Os desafios da implantação da LGPD para os órgãos públicos

Lílian Gibson

Coordenação do Gt-SI ABEP-TIC

Gestão da Qualidade e SI PRODAM

50 ANOS PRODAM

AMAZONAS
GOVERNO DO ESTADO

Sumário

ARCABOUÇO LEGAL

APOIO DOS ESTADOS NA BUSCA DE CONFORMIDADE

REQUISITOS ESSENCIAIS

REFERÊNCIAS PARA A BUSCA DA CONFORMIDADE

AVALIAÇÃO DE FERRAMENTAS DE APOIO

BALANÇO DE 2 ANOS DE GDPR E INÍCIO DA LGPD

Leis e regulamentos setoriais de privacidade e proteção de dados

Lei	Nome	
Constituição da República Federativa do Brasil/1988	Constituição Federal – Art.5º, XXXIII	
Lei 8.078/1990	Código de Defesa do Consumidor (CDC)	
Lei 12.965/2014	Marco Civil da Internet (MCI)	
Lei 12.527/2011	Lei de Acesso à Informação (LAI)	
Lei 12.414/2011	Lei do Cadastro Positivo	
Lei 13.709/2018	Lei Geral de Proteção de Dados Pessoais (LGPD)	

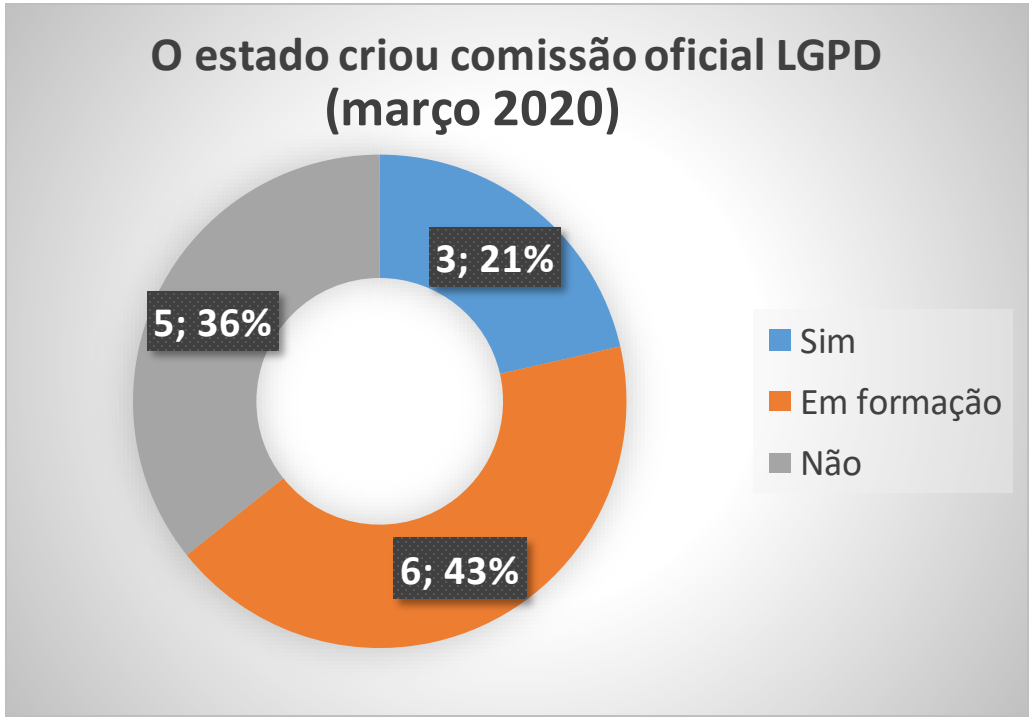
LGPD

- A Lei Geral de Proteção de Dados Pessoais é a **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018** que determina como os dados pessoais dos cidadãos, em papel ou meio digital, podem ser tratados na prestação de serviços e prevê punições para transgressões.

- Sancionada no dia 14 de agosto de 2018, a partir do Projeto Lei da Câmara 53/2018, para entrar em vigor em 2 anos.

- Alterações
  - Leis 13.853/2019 (MP 869/2018 - dispõe sobre a proteção de dados pessoais, cria a Autoridade Nacional de Proteção de Dados (ANPD))
  - Lei 14.010/2020 (sanções administrativas a partir de agosto de 2021)
  - Decreto 10.474/2020 (aprova a estrutura regimental e cargos da ANPD)
  - Lei 14.058/20 (MP 959/2020 - vigência a partir de 18/09/2020).

