

3º Seminário de

Gestão Arquivística de Documentos do Legislativo Federal 2019

**“A Lei Geral de Proteção a Dados Pessoais
e seu impacto nos arquivos”**

Data: 23 de outubro de 2019

Horário: das 9h às 18h

Local: Auditório Senador Antonio Carlos Magalhães
(Av. N2, Bloco 2 do Senado Federal)

Inscrições:
<https://www12.senado.leg.br/institucional/arquivo>

LEI GERAL DE PROTEÇÃO DE DADOS

Charlley Luz

charlley@feedconsultoria.com.br



Charlley Luz: Fui publicitário, achei que o mundo da comunicação estava mudando e me interessei pelo mundo da informação e dos documentos digitais. Tornei-me **bacharel em Arquivologia pela UFRGS** e **Mestre em Ciência da Informação pela ECA-USP**. Sou empreendedor, consultor, professor, palestrante e pesquisador. **Especialista em sistemas e serviços de informação**, desenvolvo projetos em **UX, usabilidade, portais, colaboração**, além de planejar **ambientes e repositórios digitais e de gestão documental** junto à Feed Consultoria.



INTERFACE



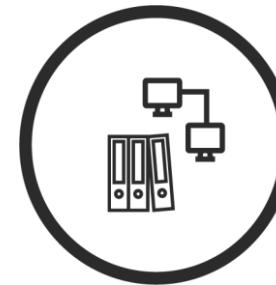
PLANEJAMENTO



TAXONOMIA



SEARCH



GESTÃO DA INFORMAÇÃO

Você protege seus dados?

- Já teve documentos roubados ou perdidos?
- Seu celular é seguro?
- Você compartilha o computador com estranhos?
- Você tem antivírus? Seu Firewall esta ativado?
- Você cadastra seus dados em sites de troca de informações?
- Você lê os termos e condições de um serviço ofertado pela internet?
- Você joga on line? Você está seguro?
- Senhas...
- Seu wifi...
- Redes sociais...
- Nuvem...
- Este site precisa que você aceite os cookies...

Governo interliga bases e permite cruzamento de dados biométricos

Cadastro Base começa com CPF; plano é incluir também dados sensíveis



10.out.2019 às 13h41

Atualizado: 10.out.2019 às 21h11

EDIÇÃO IMPRESSA

Ouvir o texto

A-

A+

Paula Soprana

SÃO PAULO O presidente [Jair Bolsonaro](#) instituiu nesta quinta-feira (10), por meio de decreto, o Cadastro Base do Cidadão, composto por uma “base integradora” de dados pessoais de todos os brasileiros. O objetivo é regulamentar o compartilhamento de dados entre diferentes esferas do governo.

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).



The screenshot shows the official website of the Brazilian Presidency (www.planalto.gov.br) displaying the text of the General Data Protection Law (LGPD). The page features the Brazilian flag and the title 'Presidência da República' at the top. The text is organized into sections: 'LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.', 'Texto compilado', 'Mensagem de veto', 'Vigência', and 'O PRESIDENTE DA REPÚBLICA'. The text discusses the purpose of protecting fundamental rights of privacy and data processing, and includes a section on 'CAPÍTULO I - DISPOSIÇÕES PRELIMINARES'.

LEI Nº 13.853, DE 8 DE JULHO DE 2019 Conversão da Medida Provisória nº 869, de 2018 Mensagem de veto

Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.



The screenshot shows the official website of the Brazilian Presidency (www.planalto.gov.br) displaying the text of the conversion law (Lei nº 13.853, DE 8 DE JULHO DE 2019) of the MP nº 869. The page features the Brazilian flag and the title 'Presidência da República' at the top. The text is organized into sections: 'LEI Nº 13.853, DE 8 DE JULHO DE 2019.', 'Conversão da Medida Provisória nº 869, de 2018', 'Mensagem de veto', and 'O PRESIDENTE DA REPÚBLICA'. The text specifies that it alters the Lei nº 13.709 to establish the National Data Protection Authority.

