cybersecurity

Perspectivas e Desafios do Tratamento de Dados Pessoais na Administração Pública

Joao Araújo Monteiro Neto
CMS Advogados
Origami Cybersecurity

#SEPLAG2019

Agenda

@ Introdução

@ Overview do panorama legal

@ Perspectivas e desafios do tratamento de dados pessoais na administração pública

@ Q&A

Introdução

Apresentação

Introdução

Varejista norte-americana descobre até gravidez de clientes com a ajuda de software

Empresa cruza dados de compras dos clientes e consegue descobrir muita coisa sobre a vida pessoal de seus consumidores

Concessionária é alvo de processo por leitura facial no metrô de SP

Coleta de dados por câmeras da empresa ViaQuatro, que opera no metrô de São Paulo, é ilegal

VÍDEO: SEU NÚMERO DE TELEFONE VALE 9 CENTAVOS NO ZAP DOS POLÍTICOS

Amanda Audi, Tatiana Dias

22 de Outubro de 2018, 16h43

Introdução

Não é só o Alexa. O Google Assistant também ouve todas as nossas conversas

12/07/2019 11h25

Oito empresas contratadas pelo Google estão ouvindo secretamente nossas conversas, via Google Assistant, mesmo que não estejamos falando diretamente com o Google Home ou com nossos smartphones. É o que diz a reportagem da emissora belga VRT News, descrevendo o processo pelo qual as gravações do Google Home acabam sendo ouvidas por terceiros.

Início » Legislação » Marriott é multada em R$ 470 milhões por vazamento de dados de hóspedes

Marriott é multada em R$ 470 milhões por vazamento de dados de hóspedes

Para autoridade britânica, a Marriott não fez investigações suficientes ao comprar a Starwood

Por Victor Hugo Silva
09/07/2019 às 16h42

NEWS

Introdução

@ Processo de evolução acelerada:

- Código de Defesa do Consumidor (1990)
- Lei de Acesso a Informação (2011)
- Marco Civil da Internet (2014)
- Lei Geral de Proteção de Dados (2018)
- Política Nacional de Segurança da Informação (Decreto nº 9.637/18)
- Política Nacional de IoT (Decreto nº 9.854/19)

Introdução

O que é a LGPD e quais seus objetivos?

@ Lei federal que dispõe sobre a proteção de dados pessoais

@ Paradigma de adequação de atividades envolvendo dados pessoais

@ Fortalecimento da **privacidade** por meio da regulamentação do tratamento de **dados pessoais**

@ Reorganização e coordenação dos vários mecanismos regulatórios relacionados ao tratamento de dados pessoais

Introdução

Por que me preocupar com a LGPD?

Introdução

Por que me preocupar com a LGPD?

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

Introdução

Por que me preocupar com a LGPD?

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Introdução

França multa Google em 50 milhões de euros por uso de dados pessoais

Autoridade disse que falta transparência e informação oferecida pela empresa é insatisfatória

A French man is suing Uber for $45 million because he claims a privacy bug led his wife to divorce him

Introdução

Netshoes terá de pagar R$ 500 mil por vazamento de dados de 2 milhões de clientes

Valor de indenização foi firmado em acordo com Ministério Público do DF. Incidente comprometeu dados pessoais de servidores da Presidência, da Polícia Federal e do STF.

Por G1 DF

05/02/2019 18h51 · Atualizado há 7 horas

Dados pessoais

Em janeiro de 2018, o MP constatou que um incidente de segurança comprometeu dados pessoais como nome, CPF, e-mail, data de nascimento e histórico de compras de clientes da empresa.

Introdução

MP DFT Ministério Público do Distrito Federal e Territórios

Unidade Especial de Proteção de Dados e Inteligência Artificial - ESPEC

Termo de Ajustamento de Conduta

TAC n. 01/2019 - ESPEC

Inquérito Civil Público n° 08190.044813/18-44

Ementa: Termo de Ajustamento de Conduta firmado pela **Netshoes** (Ns2.Com Internet S.A.) com o **Ministério Público do Distrito Federal e Territórios**, para pagamento de indenização por danos morais coletivos causados pelo incidente de segurança que gerou o comprometimento de dados pessoais de clientes.

Introdução

MJ abre investigação contra Google por violação à privacidade

O Ministério da Justiça (MJ) abriu um processo administrativo para averiguar se a empresa Google violou direitos de usuários de internet. O procedimento, que ficará a cargo da Secretaria Nacional do Consumidor (Senacom), pode resultar, se atestada a responsabilidade da empresa, em uma multa de R$ 9,7 milhões.

Introdução

CNJ confirma vazamento de milhares de dados após invasão hacker

A ação contra o CNJ levou ao vazamento de dados como nome, CPF e números de contas bancárias

Por Victor Hugo Silva
02/04/2019 às 12h02

O Conselho Nacional de Justiça (CNJ) confirmou o ataque hacker realizado contra seus sistemas na segunda-feira (1º). A ação causou, segundo o *Valor*, o vazamento de milhares de dados como nome, CPF e números de contas bancárias.

Introdução

ECONOMIA

INSS admite que dados de recém-aposentados podem ter vazado e abre apuração

Thâmara Kaoru
Do UOL, em São Paulo
10/04/2019 04h00

O INSS admitiu a possibilidade de vazamento de informações de recém-aposentados durante o processo de concessão de aposentadoria. Trabalhadores relatavam que recebiam ligações de bancos e financeiras oferecendo empréstimo consignado, antes mesmo de saberem se teriam direito ao benefício. Em alguns casos, as empresas sabiam até o valor que o aposentado iria receber.