Apoio dos estados nos processos de busca de conformidade



Requisitos Essenciais de Conformidade

Respaldo Legal,
Consentimento,
Revisão de contratos,
Transparência,
Direitos do titular

REGRAS CLARAS

[Pautadas em leis e regulações especiais]

SEGURANÇA CIBERNÉTICA

[Vigilância, monitoramento e documentação das evidencias com ferramentas – provas]

Documentos de SI e privacidade,
Inventário de dados,
Análise de riscos,
Plano de ação para SI,
Implantação de controles

Monitoramento,
ETIR,
DPIA,
Notificação,
Auditoria

PLANO DE RESPOSTA A INCIDENTES

[Rapidez e rigor nas ações]

EDUCAÇÃO DIGITAL

[Adotar a prevenção como estratégia de negócio]

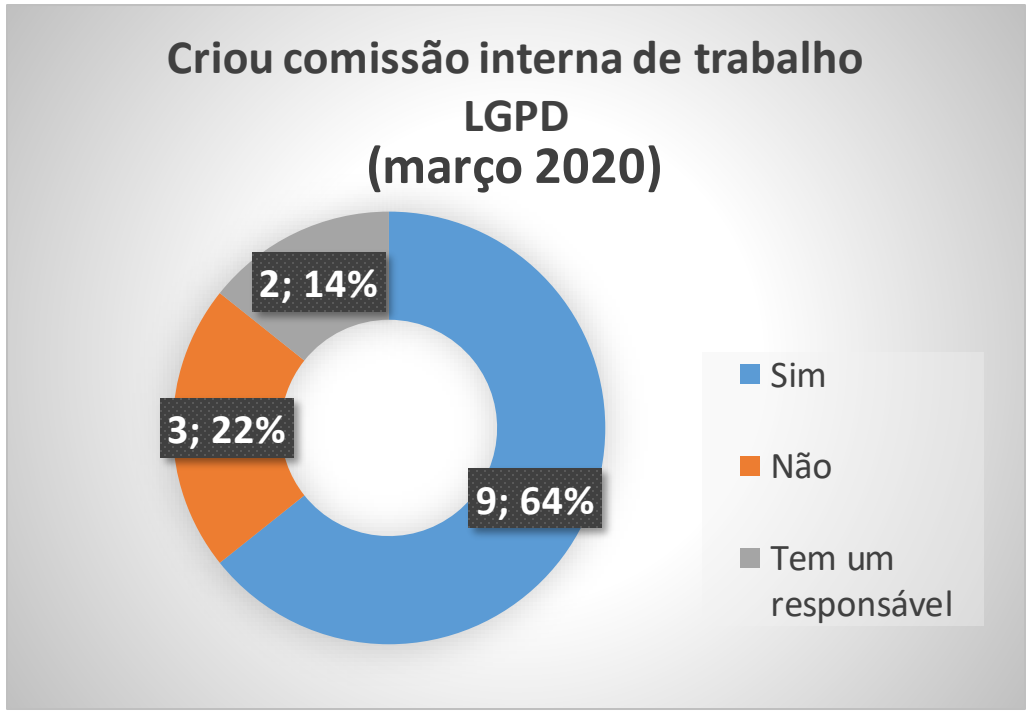
Indicação do encarregado,
Capacitação,
Certificações

Desafio 1: Apoio estadual e organizacional

- Recomendar a criação de grupo de trabalho LGPD
  - Capitanear a definição do modelo de governança de dados pessoais estadual
    - CGE, PGE, Educação, Trânsito, Saúde, Administração, Ciência e tecnologia, Segurança Pública, Fazenda, Empresa de processamento de dados, etc.
- Inclusão de ação para conformidade com a SI/LGPD na Estratégia / PPA
  - Prever orçamento comum para ferramentas de SI e governança de dados pessoais para os órgãos
- Considerar a necessidade de contratação de consultoria para todos os órgãos
- Promover padronização de processos comuns, política privacidade e SI
- Promover eventos de conscientização e treinamentos

ÁREAS IMPACTADAS

Comissão de LGPD interna



Consultoria

Principais Sujeitos

- **Titular dos dados (*data subject*).**
- **Controlador** (*controller*).

Todos os órgãos – Responsabilidade Jurídica

- ***Operador ou processador*** (*processor*).

  Todos os prestadores de serviços para os órgãos que tratam dados pessoais (responsabilidade compartilhada)

- Controlador + Operador = **Agentes de tratamento de dados**.
- **Encarregado de proteção de dados (*data protection officer - DPO*).**

Órgãos Estaduais
Como indicar?

SEDUC/AM
SECRETARIA DO ESTADO DE EDUCAÇÃO

GOVERNO DO ESTADO DO AMAZONAS
SEMA
SECRETARIA DE ESTADO DO MEIO AMBIENTE

PRODAM
TECNOLOGIA EM SUA VIDA

Desafio 2: Nomear um encarregado pelo tratamento de dados pessoais

- Conceito
  - Art. 5º, inc. VIII - 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 (ANPD).
- Indicação obrigatória
  - Art. 5º, inc. VIII: controlador ou operador;
  - Art. 23, caput + inc. III: pessoas jurídicas de direito público referidas na LAI;
  - Art. 41, caput + § 1º + § 2º, IV: controlador.

