



DISPUTES AND INVESTIGATIONS CYBER RISK SERVICES

Nível de Maturidade do Mercado Brasileiro para a Lei Geral de Proteção de dados – LGPD

Outubro de 2020



Conteúdo

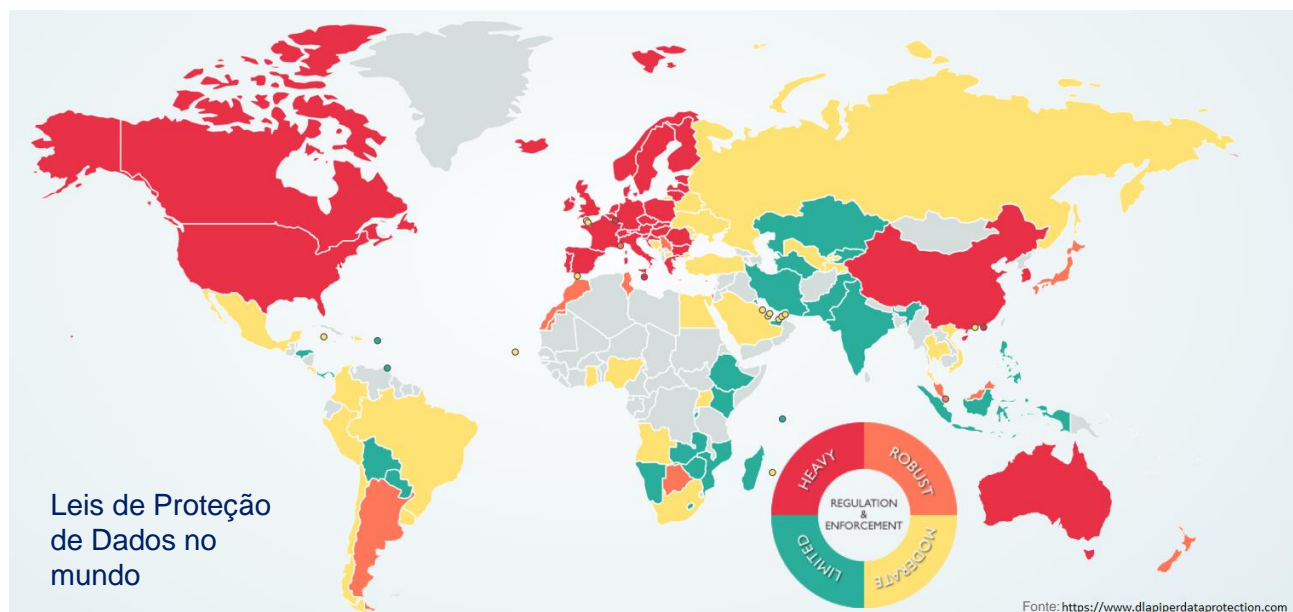
Contexto e Histórico da LGPD	[02]
Perfil das Organizações	[03]
Planejamento e Investimento	[04]
Governança e Cultura de Proteção de Dados	[05]
Atendimento aos Direitos dos Titulares	[07]
Relação Entre Controlador e Operador	[08]
Medidas de Proteção e Gestão de Incidentes de Segurança	[09]
Conclusão	[10]

LGPD – Histórico e Contexto

Após anos de discussões e da unificação de diversos projetos que tramitaram na Câmara, no Senado e no Ministério da Justiça, em 14 de agosto de 2018, a Lei Geral de Proteção de Dados do Brasil (LGPD), a Lei 13.709/2018 foi finalmente sancionada. A LGPD foi baseada na *General Data Protection Regulation* (GDPR), regulação europeia que quando surgiu em 2012 foi considerada pioneira e inspirou outros países, assim como o Brasil, a criarem suas próprias leis.

Além da Europa e dos Estados Unidos, diversos países da América Latina, como Chile, Argentina, Uruguai e Colômbia também possuem legislação de proteção de dados vigente.

