos**, na finalidade de coleta e processamento de dados, nas preferências de privacidade e na maneira como as organizações controlam os dados pessoais dos titulares de dados.

Ela se concentra em como coletar, processar, compartilhar, arquivar e excluir os dados de acordo com a lei.

Termos-chave da LGPD



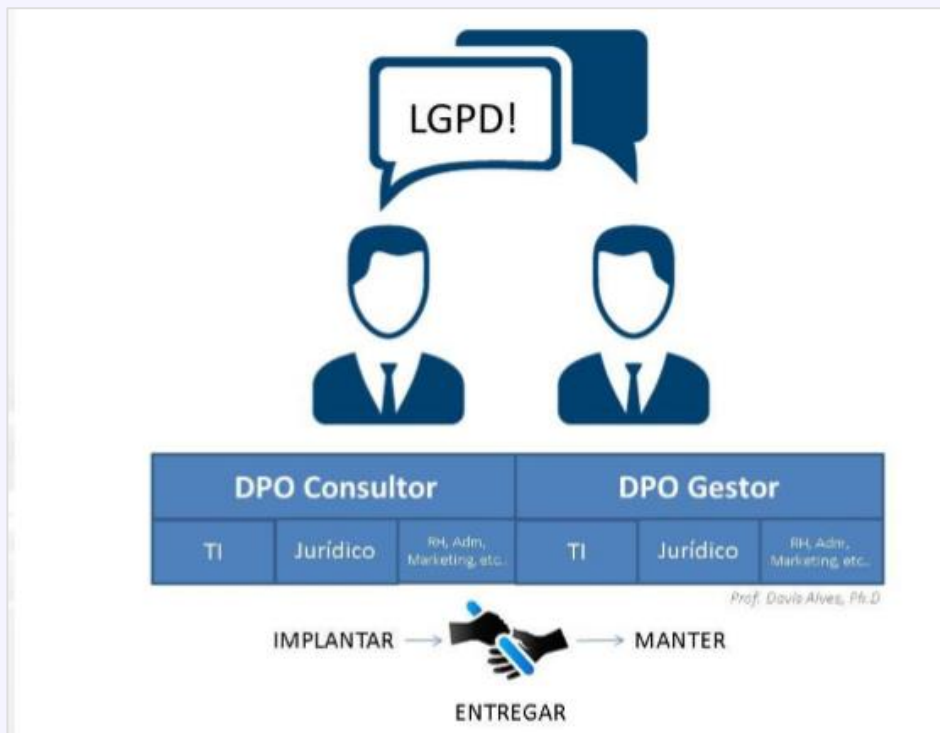


O que acontece em 1 minuto de internet?



Os dados são de **2019**

Nomeação de um encarregado



02/09/2020 Datacenters redesenham programa de privacidade | Suplementos | Valor Econômico

Valor | Suplementos

Datacenters redesenham programa de privacidade

Criptografia e dupla autenticação são reforçadas

Por **Ana Luiza Mahlmeister** — Para o Valor, de São Paulo
21/08/2020 05h02 · Atualizado há uma semana

02/09/2020 Custo da conformidade pode variar de R\$ 50 mil a R\$ 800 mil | Suplementos | Valor Econômico

Valor | Suplementos

Custo da conformidade pode variar de R\$ 50 mil a R\$ 800 mil

Valor elevado da multa compensa os investimentos, além dos ganhos de reputação

Por **Ana Lúcia Moura Fé** — De São Paulo
21/08/2020 05h02 · Atualizado há uma semana

02/09/2020 Fornecedores de TI ajustam processos de tratamento de dados | Suplementos | Valor Econômico

Valor | Suplementos

Fornecedores de TI ajustam processos de tratamento de dados

Impacto da LGPD no uso de novas tecnologias exige adequação também de usuários

Por **Martha Funke** — Para o Valor, de São Paulo
21/08/2020 05h02 · Atualizado há uma semana

“O mais importante é mudar procedimentos e treinar funcionários.”

Indústria / B2B / B2C

Maior diferença: volume de informações (titulares de dados)

Empresas Locais vs empresas Internacionais

- GDPR
 - Lições aprendidas
 - Formulários e processos
 - Sistemas (ex.: OneTrust)
- DPO
- Execução “top-down” vs convencimento local
- Processos já hospedados em servidores internacionais (ex.: servidores de e-mail, SuccessFactor, Sciforma, OneTrust, outros...)