LGPD mais que a soma de outras leis

Marco Civil da Internet

Lei de Acesso À Informação

Código de Defesa do Consumidor

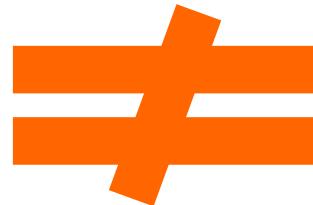
Lei do Cadastro Positivo

Estatuto da Criança e do Adolescente

Normas Setoriais

Legislações Locais

Resoluções de Conselhos Profissionais



Conceitos na lei:



DADO PESSOAL:

informação relacionada a pessoa natural identificada ou identificável;

DADO PESSOAL SENSÍVEL:

dado pessoal 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, quando vinculado a uma pessoa natural;

DADO ANONIMIZADO:

dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

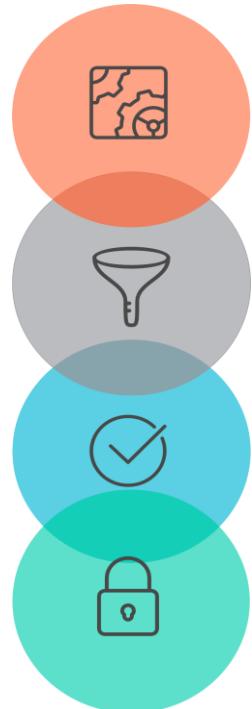
LGPD mais que a soma de outras leis



Privacidade como **direito fundamental**
Lei geral, aplicável a **todos os tipos de dados** pessoais
Escopo **territorial**
Tratamento de Dados realizados no Brasil
Bens e **serviços fornecidos no Brasil**
De dados de **indivíduos localizados no Brasil**
E **coletados** no Brasil

o vazamento de dados, bem como o acesso a dados por pessoas não-autorizadas, passa a representar um dano direto à pessoa física, **semelhante a um dano moral**.

Preceitos do Tratamento de dados



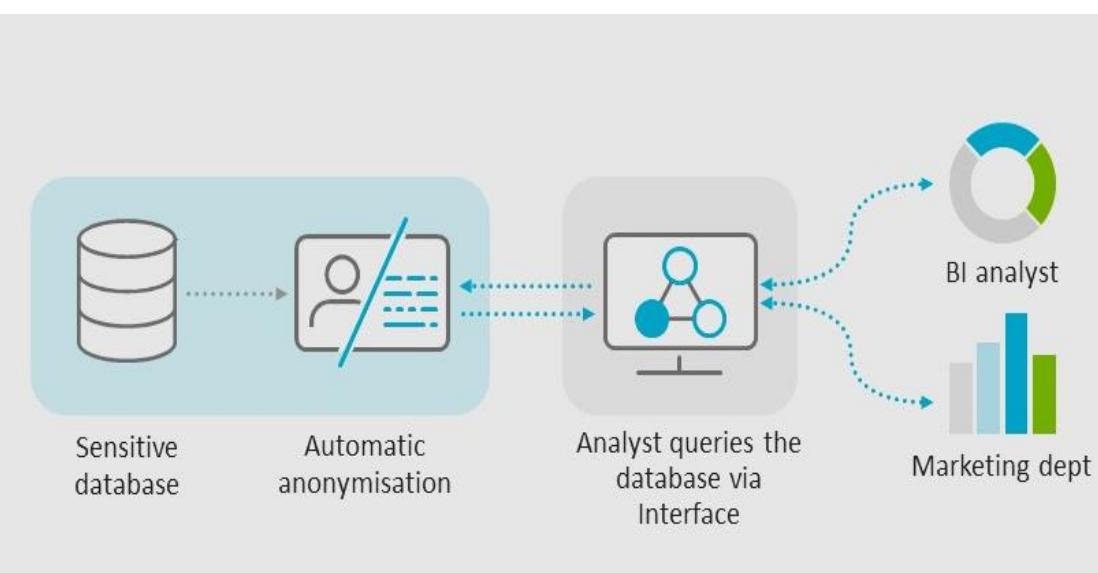
FINALIDADE LÍCITA E LEGÍTIMA

ORIGEM LÍCITA DOS DADOS

GARANTIR EXERCÍCIO DE DIREITOS DOS USUÁRIOS

**RESPEITO ÀS NORMAS DE TRATAMENTO E GARANTIA DE
SEGURANÇA DA INFORMAÇÃO**

Conceitos na lei:



CONSENTIMENTO:

manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada

ANONIMIZAÇÃO:

processos e técnicas por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

PSEUDOANONIMIZAÇÃO:

processos e técnicas por meio dos quais um dado tem sua possibilidade de associação dificultada. **O dado pseudoanonimizado é considerado dado pessoal para fins de aplicação da LGPD, tendo em vista a possibilidade de associação desse dado a uma pessoa natural.