Encarregado pelo tratamento de dados pessoais

- dedicação exclusiva;
- não ter conflito de interesses;
- reportar-se à alta gestão;
- atuar interdisciplinarmente, emprestando conceitos das áreas jurídica, de TI, SI, gestão de processos, negócio
- possuir boa comunicação e abertura para circulação

Responsabilidades

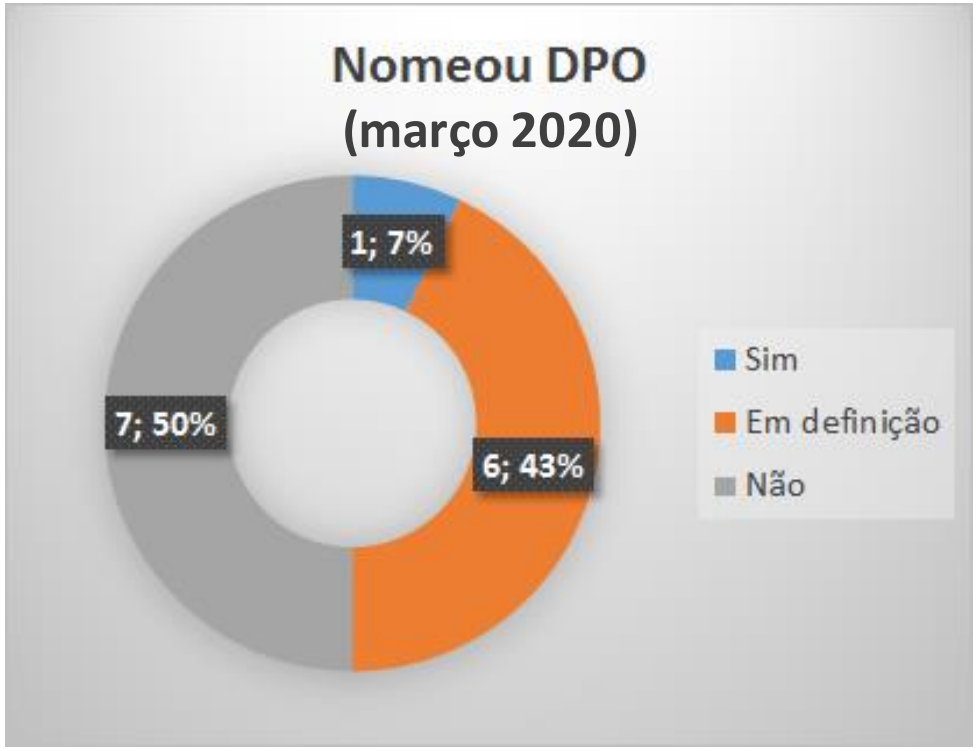
Órgãos Estaduais

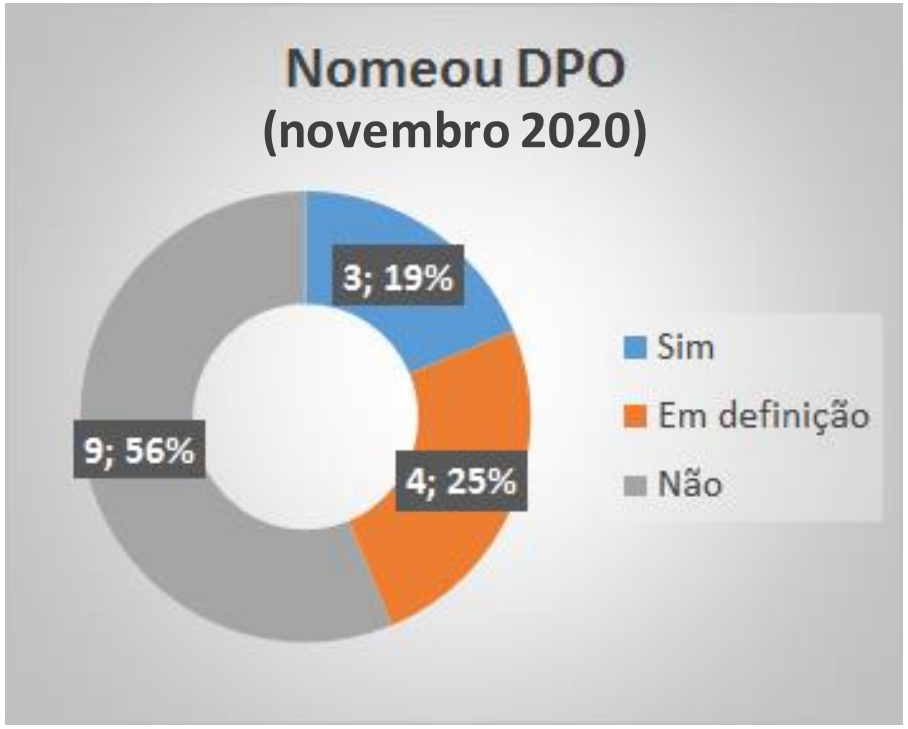
- Em **regra**, só o **controlador** responde;

Prestadores de Serviço (Fornecedores, ...)