Introdução

SUS é alvo de vazamento com dados de 2,4 milhões de usuários

A brecha para o vazamento estaria em uma API que permite acessar dados de usuários do SUS

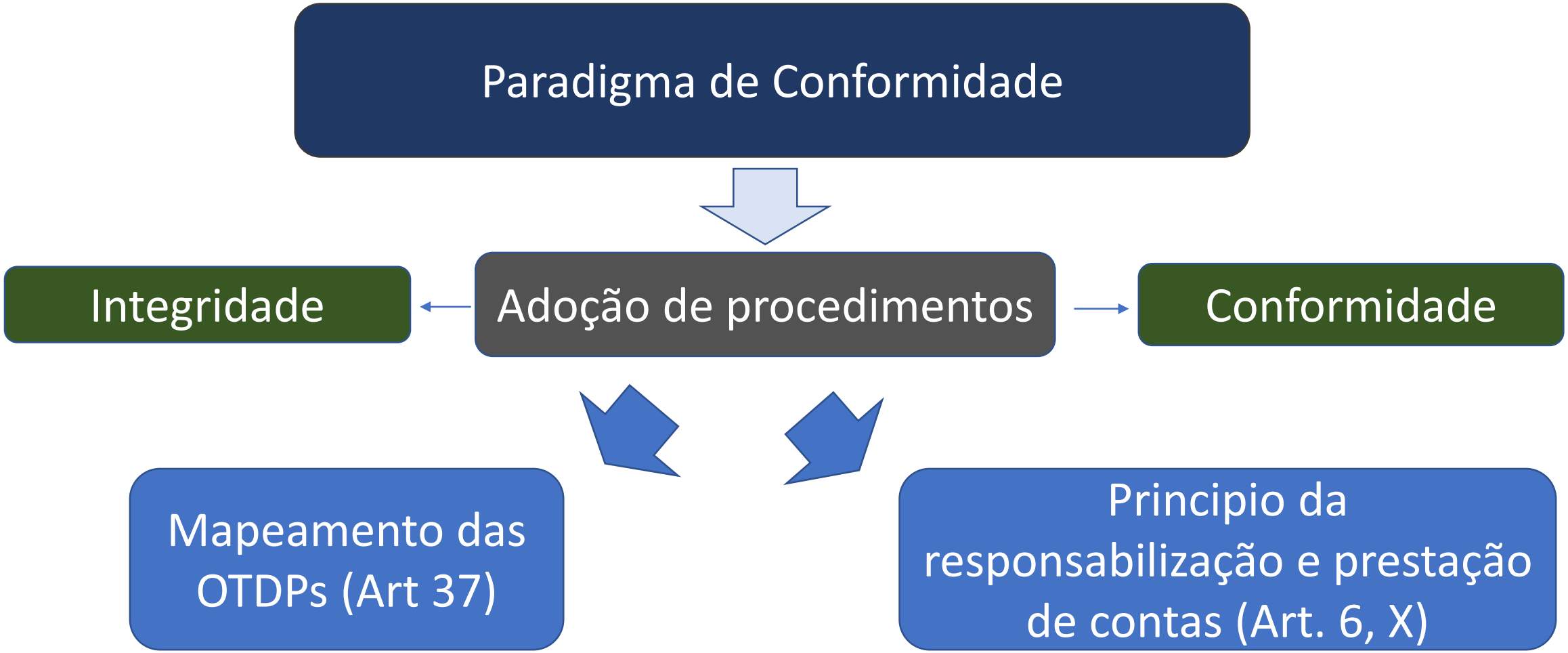
Por Victor Hugo Silva
11/04/2019 às 14h23

NEWS

As informações de cerca de 2,4 milhões de usuários do SUS (Sistema Único de Saúde) foram expostas nesta quinta-feira (11). O vazamento envolve um banco de dados com nome, nome da mãe, endereço, CPF e data de nascimento de pessoas cadastradas no serviço.

Introdução

A LGPD também:



Introdução

Esse cenário ainda está muito longe da minha atividade

Introdução

Não é bem assim....

Introdução

Vamos ver?

@ Recebe currículos?

@ Cadastra de visitantes?

@ Compartilha dados pessoais com parceiros?

@ Recebe mensagens do “fale conosco”?

@ Imprime documentos contendo dados pessoais?