Tabela de Medidas de Segurança por ATIVO

Exemplo: Proteção para um Servidor de Rede com Dados Pessoais

Segurança Organizacional	- Cadastro dos usuários autorizados	- Assinatura Digital	- Auditoria de Conteúdo	- Destinação para empresa autorizada
Segurança Técnica	- Usar com senha	- VPN	- Criptografia	- Sanitização de Dados
Segurança Física	- Usar em local seguro	- Link dedicado	- Rack de Telecom	- Triturar
Medidas de Seg. da Informação vs. Ciclo de Vida da Informação →	Manuseio	Transporte	Armazenamento	Descarte

PIA (privacy impact assessment), mapeamento

1. Escopo / contexto
 - a) Resumo, descrição e “dono” do processo
 - b) Quem tem acesso aos dados/informações
 - c) Transações regionais / transnacionais
 - d) Categoria de informações pessoais e sensíveis
 - e) Acessos de terceiros e controladores
 - f) Documentação contratual
 - g) Controles e métodos de acesso e segurança de informação (TI)
 - h) Retenção da informação



2. Validação (parecer)
 - a) Mapa de risco
 - b) Ações corretivas
 - c) Plano de remediação
3. Recomendação do encarregado / DPO

Category of Information	Specific Information	Source of Information
Identification Information	<input checked="" type="checkbox"/> Last Name, First Name <input type="checkbox"/> Address <input type="checkbox"/> Photo <input type="checkbox"/> Birth Date, Birth place <input checked="" type="checkbox"/> Other, list: time in/out; reason for coming to the factory, who met with, who had lunch with, visited areas, which transport mean was used.	<input checked="" type="checkbox"/> Directly from individual <input type="checkbox"/> Directly from another system (include name): <input type="checkbox"/> Indirectly from: Energy utility
Personal Life	<input type="checkbox"/> Life habit(s) <input type="checkbox"/> Family status <input type="checkbox"/> Other, list: energy consumption habits	<input type="checkbox"/> Directly from individual <input type="checkbox"/> Directly from another system (include name): <input type="checkbox"/> Indirectly from: Energy utility
Professional Life	<input type="checkbox"/> C.V. <input type="checkbox"/> Professional situation <input type="checkbox"/> Educational background	<input type="checkbox"/> Directly from individual <input type="checkbox"/> Directly from another system (include name):

Art. 37. O controlador e o operador devem manter **registro das operações de tratamento de dados pessoais** que realizarem, especialmente quando baseado no legítimo interesse.

Finalidade	Tipo de medida	Medidas concretas	Tempo de conservação (se aplicável)	Tratamentos a que se aplica
MS00a	ex. Medidas de proteção lógica	ex. antivírus, software para a utilização de no mínimo 8 caracteres alfanuméricos, implementação regular de atualizações de segurança, backups		ex. T000, T001, T012
MS00b	ex. Controle de acesso de instalações	ex. apenas utilizadores com cartão biométrico de acesso podem aceder		ex. todos os tratamentos
MS00c	ex. Registo de log	ex. log de acesso e alteração ou eliminação de dados com identificação, data e hora de ligação, IP	ex. 2 anos	ex. T002 a T010
MS00d	ex. Enciclopédia dos dados	ex. lista sequencial ordenada de nomes, utilização de TIC, automatização de sempre-datas de expiração		ex. T014
MS00e	ex. Salvaguarda dos dados	ex. backup diários, redundância, plano de disaster recovery com cenário alternativo	ex. os backups são conservados por 3 anos	ex. T012
MS01				
MS02				
MS03				
MS04				
MS05				
MS06				
MS07				
MS08				
MS09				
MS10				
MS11				
MS12				
MS13				
MS14				
MS15				
MS16				
MS17				
MS18				
MS19				
MS20				
MS21				
MS22				
MS23				
MS24				
MS25				

Transferência internacional de dados

É Quando o controlador/empresa oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, na forma de:

- a) cláusulas contratuais específicas para determinada transferência;
- b) cláusulas-padrão contratuais;
- c) normas corporativas globais;
- d) selos, certificados e códigos de conduta regularmente emitidos.

Além disso, pode considerar nos seguintes casos:

1. quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
2. quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
3. quando a autoridade nacional autorizar a transferência;
4. quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
5. quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público;
6. quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades.

Guia 04

LGPD x Mercado Financeiro

ELABORAÇÃO

Luciliane Ribeiro
Murilo Pastori Roberti

COORDENAÇÃO

Letícia Sugai