- **Responsabilidade excepcional do operador (art. 42, § 1º, I);**
- **Se descumprir obrigações legais da LGPD ou não seguir instruções explícitas do controlador;**
- Responsabilidade **objetiva** (art. 43 e 44);
- DPO **não tem responsabilidade** por atos do controlador ou do operador (art. 42, *caput* e 43, *caput*).

Nomeou encarregado de proteção de dados





Desafio 3: Adotar um roteiro e/ou framework para buscar a conformidade

- LGPD com várias lacunas;
- Autoridade Nacional de Proteção de Dados (ANPD) criada depois de 02 anos;
- Adotar roteiros propostos por órgãos públicos ou especialistas em direito digital
- Adotar normas de SI
  - ISOs 27.001, 27.002, 27.005, 27.701
- Adaptar modelos da GDPR
- Framework de Direito Digital ABEP-TIC

Roadmap LGPD GT-SI – Visão Geral

1. Treine e conscientize
2. Estabeleça rede de apoio
3. Estruture o novo desafio
4. Estabeleça o DPO
5. Inventarie os dados pessoais
6. Formalize o DPIA

Entenda → **Planeje** → **Avalie Riscos**

7. Revise a documentação institucional
8. Implemente o plano de redução dos riscos
9. Formalize o canal de comunicação institucional
10. Estabeleça Privacy by Design
11. Fortaleça a equipe de SI
12. Audite e reavalie

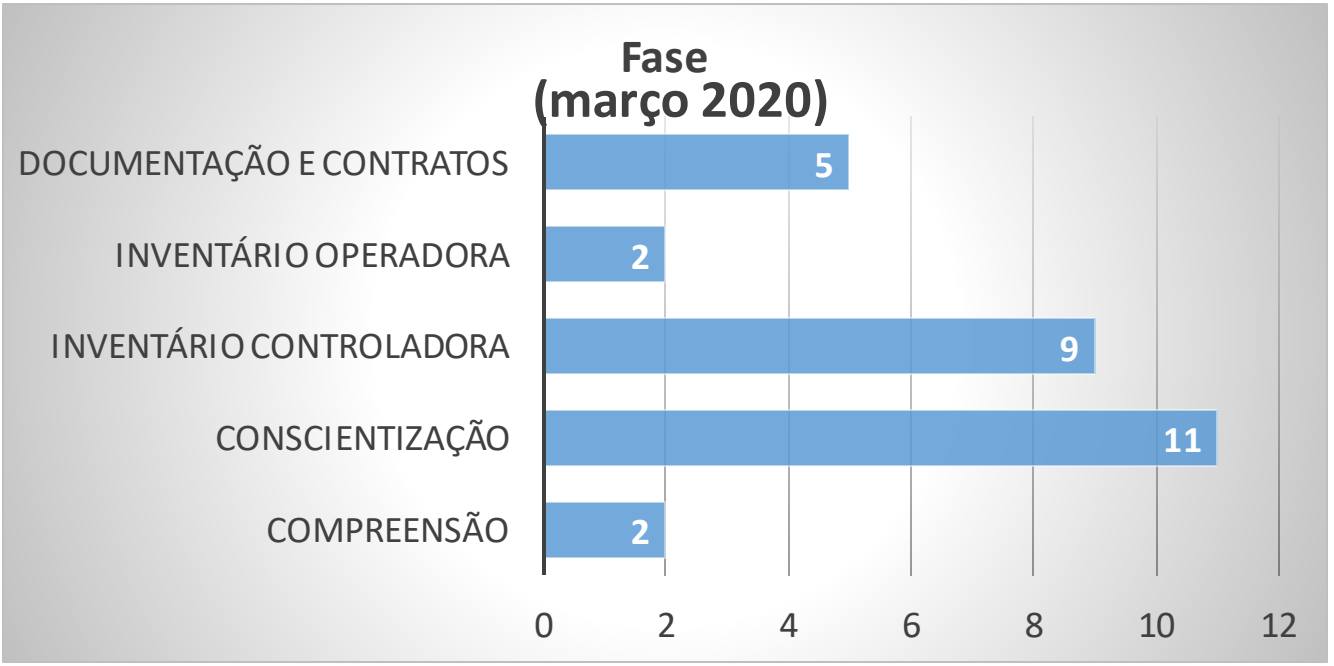
Reduza riscos → **Organize** → **Avance**