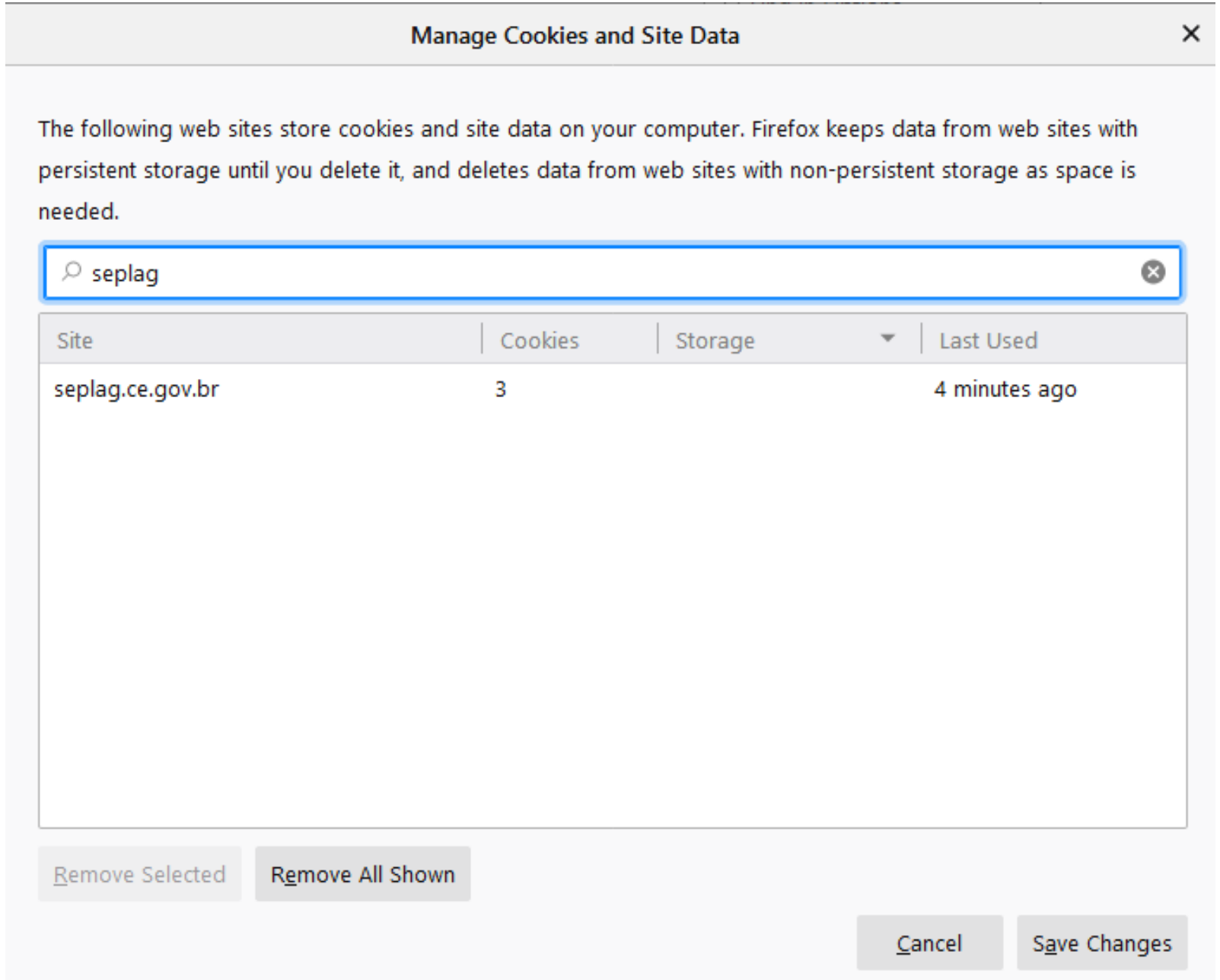
Introdução

Quer ver de novo?

ORTAL DO GOVERNO | CASA CIVIL | MAIS SITES
A A- A+
OUVIDORIA ESTADUAL | CEARA TRANSPARENTE | ACESSO A INFORMAÇAO
GOVERNO DO ESTADO DO CEARÁ
IMPRENSA | SERVIÇOS | GOVERNO
privacidade
ENCONTRAMOS 19 REGISTROS PARA SUA BUSCA
Serviços
0 RESULTADOS
Notícias
19 RESULTADOS
Outros
2 RESULTADOS
Não encontrou o que procura?
Avisa pra gente!
Nenhum serviço foi encontrado
Busque com outras palavras, tente novamente.

GOVERNO DO ESTADO DO CEARÁ
IMPRENSA
SERVIÇOS
GOVERNO
privacidade
ENCONTRAMOS 19 REGISTROS PARA SUA BUSCA
Serviços
0 RESULTADOS
Notícias
19 RESULTADOS
Outros
2 RESULTADOS
efine sua busca:
LIMPAR FILTRO
ECRETARIAS
DAGRI - ACADEMIA ESTADUAL DE EGURANÇA PÚBLICA DO CEARÁ
ESP - AGÊNCIA DE DEFESA GROPECUÁRIA DO ESTADO DO EARÁ
EE - CASA CIVIL DO GOVERNO DO STADO DO CEARÁ
EPI - CENTRAIS DE BASTECIMENTO DO CEARÁ - S/A
GD - COLÉGIO MILITAR DO ORPO DE BOMBEIROS
GE - COLÉGIO DA POLÍCIA ILITAR DO CEARÁ GENERAL OGARD FACÓ
CATEGORIAS
#PORDENTRODAPEFOCE
A EMPRESA
A SECRETARIA
A SEINFRA
A3P
ADOÇÃO
AESP
ASSISTÊNCIA SOCIAL
ATER
ATRAÇÃO DE INVESTIMENTOS
27 DE NOVEMBRO DE 2014 - 16:43 em www.etice.ce.gov.br
ONU adota resolução sobre privacidade digital proposta por Brasil e Alemanha
2 DE JUNHO DE 2015 - 18:28 em www.saude.ce.gov.br
Sobe para 9 total de salas de apoio à trabalhadora que amamenta
4 DE DEZEMBRO DE 2012 - 19:45 em www.saude.ce.gov.br
Ceará tem primeira sala de amamentação à mulher trabalhadora
6 DE DEZEMBRO DE 2012 - 12:35 em www.ceara.gov.br
Ceará terá primeira sala de amamentação à mulher trabalhadora
28 DE JANEIRO DE 2010 - 03:00 em www.ceara.gov.br
CTI - Coordenadoria de Tecnologia da Informação

GOVERNO DO ESTADO DO CEARÁ
IMPRENSA
SERVIÇOS
GOVERNO
privacidade
ENCONTRAMOS 19 REGISTROS PARA SUA BUSCA
Serviços
0 RESULTADOS
Notícias
19 RESULTADOS
Outros
2 RESULTADOS
efine sua busca:
LIMPAR FILTRO
ECRETARIAS
DAGRI - ACADEMIA ESTADUAL DE
EGURANÇA PÚBLICA DO CEARÁ
ESP - AGÊNCIA DE DEFESA
GROPECUÁRIA DO ESTADO DO
EARÁ
19 DE OUTUBRO DE 2018 - 08:38 em www.saude.ce.gov.br
Competências
27 DE SETEMBRO DE 2018 - 11:13 em www.pge.ce.gov.br
Competências


Manage Cookies and Site Data
The following web sites store cookies and site data on your computer. Firefox keeps data from web sites with persistent storage until you delete it, and deletes data from web sites with non-persistent storage as space is needed.
seplag
Site
Cookies
Storage
Last Used
seplag.ce.gov.br
3
4 minutes ago
Remove Selected
Remove All Shown
Cancel
Save Changes

Introdução

E como faço para me adaptar a esse novo paradigma?

Introdução

E como faço para me adaptar a esse novo paradigma?