A LGPD trouxe importantes discussões no Brasil sobre privacidade e proteção de dados. Na era da informação digital em que atualmente vivemos, as recorrentes notícias sobre espionagem, vazamento de dados e abuso na utilização de dados pessoais, aumentaram a conscientização sobre privacidade e proteção de dados e a lei vem justamente para empoderar o titular de dados e garantir a transparência e direito à liberdade e à privacidade. Com a LGPD nasce uma nova cultura e deve ser encarada pelas empresas como um aspecto diferenciador para a competitividade do negócio, capaz de transmitir uma imagem de confiança perante o mercado.

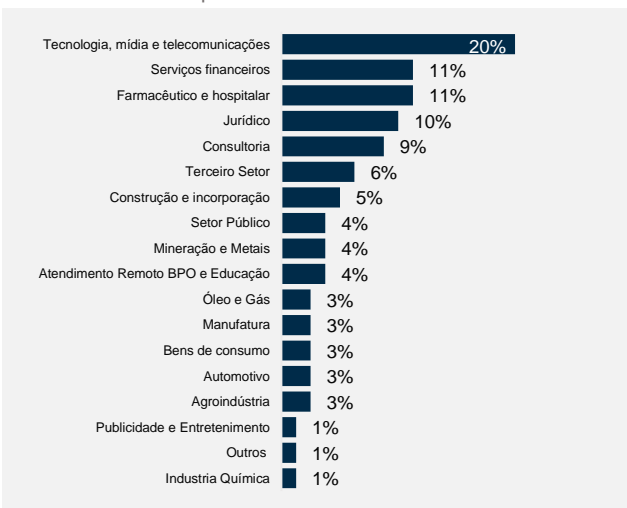


Principais Marcos de Privacidade e Proteção de Dados

Primeira lei sobre proteção de dados pessoais Publicada no Estado de Hesse, na Alemanha.	1970	2016	GDPR: General Data Protection Regulation Legislação é adotada para todos os países membros da UE.
Privacy Act Primeira lei sobre o uso de dados pessoais dos EUA.	1974	2018	Escândalo Cambridge Analytica Criação de perfis psicológicos a partir de coleta e tratamento de dados pessoais de usuários do Facebook.
Iniciativa Brasileira Consulta pública do Ministério da Justiça sobre anteprojeto de lei de proteção de dados pessoais.	2010	2018	Lei 13.709 – Proteção de Dados Regulamenta a proteção de dados pessoais no Brasil.
Lei 12.527 – Lei de Acesso à Informação Transparência de informações do poder público.	2011	2019	Criação da Agência Nacional de Proteção de Dados Com fins de regular e supervisionar a aplicação da Lei.
Publicação da proposta do GDPR Comissão Europeia publica a proposta	2012	2019	PL 5762/19 Propunha a prorrogação da data de entrada em vigor da LGPD para 15 de agosto de 2022.
Snowden e a NSA Divulgadas as práticas de espionagem e vigilância da NSA (National Security Agency)	2013	2020	Pandemia COVID-19 Câmara dos Deputados votou e aprovou a Medida Provisória 959/2020, que pretendia adiar a entrada da Lei Geral de Proteção de Dados (LGPD) para maio de 2021. A MP foi alterada propondo uma redução no adiamento, estabelecendo a vacatio legis para 31 de dezembro.
Lei 12.737 – Lei Carolina Dieckmann Invasão de aparelhos eletrônicos vira crime.	2012	2020	Sanção ou Veto Presidencial A LGPD entra em vigor assim que a 959/2020 for sancionada ou vetada pelo presidente Jair Bolsonaro — independentemente de sua escolha, o regulamento entrará imediatamente em vigor.
Lei 12.965 – Marco Civil Teve como uma das premissas o direito à privacidade.	2014		

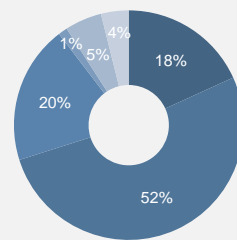
Perfil das Organizações

A LGPD se aplica às esferas pública e privada, a qualquer organização que realizar qualquer tipo de tratamento de dados pessoais, o objetivo da pesquisa é captar a percepção de maturidade das organizações que estão em fase de adequação. Com duração de cerca de dois meses, a pesquisa contou com um total de 175 respostas, com participação de organizações com capital predominantemente brasileiro e de organização societária de capital fechado. O maior volume de participantes é do setor de Tecnologia, Mídia e Telecomunicações, seguido por Serviços Financeiros, Farmacêutico e Hospitalar.