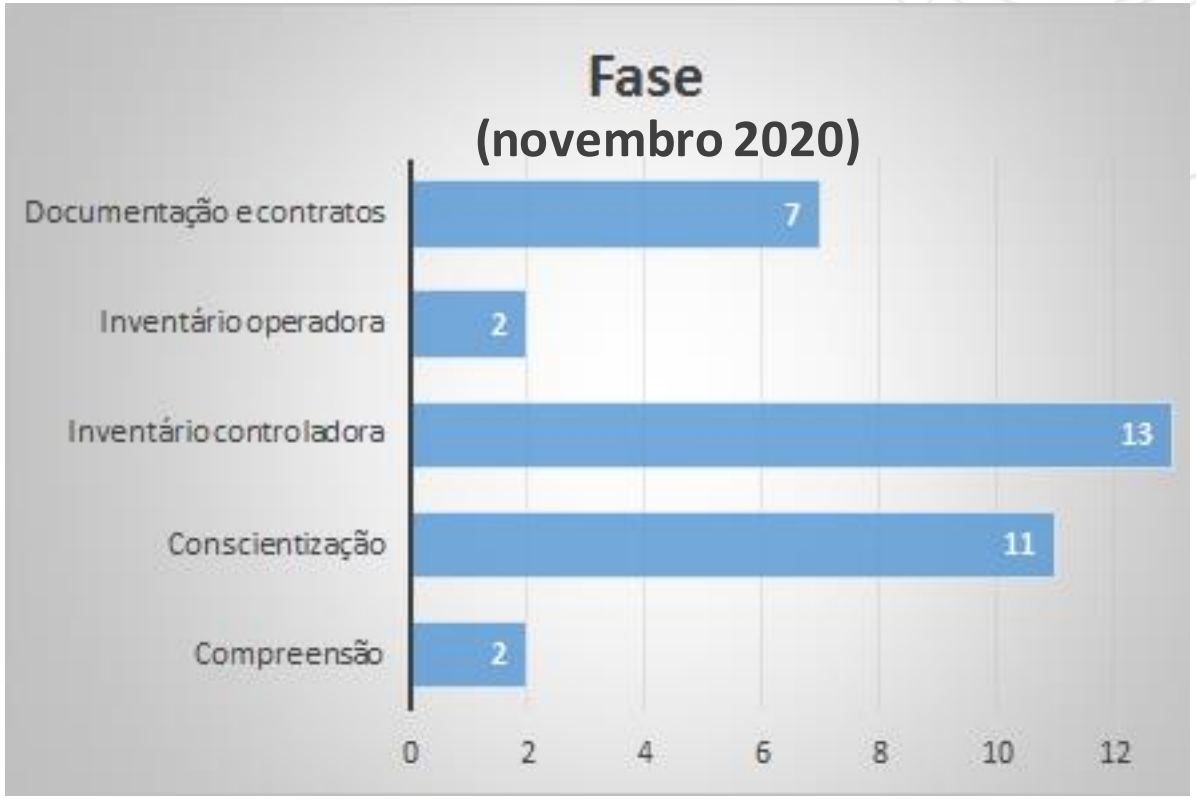
Nível de maturidade em LGPD

	ISO 21827:2008	Definições
0	Não Realizado	Não há **controles de segurança ou planejamento** em andamento. Os controles não existem.
1	Executado Informalmente	Práticas básicas das áreas de controle sã[illegible] forma geral, executadas em base **ad hoc**. Há um acordo gera[illegible] organiza[illegible] as a[illegible]es que deveriam ser executadas, e as mesmas são exe[illegible] [illegible]áticas não são formalmente implem[illegible] [illegible]ssadas.
2	Planejado	Os requisito[illegible] [illegible]nejados, implementados e **repetíveis.**
3	Bem definido	A prin[illegible] [illegible]do e Rastreável, é que além de ser **repetível** [illegible]o: **documentado, aprovado e implementado e com[illegible]**
4	Controlado Quantitativamente	A principal difere[illegible]ça em relação ao Nível 3, Bem Definido, é que o processo é **mensurável e pode ser comprovado** (ex., é auditável)
5	Melhorado Continuamente	A principal diferença em relação ao Nível 4, Controlado Quantitativamente, é que o processo definido e padronizado é, **regularmente revizado e melhorado**. As melhorias refletem um entendimento de, e resposta para, os impactos das vulnerabilidades.

0-5

Fase atual


Fase
(março 2020)
DOCUMENTAÇÃO E CONTRATOS
INVENTÁRIO OPERADORA
INVENTÁRIO CONTROLADORA
CONSCIENTIZAÇÃO
COMPREENSÃO
5
2
9
11
2
0
2
4
6
8
10
12


Fase
(novembro 2020)
Documentação e contratos
Inventário operadora
Inventário controladora
Conscientização
Compreensão
7
2
13
11
2
0
2
4
6
8
10
12

Desafio 4: Garantir respaldo legal e transparência

- Regras do tratamento de dados pelo Poder Público

Dever de informação qualificada (art. 23 – CAPÍTULO IV);

I - informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, **preferencialmente em seus sítios eletrônicos**;

Carta de serviços

Impacto em todos os órgãos estaduais

Desafio 5: Garantir os direitos do titular - Artigo 18º

O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

15 dias para responder I e II

I - confirmação da existência de tratamento

II - acesso aos dados

III - correção de dados

IV - anonimização, bloqueio ou eliminação de dados

V - portabilidade dos dados a outro fornecedor de serviço

VI - eliminação dos dados pessoais

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento

Desafio 6: Garantir os direitos do titular

- Mapeamento de processos de negócios;
- Inventário de dados pessoais informatizados ou não;
- Identificação dos riscos;
- Elaboração dos relatórios;
- Criação de processos de atendimento aos direitos do titular;
- Adoção dos conceitos de "Privacy by Design";
- Eliminação de dados.