Compreender os sistema regulatório				
Desenvolver um framework de trabalho customizado	Estruturar e gerenciar mudanças de governança	Desenvolver e implantar controles técnicos, administrativos, legais e organizacionais	Fomentar rotinas orgânicas e capilarizadas entre setores	Instituir sistema de governança de conformidade

Overview da LGPD

A quem se aplica a LGPD

ou

Tem estabelecimento no Brasil

Trata dados pessoais no Brasil

Oferece serviços ou bens ao mercado brasileiro

Trata dados de pessoas localizadas no Brasil

Overview da LGPD

A quem se aplica a LGPD (Descontruindo os mitos)

@ Não importam:

- O meio ou tecnologia utilizado no tratamento

. Dado em suporte eletrônico e dado em suporte físico
. Dado em formato estruturado ou em formato não estruturado

- O país sede da empresa
- Onde os dados estão
- A nacionalidade dos titulares dos dados
- A natureza jurídica do agente que trata dados pessoais

Overview da LGPD

A quem **não** se aplica a LGPD:

*Tratamento de dados pessoais realizado por **pessoa natural** para fins exclusivamente **particulares** e não **econômicos***

ou

Realizado por qualquer pessoa para fins exclusivamente:
jornalístico e artísticos
*Acadêmicos (pesquisa)**

ou

Segurança pública
Defesa nacional

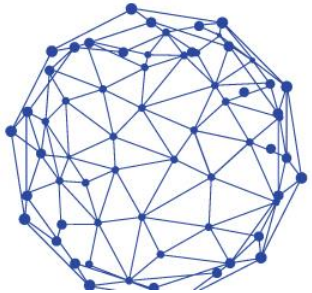
Segurança do Estado
Investigação de crimes

Overview da LGPD

Quais a inovações trazidas pela LGPD

Conceitos

Regras de tratamento



Obrigações e responsabilidades

Sistema de governança de dados pessoais

Overview da LGPD

A LGPD define a moldura conceitual do sistema regulatório

Dado pessoal sensível

Dado pessoal

Dado de saúde

Dado anonimizado

Overview da LGPD

Dado pessoal

Informação relacionada a pessoa natural identificada ou identificável, tais como

Nome e sobrenome
Endereço de uma residência
E-mail
Dados de localização
Endereço IP
Testemunhos de conexão
Telefone
Identificadores únicos e single out

Overview da LGPD

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 biométrico

Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person

Cuidado com o ***contexto***

Cuidado alguns dados que podem não parecer sensíveis como a localização de um indivíduo (geolocalização de uma pessoa que está frequentemente em uma igreja) podem, permitem inferir dados sensíveis (convicção religiosa)

Overview da LGPD

Dado de saúde

os dados de saúde estão dentro da categoria de dados sensíveis (saúde, vida sexual, os dados genéticos e biométricos como por exemplo: se é portador de determinada doença, tipo sanguíneo, frequência cardíaca, se é doador de órgãos). O conceito também permite a inclusão de dados pessoais que, num primeiro momento, podem não parecer ser de saúde, mas que, dentro de um contexto, podem permitir inferir dados de saúde, como a frequência de corridas de um determinado indivíduo (Luz, 2019).

Overview da LGPD

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

Anonimização

utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo

Overview da LGPD

A LGPD define a moldura conceitual do sistema regulatório

Controlador

Tratamento

EPD

Operador

Overview da LGPD

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

*A importância do estabelecimento de um Data Lifecycle Management - DLM (Data collection, permission structure e retention/deletion rules)

Overview da LGPD

Controlador

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

Operador

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

Overview da LGPD

EPD

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

Overview da LGPD

 # Princípios orientadores do tratamento de dados pessoais

Necessidade

Segurança

Finalidade

Adequação

Responsabilização e prestação de contas

Transparência

Prevenção

Não discriminação

Livre acesso

Boa-fé

Qualidade dos dados

Overview da LGPD

Princípios orientadores do tratamento de dados pessoais

Finalidade

Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades

Adequação

Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento

Overview da LGPD

 # Princípios orientadores do tratamento de dados pessoais

Necessidade

limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados

Segurança

Utilização de medidas aptas a proteger os dados pessoais de acessos não autorizados e destruição, perda, alteração, difusão ou comunicação

Overview da LGPD

 # Princípios orientadores do tratamento de dados pessoais

Responsabilização
e prestação de contas

demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Overview da LGPD

 # Princípios orientadores do tratamento de dados pessoais

Transparência

garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial

Prevenção

adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais

Overview da LGPD

Bases legais autorizadoras do tratamento de dados pessoais

Consentimento	Proteção da vida ou tutela da saúde	Exercício regular de direito
Cumprimento de obrigação legal	Execução de politica pública	Execução de contrato
Interesse legitimo do controlador	Proteção de crédito	Estudos e pesquisa*

Overview da LGPD

Obrigações para controladores e operadores de dados pessoais

Registro e transparência

Mapas de tratamento

Gerenciamento de risco

RIPDPs, Notificações e EPDs

Segurança e boas práticas

Programa de governança

Transferência internacional de dados pessoais

Salvaguardas legais e técnicas de proteção

Overview da LGPD

Estabelece um conjunto de direitos para os titulares

Acesso e obter informações

Correção e atualização

Informações sobre compartilhamento

Anonimização, bloqueio ou eliminação

Portabilidade

Overview da LGPD

Criação de um sistema de governança e um regime de fiscalização focado

Segurança e minimização de riscos

Fiscalização e fixação de punições administrativas

Reparação de prejuízos

Overview da LGPD

Segurança e minimização de riscos

@ Levando em consideração a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados o controlador poderá implementar programa de governança em privacidade que, no mínimo:

Overview da LGPD

Segurança e minimização de riscos

- Comprove a adoção de processos e políticas internas que assegurem o cumprimento de normas e boas práticas de proteção de dados pessoais;

- Estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade

- Esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos

- Conte com planos de resposta a incidentes e remediação e seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

Overview da LGPD

Fiscalização e fixação de punições administrativas

@ Cria a Autoridade Nacional de Proteção de Dados Pessoais

@ Cria o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

@ Fixa as seguintes punições:

. Advertência, com indicação de prazo para adoção de medidas corretivas
. Multa simples (até 2% do faturamento limitada a R$ 50 milhões por infração
. Multa diária
. Publicização da infração
. Bloqueio e/ou eliminação dos dados pessoais

Perspectivas e Desafios

Quais os principais desafios da LGPD para a administração pública:

a) Regulatório – legal

b) Regulatório – tecnologia da informação

c) Governança

d) Orçamentário

Perspectivas e Desafios

Elementos regulatórios – aspectos legais

@ Identificar qual a natureza e o escopo das operações de tratamento

@ Identificar as bases legais sustentando o tratamento de dados pessoais

@ Cumprir as obrigações legais vinculadas ao tratamento como por exemplo:

. Mapeamento das operações de tratamento e RIPDPs
. Notificações de privacidade
. Direito dos titulares

Perspectivas e Desafios

Identificar qual a natureza e o escopo das operações de tratamento

@ O que se considera administração pública:

. Lei n. 12.527/11 (Lei de Acesso a Informação):

I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;

II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Perspectivas e Desafios

Identificar qual a natureza e o escopo das operações de tratamento

@ No que tange a natureza do ente deve se observar também qual o escopo de suas atividades (regime de mercado concorrencial):

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Perspectivas e Desafios

Identificar qual a natureza e o escopo das operações de tratamento

@ Mas não é somente isso:

. A administração pública deve verificar qual o escopo da operação de tratamento de dados pessoais:

a) Atividades vinculadas a execução de políticas públicas
b) Atividades não vinculadas a execução de políticas públicas

Perspectivas e Desafios

Elementos regulatórios – aspectos legais

@ Identificar as bases legais sustentando o tratamento de dados pessoais:

. Execução de politica pública
. Consentimento
. Cumprimento de obrigação legal
. Legitimo interesse*

Perspectivas e Desafios

Elementos regulatórios – aspectos legais

@ Identificar as bases legais sustentando o tratamento de dados pessoais:

. Execução de política pública:

- Art. 7º e 11:

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (...)

Perspectivas e Desafios

Elementos regulatórios – aspectos legais

@ Identificar as bases legais sustentando o tratamento de dados pessoais:

. Execução de política pública:

- Obediência a finalidade pública;
- Caracterizada pela persecução do interesse público;
- Vinculada a executar competências/atribuições legais do serviço público;

Perspectivas e Desafios

@ Identificar as bases legais sustentando o tratamento de dados pessoais:

. Execução de política pública:

- O ente público fica obrigado a informar:

  i) as hipóteses em que realiza tratamento de dados pessoais;
  ii) a previsão legal;
  iii) a finalidade;
  iv) os procedimentos e as práticas utilizadas

Obs.: De forma clara e objetiva e em veículos de fácil acesso

Perspectivas e Desafios

@ Identificar as bases legais sustentando o tratamento de dados pessoais:

. Execução de política pública:

- O ente público fica obrigado a:

  i) Garantir a segurança do dado pessoal tratado;
  ii) Cumprir os princípios orientadores previstos na lei;
  iii) Nomear um EPD
  iv) Cumprir as obrigações previstas no artigo 37;

Perspectivas e Desafios

Elementos regulatórios – aspectos legais

@ Identificar as bases legais sustentando o tratamento de dados pessoais:

. Consentimento:

Perspectivas e Desafios

Consentimento:

@ Um dos elementos centrais autorizando o tratamento de dados pessoais, **mas não o único!**

@ O consentimento deverá referir-se a finalidades determinadas

@ As autorizações genéricas para o tratamento de dados pessoais são nulas.

Obs.: É dispensada a exigência do consentimento para os **dados tornados manifestamente públicos pelo titular**, resguardados os direitos do titular e os princípios previstos nesta Lei

Perspectivas e Desafios

 # Consentimento

@ Requisitos e características do consentimento válido :

- Registro por escrito ou por outro meio idôneo
- Cláusula destacada das demais cláusulas contratuais
- Manifestação livre
- Informada
- Inequívoca
- Finalidade determinada
- Revogável

Perspectivas e Desafios

 # Consentimento

@ Direitos do titular (quem consente):

- Acesso facilitado às informações sobre o tratamento de seus dados
- Informações disponibilizadas de forma clara, adequada e ostensiva sobre:

a) finalidade específica do tratamento
b) forma e duração do tratamento (respeito ao segredo comercial e industrial)
c) identificação do controlador
d) contato do controlador
e) Possível compartilhamento dos dados pelo controlador e a finalidade
f) Os outros direitos fixados no artigo 18 da LGPD

Perspectivas e Desafios

 # Consentimento

@ Cuidado:

a) Necessidade de confirmação do consentimento caso houver mudança da finalidade para o tratamento de dados pessoais e esta não seja compatível com o consentimento original (aviso prévio e que autoriza a revogação do consentimento)

b) Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato.

Perspectivas e Desafios

 # Bases legais: Consentimento

@ Repetindo:

- Escrito ou outra forma capaz de demonstrar a manifestação de vontade
- Livre e esclarecido e especificado (consentimento genérico é nulo)
- Deve constar de cláusula destacada das demais
- Ônus de licitude do consentimento é do controlador
- Revogável
- Necessidade de atualização em casos de mudança da finalidade

Perspectivas e Desafios

 # Cumprimento de obrigação legal

@ Obrigatoriedade em virtude de outros elementos regulatórios como por exemplo:

- Provedores de aplicação: Registros de acesso a aplicação (MCI, art. 15)
- Empregadores (E-social*)
- Operadoras de saúde (ANS)

Obs**.: Cumprimento das outras obrigações estabelecidas pela LGPD, tais como tratamento de forma segura e vinculada a finalidade, mapeamento das operações e garantia do exercício de seus direitos.**

Perspectivas e Desafios

Elementos regulatórios – aspectos legais

@ Identificar as bases legais sustentando o tratamento de dados pessoais:

. Legítimo interesse e os riscos inerentes a essa abordagem!