Alguns pontos da nova lei:

- ✓ O titular tem **direito de saber** quais dados estão sendo coletados e para quais finalidades;
- ✓ O titular deve saber como os seus dados serão tratados, podendo autorizar o tratamento ou não;
- ✓ O titular poderá solicitar a exclusão de informações pessoais;
- ✓ O titular pode acessar, solicitar cópia ou migrar dados (portabilidade);
- ✓ As comunicações com o titular devem utilizar **linguagem clara, concisa e transparente**;
- ✓ **Incidentes** com vazamentos ou violação de dados devem ser notificados em até 72 horas;

Alguns pontos da lei:

Resumidamente, o tratamento de dados pessoais pode ser feito para:

1. Finalidades autorizadas pelo titular (manifestação inequívoca de vontade);
2. Proteção da vida do titular;
3. Tutela da saúde do titular;
4. Exercício regular do direito (processos judiciais, administrativos e arbitrais)
5. Cumprimento de obrigações da empresa;
6. Execução do contrato do titular com a empresa;
7. Atender interesse legítimo do controlador ou de terceiro;
8. Proteção de crédito;
9. Uso particular / não econômico;
10. Fins jornalísticos;
11. Fins artísticos;
12. Fins acadêmicos;
13. Estudos e pesquisas;
14. Gestão pública;
15. Segurança pública; *
16. Defesa nacional; *
17. Segurança do Estado; *
18. Investigação e repressão de infrações penais; *
19. Tratamento de dados provenientes de fora do território nacional.

Atenção:
**Dados tornados manifestadamente
públicos pelo titular podem ser
utilizados!**

* Lei específica a ser editada

Conceitos na lei:



TRATAMENTO:

toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

CONTROLADOR:

pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

PROCESSADOR:

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

Tratamentos de Dados Consentidos pela LGPD:

Ainda no art. 7º:

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

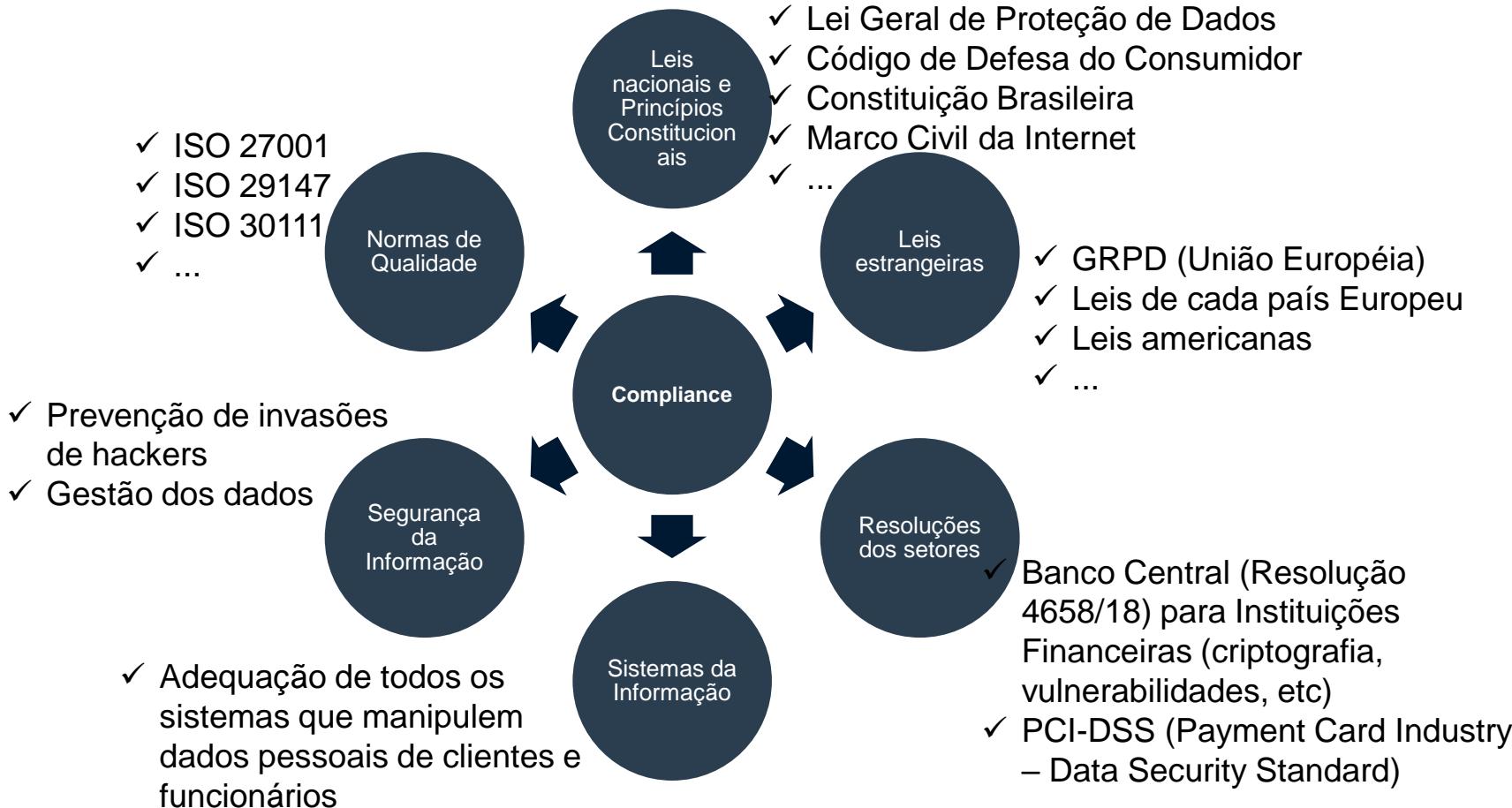
Art. 12º

Os dados anonimizados não serão considerados desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Me parece que a melhor forma de se proteger da LGPD é anonimizar os dados o mais rápido possível e ter um controle mais acirrado sobre quem tem acesso à tabela que possibilita personificar esses dados.

Atenção:

Dados tornados manifestadamente públicos pelo titular podem ser utilizados **COM RESSALVAS!**

Pensando compliance





Família 27000 – ISO/IEC 27000 series –

Descrição e Vocabulário

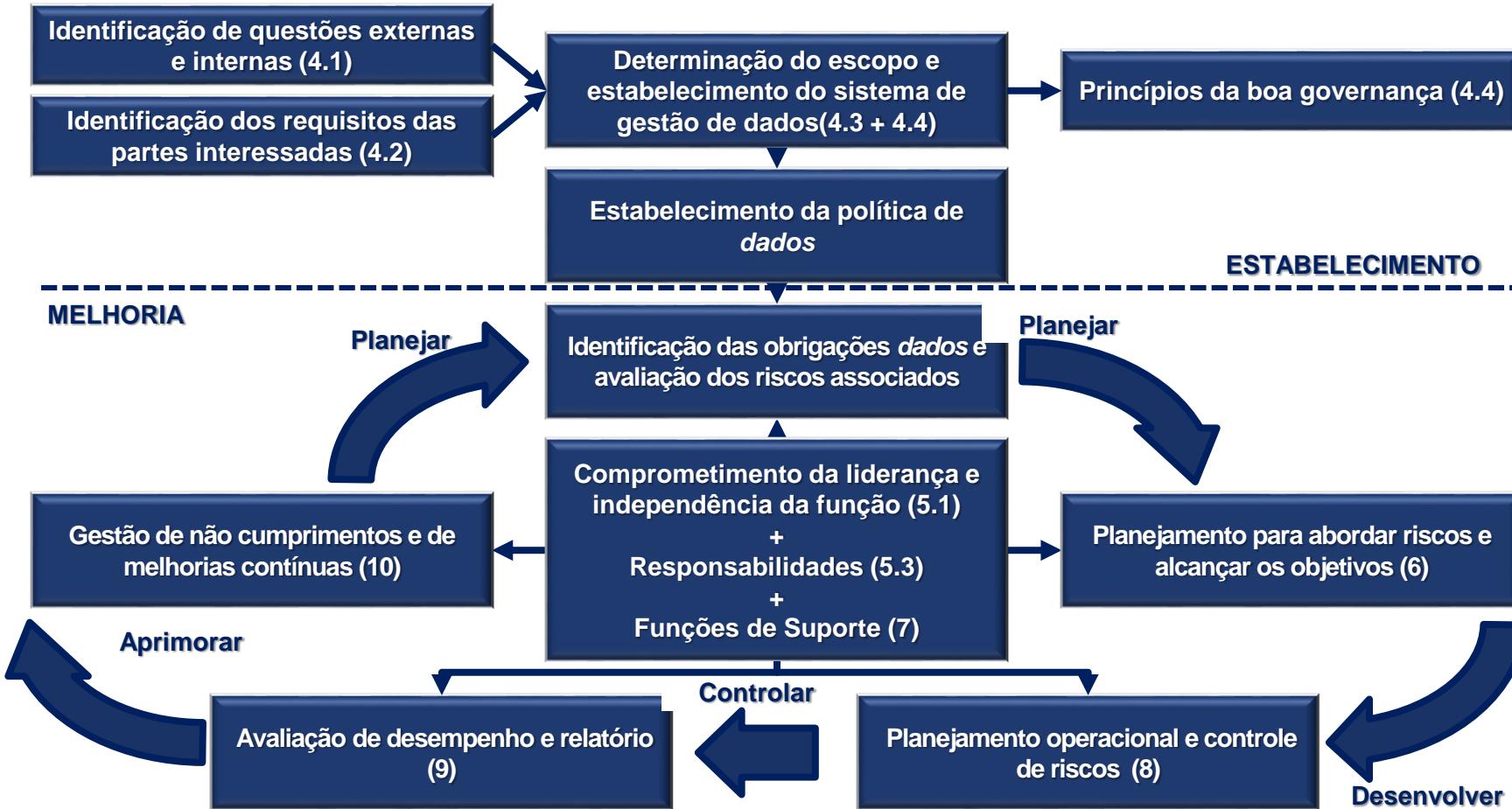
Organizações podem desenvolver e implementar **uma estrutura para gerenciar a segurança de seus ativos de informação**