Regras de tratamento de dados pessoais pelo Poder Público

- Princípios da LGPD (art. 6º – CAPÍTULO I);
  - Em regra, dispensa o consentimento do titular.

- Regras para Uso Compartilhado de dados pelo poder público a privados (Art. 26 – Cap IV)
  - Regra: vedação!
  - *execução descentralizada de atividade pública;*
  - *quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres*

Consentimento da criança

- Capítulo II

Art. 20. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Não podem ser repassados para terceiros

Desafio 6: Revisar contratos

- Incluir cláusulas que garantam a conformidade com a LGPD;
- Reajustar valores;
- Garantir o atendimento aos direitos do titular com fornecedores;
- Definir responsabilidades.

Desafio 7: Detectar e notificar incidentes de SI que envolvam dados pessoais

- Identificação dos riscos;
- Manutenção de logs por temporalidade legal;
- Monitoramento contínuo;
- Gestão de vulnerabilidades;
- Identificação proativa do incidentes de SI;
- Adoção dos conceitos de "Security by Default".

Desafio 8: Sanções para os órgãos públicos

- 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:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

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;

Desafio 8: Sanções para os órgãos públicos

X - (Mantido VET 24/2019) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)

XI - (Mantido VET 24/2019) suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)

XII - (Mantido VET 24/2019). proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

Responsabilidade Social

- Hipótese: Uma empresa vazou os dados de um indivíduo qualquer que continha no banco de dados
  - o setor responsável foi o de processamento da folha de pagamento
  - a empresa não tem um projeto de governança de dados
  - não há uma preocupação em adequação à LGPD
  - o indivíduo afetado, sofreu fortes prejuízos financeiros com tal atitude da organização

➢ É provável que as sanções de multa financeira sejam extremas se houver envolvimento de empresa privada

➢ É provável que o gestor responda por improbidade administrativa

➢ Pode haver sanção de bloqueio parcial ou total do banco de dados da folha de pagamento até que a situação seja regularizada e haja uma prova de contenção de vazamento.

➢ Percebe-se o perigo de uma situação dessas? Uma organização com o setor de processamento da folha sem devido funcionamento, por um dia que seja?!

Reputação

Prejuízo para a imagem

Atenuantes para as sanções

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Algumas referências para busca de conformidade

- Frameworks
  - NBR ISO 27.002:2013 – Tecnologia da Informação – Código de prática para controles de segurança de informação;
  - NBR ISO 27.018 – Tecnologia da Informação – Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas que atuam como processadores de PII;
  - NBR ISO 27.701:2019 – Gestão da Privacidade da Informação;
  - NBR ISO 16.167:2013 – segurança da Informação - Diretrizes para classificação, rotulação e tratamento da informação.
  - Privacy by Design - Ann Cavoukian, Ph.D. - https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf
- Guias
  - Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD) - Setor Público Federal (Governo Federal) - https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd
  - Diagnóstico de Adequação à LGPD - https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd
  - Guias Operacionais para adequação à LGPD - https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd
  - Guia para LGPD na Advocacia - http://www.oabdf.org.br/wp-content/uploads/2020/10/GUIA%20LGPD%20PARA%20A%20ADVOCACIA%20OABDF%20OUTUBRO2020.pdf

Algumas referências para busca de conformidade

- Políticas de Privacidade
  - Política de Privacidade (TJDFT) - https://www.tjdft.jus.br/ouvidoria/protecao-de-dados-pessoais/politica-de-privacidade
  - Política Estadual de Proteção de Dados Pessoais (PEPD) - Governo de Pernambuco - https://legis.alepe.pe.gov.br/texto.aspx?id=51399
- Segurança da Informação
  - http://dsic.planalto.gov.br/assuntos/editoria-c/instrucoes-normativas
  - Estratégia Nacional de Segurança Cibernética - https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419
- Framework de Direito Digital ABEP-TIC

Critérios de avaliação de ferramentas para apoio à LGPD

Lei 13.709	Fase Roadmap GT-SI	Requisitos da ferramenta
Art. 1- 21, 33, 36-51	3.6. Crie o processo de governança de dados pessoais	1. Programa de governança de dados pessoais
	5.2. Faça analise de riscos do vazamento	1.1. Gestão de riscos
	5.1. Inventarie os dados pessoais	1.2. Mapeamento/documentação de fluxo de processos/negócios que trata dado pessoal
	5.9. Monitore e reavalie	1.3 Auditoria
Art 32o		1.4. Relatório de DPIA
		1.5 Integração com a Estratégia/SWOT
		1.6. Indicadores de desempenho
		1.7 Gestão de fornecedores
		1.8 Maturidade em SI
		1.9. Gestão de vulnerabilidades de exposição de dados pessoais