. A necessidade do RIPDP

Perspectivas e Desafios

Elementos regulatórios – aspectos legais

@ Cumprir as obrigações legais vinculadas ao tratamento. Por exemplo:

. Mapeamento das operações de tratamento
. Notificações de privacidade
. Direito dos titulares

Perspectivas e Desafios

Cumprir as obrigações legais: Registro e transparência – mapas de OTDP

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

@ Necessidade de conhecer quais os dados tratados e quais as operações de tratamento realizadas:

- Inventário dos dados pessoais
- Mapa de tratamento de dados pessoais
- Data flows (Fluxo de dados) e DLM (Ciclo de vida do dado)

Perspectivas e Desafios

Cumprir as obrigações legais: Registro e transparência – mapas de OTDP

@ Mapas devem conter:

- Tipo de dado pessoas
- Titular do dado pessoal
- Finalidade do tratamento
- Base legal para o tratamento
- Onde o tratamento é realizado
- Quem é responsável pelo tratamento
- Outras informações.

Perspectivas e Desafios

Cumprir as obrigações legais: Registro e transparência – mapas de OTDP

Descrição da Atividade	
Dados pessoais tratados	
Finalidade do tratamento	
Titulares dos dados tratados	
Mecanismos de processamento	
Destinatários dos dados pessoais	
Responsável pelo tratamento	

Perspectivas e Desafios

Cumprir as obrigações legais: RIPDP (Relatório de impacto à proteção de dados pessoais)

@ Em que consiste o RIPDP?

. documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco

Perspectivas e Desafios

Cumprir as obrigações legais: RIPDP (Relatório de impacto à proteção de dados pessoais)

@ Estrutura:

. Descrição dos tipos de dados coletados

. Descrição da natureza, o escopo, o contexto e os propósitos do tratamento

. Avalia a necessidade, a proporcionalidade e a adequação do tratamento

. Identifica e avalia os riscos para os titulares dos dados

. Indica medidas de segurança e mecanismos de mitigação de risco adotados

Perspectivas e Desafios

RIPDP (Relatório de impacto à proteção de dados pessoais)

@ Deve-se considerar a elaboração de um RIPDP quando se pretende

. Realizar avaliação ou pontuação de sujeitos
. Realizar tomada de decisão automatizada com efeitos significativos
. Realizar monitoramento sistemático
. Tratar dados sensíveis ou dados de natureza altamente pessoal
. Tratar dados pessoais em larga escala
. Tratar dados pessoais de sujeitos vulneráveis
. No desenvolvimento de soluções tecnológicas ou organizacionais inovadoras

Perspectivas e Desafios

RIPDP (Relatório de impacto à proteção de dados pessoais)

@ Deve-se obrigatoriamente elaborar um RIPDP quando se pretende

. Monitorar sistematicamente um local publicamente acessível
. Tomar decisões sobre o acesso de alguém a um serviço ou benefício
. Tratar dados biométricos ou genéticos
. Combinar, comparar ou associar dados de várias fontes
. Tratar dados pessoais envolvendo o rastreamento de localização
. Tratar dados pessoais envolvendo comportamento on-line ou off-line
. Tratar dados pessoais das crianças para criar perfis

Perspectivas e Desafios

Elementos regulatórios – tecnologia da informação

@ Cumprir as obrigações técnicas:

. Políticas e mecanismos de segurança
. Notificações de incidentes de segurança (Data Breachs)
. Transferências internacionais de dados pessoais

Perspectivas e Desafios

Seguranca e Resposta a Incidentes

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional

A) a descrição da natureza dos dados pessoais afetados;

B) as informações sobre os titulares envolvidos;

C) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

D) os riscos relacionados ao incidente e as medidas que foram adotadas para reverter ou mitigar os efeitos do prejuízo.

Perspectivas e Desafios

 # Transferência internacional de dados pessoais

A) para países ou organismos internacionais com mesmo grau de proteção;

B) Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, 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

Perspectivas e Desafios

Transferência internacional de dados pessoais

C) 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;

D) Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

E) Quando a autoridade nacional autorizar a transferência ou quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

G) Quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

H) 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; ou

Adequação

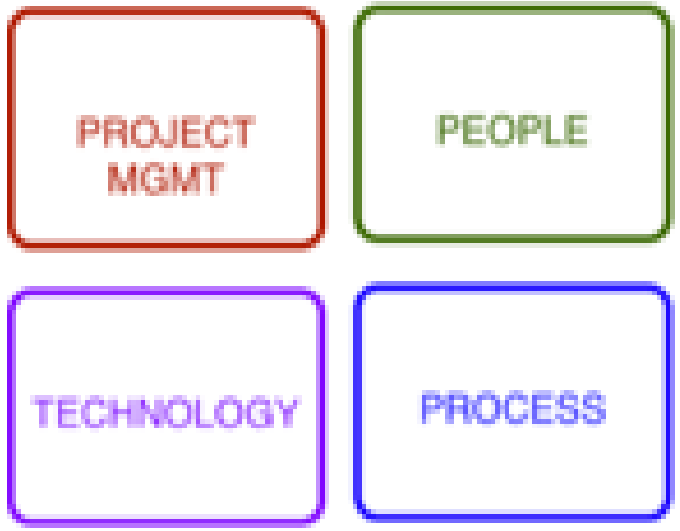
E como faço para me adaptar a esse novo paradigma?