Se preparar para uma avaliação independente do seu SGS I (Sistema de Gestão de Segurança da Informação) aplicado à proteção de informações

Normas

1. ISO/IEC 27002:2005 - Código de Prática para Gestão da Segurança da Informação
2. ISO/IEC 27005:2011 - Gestão de Riscos de Segurança da Informação
3. ISO/IEC 27007 :2012– Diretrizes para auditoria de SGSI
4. ISO/IEC 27014:2013 – Governança de segurança da informação 5/30

Implementação ISO 27000



LGPD x ISO 27000

Lei 13709	ISO 27002
Capítulo 1 – Disposições Gerais	Item 4.1 – Entendendo a organização
Capítulo 2 – Tratamento de dados pessoais	4.2 – Partes interessadas 4.3 – Escopo de atuação 4.4 - Governança
Capítulo 3 – Direitos do Titular	4.4 – Governança 5.2 – Política de Segurança de dados 5.3 - Responsabilidades 6 – Planejamento 8 – Riscos 9 – Melhoria Continua

Framework

Lei 13709	ISO 27002
Capítulo 4 – Tratamento de dados pelo poder público	4.2 – Partes interessadas 4.3 – Escopo de atuação 4.4 - Governança 4.4 – Governança 5.2 – Política de Segurança de dados 5.3 - Responsabilidades 6 – Planejamento 8 – Riscos 9 – Melhoria Continua
Capítulo 5 – Transferência Internacional de dados	Idem ao anterior

Framework

Lei 13709	ISO 27002
Capítulo 6 – Agentes de tratamento de dados	4.4 - Governança 5.3 - Responsabilidades 6 – Planejamento 8 – Riscos 9 – Melhoria Continua
Capítulo 7 – Segurança de dados	ISO 27001
Capítulo 8 – ANPD	4.4 - Governança 5.3 - Responsabilidades 6 – Planejamento 8 – Riscos 9 – Melhoria Continua

Implementação ISO 27000



Quem são os atores?