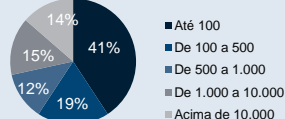


Tipo de organização societária

- Capital Aberto
- Capital fechado
- Empresa familiar
- Estatual ou economia mista
- Sem fins lucrativos
- Outros (Descraver):

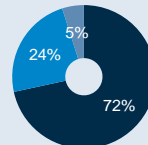


Colaboradores próprios



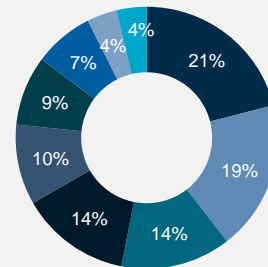
Capital predominantemente Brasileiro

- Sim
- Não
- Não sei informar

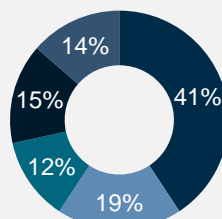


Receita das organizações

- Até 10 mi
- R\$ 10 mi a R\$ 50 mi
- R\$ 100 mi a R\$ 300 mi
- R\$ 1 bi a R\$ 5 bi
- R\$ 500 mi a R\$ 1 bi
- Acima de R\$ 5 bi
- R\$ 75 mi a R\$ 100 mi
- R\$ 50 mi a R\$ 75 mi
- R\$ 300 mi a R\$ 500 mi



Enquanto a exata vigência da LGPD ainda segue em análise, apenas uma pequena parcela (13%) das organizações participantes se consideram em um nível médio (61 a 80%) ou alto (81 – 100%) de maturidade quanto ao atendimento dos requisitos da lei. Sendo os setores de Óleo&Gás e Farmacêutico e Hospitalar os que se consideram com a maturidade mais alta entre os demais segmentos.



Quantidade de funcionários próprios

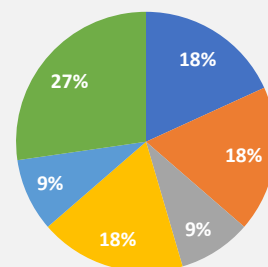
- Até 100
- De 100 a 500
- De 500 a 1.000
- De 1.000 a 10.000
- Acima de 10.000

As organizações com maior percepção de maturidade são também as empresas que possuem a maior receita dentre as participantes, além do maior investimento em medidas de proteção contra o vazamento de dados, considerando investimentos acima de 15 milhões.

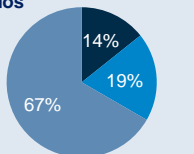
Já as organizações com percepção de baixa maturidade (de 0 a 40% dos requisitos atendidos) variam quanto a segmento e receita, o que mostra que a maioria das empresas ainda está no início das ações de adequação.

Segmentos com 0 a 40% dos requisitos atendidos

- Farmacêutico e hospitalar
- Jurídico
- Serviços financeiros
- Tecnologia, mídia e telecomunicações
- Terceiro Setor
- Demais Sektors

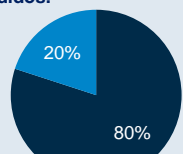


61 a 80% dos requisitos atendidos



- Atendimento Remoto BPO e Educação
- Construção e incorporação
- Tecnologia, mídia e telecomunicações

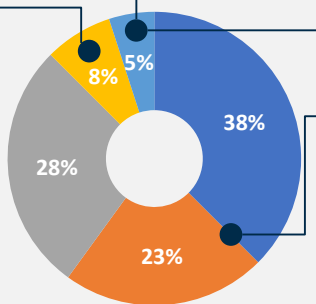
81 a 100% dos requisitos atendidos



- Farmacêutico e hospitalar
- Óleo e Gás

Percepção de maturidade das organizações quanto à LGPD

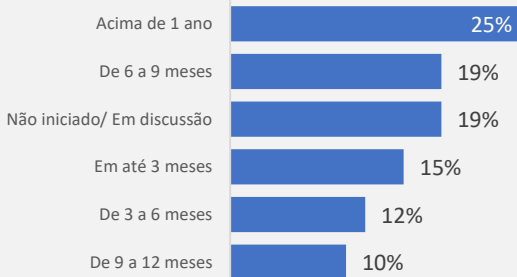
- 0 – 20% dos requisitos atendidos
- 21 – 40% dos requisitos atendidos
- 41 – 60% dos requisitos atendidos
- 61 – 80% dos requisitos atendidos
- 81 – 100% dos requisitos atendidos