Compreender os sistema regulatório				
Desenvolver um framework de trabalho customizado	Estruturar e gerenciar mudanças de governança	Desenvolver e implantar controles técnicos, administrativos, legais e organizacionais	Fomentar rotinas orgânicas e capilarizadas entre setores	Instituir sistema de governança de conformidade

Adequação

 # E como faço para me adaptar a esse novo paradigma?

@ Quatro vetores



Adequação

Design do processo

@ Top down/feet on the ground?

@ Multidisciplinar

@ PMO

@ Gap analysis

@ Risk assessment

@ Desenho

Adequação

Roadmap do processo de adequação a LGPD

Adequação

 # Vetores de adequação a LGPD

Proteção dos dados pessoais de

@ Riscos e vulnerabilidades associadas a proteção da informação

@ Riscos e vulnerabilidades regulatórios decorrentes dos direitos e , garantias dos titulares dos dados pessoais tratados

e

Abordagem sistêmica do ecossistema de tratamento de dados pessoais

@ Atividades isoladas

@ Ecossistema de tratamento

Adequação

Lei Federal 13.709/18 (LGPD)

Lei Federal 12.846/13 (Lei do Compliance)

Normas ISO 27001 (Segurança da Informação)

Norma ISO 29134:2017 (Privacy Impact Assesment)

Norma ISO 31000:2017 (Risk Management)

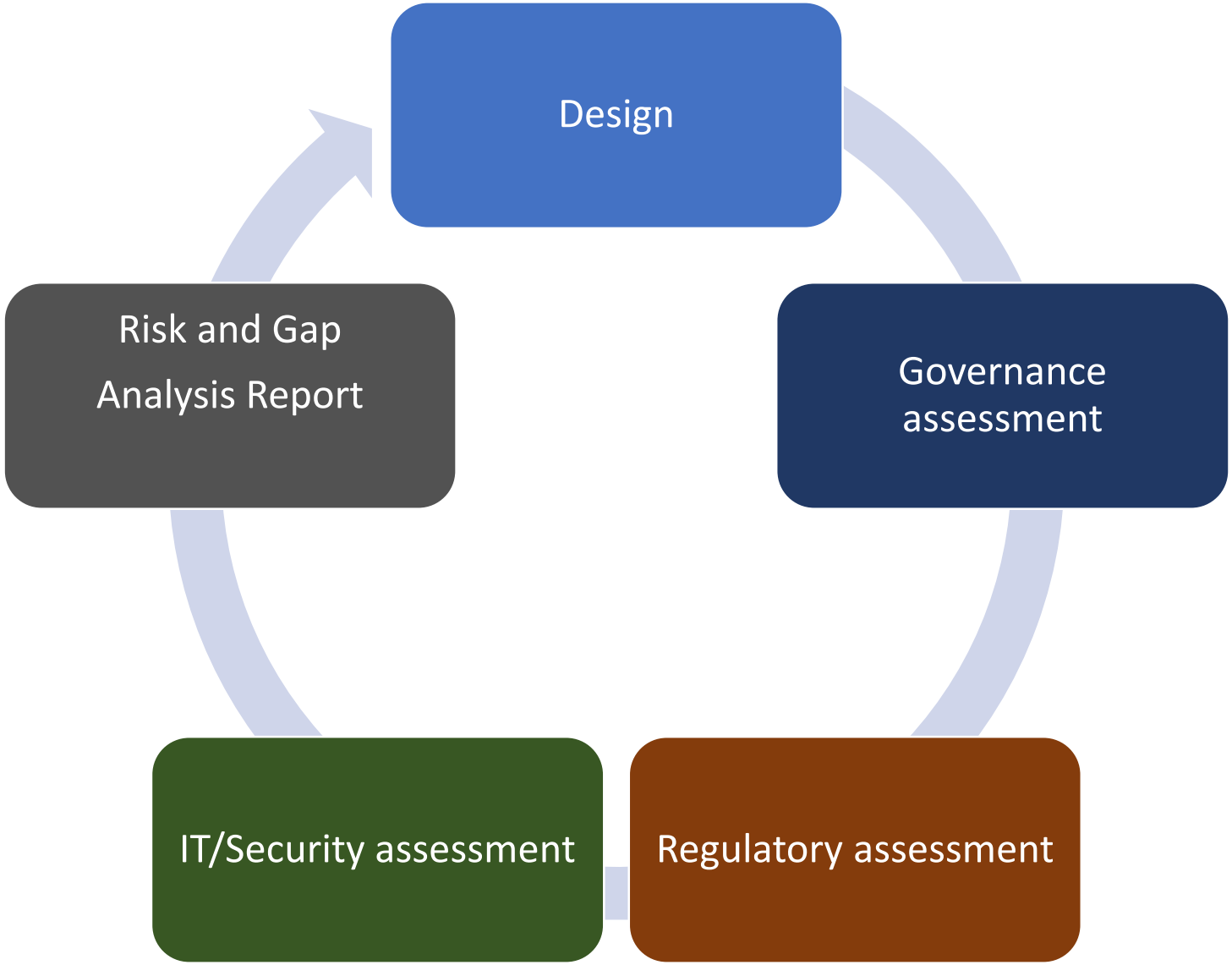
General Data Protection Regulation – GDPR (EU 2016/679)

Manuais de boas praaticas e guidelines da Agencia Espanhola de Proteção de Dados Pessoais – AEPD

Manuais de boas práticas e guidelines do Information Commissioner's Office – ICO

Manuais de boas práticas e guidelines da European Union Agency for Cybersecurity - ENISA

Adequação


Design
Governance assessment
Regulatory assessment
IT/Security assessment
Risk and Gap Analysis Report

Adequação

Uso da taxinomia de gestão de dados pessoais desenvolvida por Kemp (2014)

Nível 1: infraestrutura da plataformas	Nível 2: arquitetura da informação	Nível 3: propriedade intelectual e dados
Nível 4: Contratos aplicados aos dados	Nível 5: Regulamentação dos dados	Nível 6: Gerenciamento de informações e seguranca da informação

Adequação

 # O processo de adequação busca

- Identificar situações de vulnerabilidade e não adequação a LGPD
- Apontar e implantar medidas legais, organizacionais e técnicas de correção
- Estabelecer rotinas de monitoramento e compliance a LGPD

@ Fases:

- Diagnóstico, Adequação e Validação

Adequação

 # Processo e entregáveis:

1) **Diagnóstico**

1.1 Atividade: Averiguação preliminar de adequação a LGPD

Produto: Relatório preliminar de Compliance a LGPD

Adequação

 # Processo e entregáveis:

2) **Adequação:**

2.1 Inventário e mapeamento dos dados e das atividades de tratamento.
Produtos: Inventário de dados pessoais
Mapa de registro de atividades de tratamento.