O TITULAR:

Pessoa natural que tem seus dados pessoais tratados pelo controlador;



O CONTROLADOR: *

Pessoa natural ou jurídica, de direito público ou privado, a quem competem **as decisões referentes ao tratamento de dados pessoais**;



O OPERADOR: *

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



O ENCARREGADO - DPO (Data Protection Officer):

Pessoa **indicada pelo controlador** para atuar **como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados**;

* Agentes de tratamento

Competências dos profissionais envolvidos

- Segurança da Informação
- Gestão da Informação
 - Administração de Dados / Banco de Dados
 - Gestão de Processos
 - Gestão de Sistemas
 - Gestão da Qualidade
- Compliance
- Marketing
- Análise de Riscos
- Direito – conhecimento das leis e políticas públicas
 - Gestão de mudanças / cultura organizacional
 - Comunicação, inclusive com a alta gerência
 - Poder de persuasão / psicologia



Algumas atividades para estar “Compliance”

- ✓ Mapeamento dos canais de entrada de dados pessoais
- ✓ Identificar os focos de tratamento de dados pessoais (marketing, RH, vendas, empresas terceirizadas)
- ✓ Identificar foco de documentos pessoais físicos e digitais;
- ✓ Definir regras de privacidade / modelo de governança;
- ✓ Conscientizar funcionários / campanhas internas / gestão da mudança;
- ✓ Revisar Sistemas de Informação;
- ✓ Revisar rotinas de tratamento de dados;
- ✓ Revisar contratos e relações com terceiros;
- ✓ Proteger os dados: Anonimização, Pseudomização e Criptografia;
- ✓ Elaborar planos de resposta a incidentes e remediação;
- ✓ Estar pronto para a auditoria: Gerenciamento, rastreio e relatórios.

Alguns pontos da nova lei:

- ✓ **Projetos de sistemas devem considerar a proteção dos dados** como parte imprescindível;
- ✓ **Implementação de práticas e medidas para segurança de dados;**
- ✓ **Recomendação de pseudonimização:** quando cabível, é recomendável que a empresa proteja informações sensíveis ocultando-as ou substituindo-as de alguma forma para que a identificação do usuário só seja possível com a adição de outros dados;
- ✓ **Dados que forem anonimizados não serão considerados dados pessoais;**
- ✓ **Entidades públicas não poderão repassar dados** de usuários a entidades privadas;
- ✓ **Responsabilização** sobre o tratamento dos dados;

Algumas documentos a ser criados / revisados:

- ✓ Relatório de impacto à proteção de dados pessoais *
 - ✓ Mapa de fluxo de dados pessoais (Personal Data Flow Map);
- ✓ Tabela de temporalidade de guarda de logs de consentimento;
- ✓ Política de gestão de dados pessoais;
- ✓ Política para tratamento de dados pessoais para terceirizados;
- ✓ Termo de uso e Política de privacidade;
- ✓ Contratos;
- ✓ NDA (Non-Disclosure Agreement, ou acordo de não divulgação) ;
- ✓ Check-list Compliance;
- ✓ Código de Conduta;
- ✓ Política de Segurança da Informação.

* Exigência determinada na Lei

Autoridade Nacional de Proteção de Dados

Conceito:

- Órgão da administração pública responsável por zelar, implementar, fiscalizar e aplicar sanções para o cumprimento desta Lei.
- É um órgão independente.
- Natureza transitória, podendo ser transformada em Autarquia vinculada à Presidência da República após dois anos, a critério do governo.

Composição:

- Conselho Diretor, órgão máximo de direção;
- Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;
- Corregedoria;
- Ouvidoria;
- Órgão de assessoramento jurídico próprio;
- Unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.

Competências:

- ✓ Editar regulamentos e procedimentos e medidas cabíveis sobre proteção de dados pessoais e privacidade;
- ✓ Promover o conhecimento das normas e políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
- ✓ Realizar auditorias e celebrar compromissos para eliminação de irregularidades;
- ✓ Deliberar sobre a interpretação desta Lei, suas competências e os casos omissos;
- ✓ Fiscalizar e aplicar sanções nos casos de descumprimento da legislação;
- ✓ Dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Responsabilização dos Agentes de Tratamento de Dados:

- Danos morais
- Danos materiais
- Para se livrar:
 - Provar que não houve má-fé
 - ...

Multas para as empresas:

- Até 2% do faturamento anual
 - Faturamento mensal de 100 mil reais mensais gera uma multa de 24 mil reais!

Oportunidades de Trabalho

Em empresas privadas

- 👤 Trabalho em empresas com projetos internos
- 👤 Trabalho em empresas especializadas na LGPD
- 👤 Consultor especialista na LGPD

Nas demais empresas públicas

- 👤 Diversas funções na própria ANPD
- 👤 Ministério Público
- 👤 Empresas públicas que utilizem dados pessoais

Obrigado

Charlley Luz



charlley@feedconsultoria.com.br



facebook.com/charlley



Linkedin.com/charlley



twitter.com/charlley