Lei 13.709	Fase Roadmap GT-SI	Requisitos da ferramenta
Art 46o	5.1. Inventarie os dados pessoais	2. Mapeamento de dados pessoais
Art. 6-8, 15, 19, 33, 37		2.1. Estruturado (Data discovery)
Art. 6-8, 15, 19, 33, 37		2.2. Não estruturado (Data Mapping)
		API de integração
		2.3. Atualização periódica do inventario
		2.4. Qualifica o dado pessoal
		2.5. Elaboração de questionarios
		2.6 Permite documentar a base legal
Art. 6, 9, 15, 18-21, 50	5.6.1 Defina como se dará o atendimento a solicitação do Titular (e ANPD)	3. Portal de comunicação para atendimento ao direitos do titular e DPO
		3.1. Autenticação dos titulares
		3.2. Consulta sobre existência do dado pessoal
		3.3. Correção do dado pessoal
		3.4. Canal com a ANPD

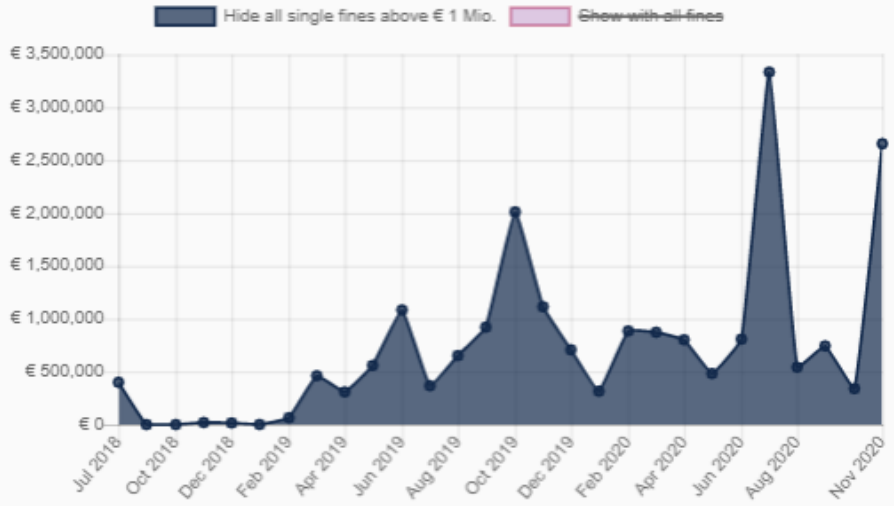
Critérios de avaliação de ferramentas para apoio à LGPD

Lei 13.709	Fase Roadmap GT-SI	Requisitos da ferramenta
		3.3. Correção do dado pessoal
		3.4. Canal com a ANPD
Art. 6-9, 11, 14-15, 18-19, 33		3.5. Gestão do consentimento
Art. 6-9, 11, 14-15, 18-19, 33		3.6 Gestão de cookies
		3.7 Gestão do compartilhamento do dado com terceiros
Art 48º	5.8. Estabeleca uma estrutura para monitorar o incidente	4. Geração de logs das operações com dados pessoais
		4.1 Registro do processamento
		4.2 Mapeamento de logs (busca?)
Art 46º	5.5. Implementar plano de redução de riscos	5. Gestão do plano de ação
		5.1 Criptografia
		5.1.1 A ferramenta disponibiliza um cofre para os dados pessoais estruturados - DB
		5.1.2 Do armazenamento dos dados pessoais não estruturados
		5.2. Do backup

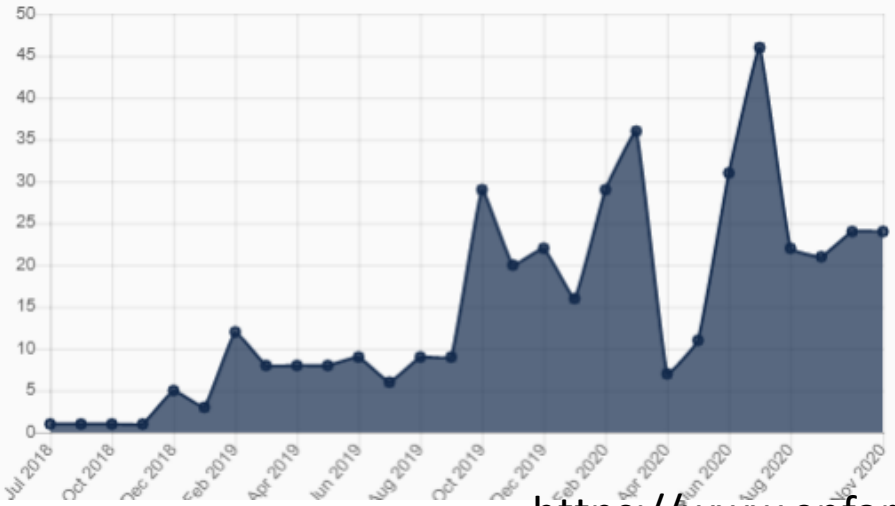
Lei 13.709	Fase Roadmap GT-SI	Requisitos da ferramenta
		5.2. Do backup
		5.3. Do canal de transferência do dados
		5.4 Do e-mail
		5.5. das senhas
		5.6 Anonimização
Art 48º	5.8. Estabeleça uma estrutura para monitorar o incidente	6. Rastreamento do incidente
		6.1 Registrar o incidente
Art 49º	5.5. Implementar plano de redução de riscos	7. Ferramenta
		7.1. DLP
		7.2 Ratreamento de cookies
Art 50º		8. Gestão de Documentos
		8.1. Modelos de documentos de SI
	5.3.2. Revise doc de SI	8.1.1 Política de privacidade
Art 50º	5.4. Revise documentos institucionais	8.1.2 Modelos de aditivos para contrato
		9. Privacy by Design