2.2 Análise do ecossistema de tratamento de dados (aspectos técnicos e legais).
Produtos: Catálogo de atividades de tratamento
Relatório preliminar de Compliance com a LGPD (Risk Assessment)

Adequação

 # Processo e entregáveis:

2) **Adequação:**

2.3 Elaboração do programa e da política de governança de proteção a dados pessoais

Produtos: Programa de governança em proteção de dados pessoais

Política de proteção de dados pessoais

2.4 Elaboração de relatórios de impacto para a proteção de dados pessoais – (RIPD)

Produtos: Relatórios de impacto para a proteção de dados pessoais

Adequação

 # Processo e entregáveis:

2) **Adequação:**

2.5 Elaboração e revisão de documentos jurídicos

Produtos: Termos de consentimento

Termos de uso

Políticas de privacidade e segurança

Política de utilização de recursos tecnológicos

Contratos e aditivos

Adequação de mecanismos relacionais e contratuais

Adequação

 # Processo e entregáveis:

2) **Adequação:**

2.6 Implantação de rotinas e processos administrativos e operacionais
Produtos: Relatório de acompanhamento

2.7 Implantação de ferramental técnico de apoio (softwares e aplicações)
Produtos: Relatório de acompanhamento

2.8 Auditagem da garantia de exercício dos direitos do titular dos dados
Produtos: Relatório de acompanhamento

Adequação

 # Processo e entregáveis:

2) Adequação:

2.9 Treinamento

Produtos: Cursos

Workshops

Certificações

3) Validação:

Produtos: Relatório de adequação

Relatório de rotinas de monitoramento

Proposta de atividade de Encarregado de Proteção de Dados Pessoais

Adequação

@ Frameworks de adequação (IBM Approach)

Entenda as obrigações

Familiarize-se com os requerimentos propostos na LGPD e monitore o desenvolvimento da implementação

Estabeleça uma equipe multidisciplinar

Assegure que todos os aspectos do negócio, impactados pela Lei, estejam incluídos nos planos de implementação das mudanças

Nomeie um *Data Protection Officer*

Estabeleça um escritório de privacidade e nomeie um responsável especialista tanto no tema quanta nos requisitos das leis.

Saiba onde estão os dados pessoais na sua organização

Conduza um inventário de dados e um mapeamento do fluxo da informação para auxiliar na avaliação das alterações operacionais e tecnológicas requeridas para o cumprimento da Lei.

Reveja as declarações e as políticas de privacidade

Confirme que as notificações de privacidade são apresentadas em linguagem clara e transparente e facilmente acessíveis pelo Titular

Reveja os mecanismos de consentimento e opção

Assegure que mecanismos apropriados de consentimento e opção atendem aos requerimentos da Lei, sendo de fácil acesso e uso pelos Titulares.

Revise os processos para atendimento dos pedidos de acesso, correção e eliminação dos dados

Confirme que medidas operacionais e técnicas estejam acessíveis para atender aos pedidos dos Titular

Revise os prazos de retenção de dados

Confirme que os dados são mantidos somente pelo prazo requerido pelo negócio ou requeridos por leis.

Adequação

@ Frameworks de adequação (IBM Approach)

Documente as atividades de cumprimento da Lei

Documente adequadamente todos os processos operacionais que envolvam dados pessoais através do uso de Avaliações de Impacto e Riscos à Proteção dos Dados

Reveja processos de transferência internacional de dados

Confirme a existência de bases legais para transferência internacionais de dados com regimes de proteção de dados compatíveis aos requeridos na Lei.

Implemente e documente medidas apropriadas de segurança

Providencie medidas técnicas, físicas e administrativas apropriadas para a mitigação dos riscos.

Treine os colaboradores

Assegure que os colaboradores sejam periodicamente treinados sobre os requerimentos e obrigações relacionadas a proteção de dados

Desenvolva processos especializados de auditoria

Estabeleça um planejamento robusto de auditoria e monitoramento constante para identificação tempestiva e mitigação dos riscos internos e nos Operadores

Implemente uma abordagem de Privacidade (e Segurança) *by Design*

Estabeleça um modelo de Privacidade *by Design* para assegurar que os requerimentos sejam atendidos desde os estágios iniciais do desenvolvimento de produtos, sistemas e serviços

Estabeleça protocolos de resposta e notificação de violações de segurança

Implemente processos de investigação, contenção e resposta a violações de segurança. Assegure a efetividade dos mesmos através de testes periódicos.

Assegure orçamento e patrocínio executivo para suportar as mudanças!

Adequação

@ Frameworks de adequação (EY Approach)

Governance:	Use of data:	Validation:
Accountability and compliance	Consent and privacy notification	Contract management
Privacy and security by design	Data protection	Third-party risk management
Privacy data assessment (appropriate collection & use)	Data rights management	Internal and external assurance
Incident and breach management	Records management	Continuous monitoring and improvement

Considerações finais

Não subestimar a complexidade das mudanças

Construir o ambiente propício a adequação

Enfrentar os desafios com expertise técnica e simplicidade

Obrigado

joao@origamisec.com.br
joao@cmslaw.com.br
85 99812 6572

R. Francisco Paracampos, 55
Fortaleza - CE

lgpd@origamisec.com.br
(85) 3535-6262

ORIGAMI
cybersecurity