Balanço de 2 anos de GDPR

a) Sum of fines per month (non-cumulative):



b) Number of fines per month (non-cumulative):



Month	Sum of Fines (in month)	Number of Fines (in month)
Jul 2018	€ 400,000	1
Sep 2018	€ 300	1
Oct 2018	€ 388	1
Nov 2018	€ 20,000	1
Dec 2018	€ 15,700	5
Jan 2019	€ 50,000,888	3
Feb 2019	€ 65,108	12
Mar 2019	€ 462,300	8
Apr 2019	€ 309,135	8
May 2019	€ 559,526	8
Jun 2019	€ 1,084,550	9
Jul 2019	€ 367,575	6
Aug 2019	€ 3,252,835	9
Sep 2019	€ 921,523	9
Oct 2019	€ 34,512,374	29
Nov 2019	€ 1,114,800	20
Dec 2019	€ 12,207,530	22
Jan 2020	€ 28,116,160	16
Feb 2020	€ 886,090	29
Mar 2020	€ 5,873,600	36
Apr 2020	€ 802,200	7
May 2020	€ 483,400	11
Jun 2020	€ 2,048,308	31
Jul 2020	€ 20,034,548	46
Aug 2020	€ 542,948	22
Sep 2020	€ 743,900	21
Oct 2020	€ 78,095,408	24
Nov 2020	€ 18,563,701	24

Home License Privacy Imprint

https://www.enforcementtracker.com/

Motivo das infrações a GDPR

- Base legal insuficiente para tratamento de dados pessoais;
- Medidas técnicas e organizacionais insuficientes para garantir a segurança de dados pessoais;
- Não conformidade com os princípios de tratamento de dados pessoais;
- Colaboração ineficiente com a autoridade de proteção de dados;
- Vazamento de dados pessoais.

https://www.enforcementtracker.com/

Ação Civil Pública

MP DFT Ministério Público do Distrito Federal e Territórios

Unidade Especial de Proteção de Dados e Inteligência Artificial - Espec

Excelentíssima Senhora Juíza de Direito da ____ Vara Cível da Circunscrição Especial Judiciária de Brasília – DF

Excelentíssimo Senhor Juiz de Direito da ____ Vara Cível da Circunscrição Especial Judiciária de Brasília - DF

O **Ministério Público do Distrito Federal e Territórios**, por sua **Unidade de Proteção de Dados e Inteligência Artificial - Espec**, vem à presença de Vossa Excelência, com fundamento na Constituição Federal, Código de Defesa do Consumidor, Lei Geral de Proteção de Dados Pessoais e Lei da Ação Civil Pública, ajuizar

Ação Civil Pública
Com Pedido de Tutela de Urgência

MP DFT Ministério Público do Distrito Federal e Territórios

Unidade Especial de Proteção de Dados e Inteligência Artificial - Espec

II) Seja a ré **Infortexto LTDA** condenada a eliminar[17] todos os dados pessoais tratados de forma irregular, conforme diretrizes da Lei Geral de Proteção de Dados Pessoais - LGPD;

III) Seja o réu **Núcleo de Informação e Coordenação do Ponto BR** condenado a cancelar definitivamente o registro do domínio *lojainfortexto.com.br* vinculado à ré **Infortexto LTDA**;

IV) Seja o **Ministério Público do Distrito Federal e Territórios** intimado pessoalmente de todos os atos processuais;

V) Protesta, ainda, se assim for necessário, provar o alegado pela produção de todas as provas admitidas em Direito. Atribui-se à presente Ação Civil Pública o valor de R$ 1.000,00 (mil reais), para fins meramente fiscais.

Brasília/DF, 21 de setembro de 2020.

Frederico Meinberg
Promotor de Justiça
Coordenador da Espec

Obrigada

Lílian Gibson

lilian@prodam.am.gov.br

50 ANOS PRODAM

AMAZONAS
GOVERNO DO ESTADO