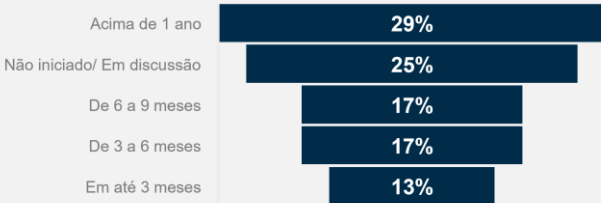
Planejamento e Investimento

Adequar a organização à LGPD exige muito planejamento e envolvimento de todas as áreas da organização, sendo que os maiores desafios estão entre a questão tecnológica, processos de negócio e aspectos culturais. 61% das organizações participantes com a percepção de baixa maturidade (de 0 a 40%) quanto ao atendimento dos requisitos da lei, considera um período no mínimo acima de 6 meses para se adequar, sendo que 25% dos participantes ainda estão discutindo ou não iniciaram as ações de adequação. 54% das organizações pretendem contratar consultorias para ajudá-las nas ações de adequação, mas consideram um investimento de até 100 mil, seguido por 15% que consideram investir até 500 mil.

Período esperado de adequação das organizações

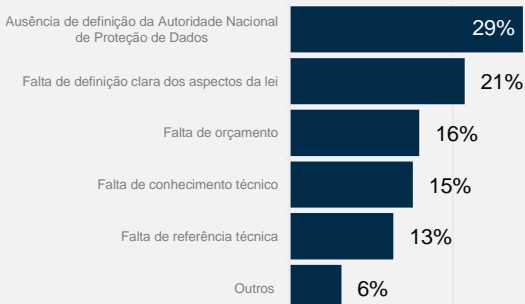


Período esperado de adequação das organizações com maturidade de 0 a 40% dos requisitos atendidos

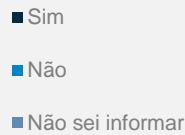


Quando questionadas quanto aos benefícios de dificuldades na jornada de adequação, os principais citados pelos participantes são a aderência aos requisitos regulatórios e proteção contra possíveis sanções, e por estes motivos apontam que a maior dificuldade hoje, além da incerteza quanto às datas de vigência da LGPD gerada pela sobreposição de leis e MP, é a ausência de uma autoridade para fazer a legislação prevalecer.

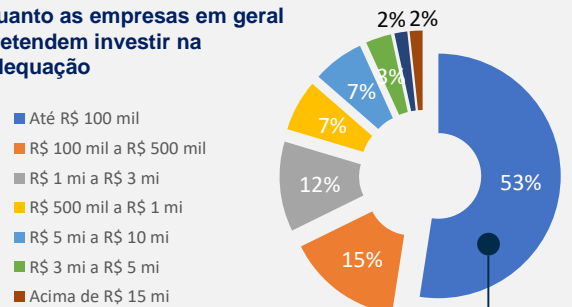
Maiores dificuldades na adequação à LGPD



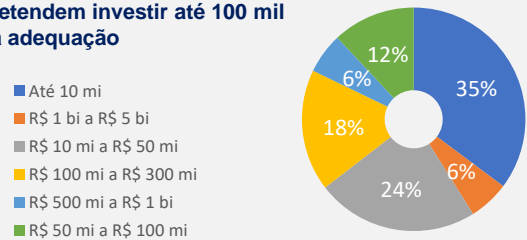
Organizações que pretendem contratar terceiros para auxiliar na adequação



Quanto as empresas em geral pretendem investir na adequação

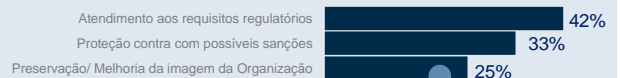


Receitas das empresas que pretendem investir até 100 mil na adequação

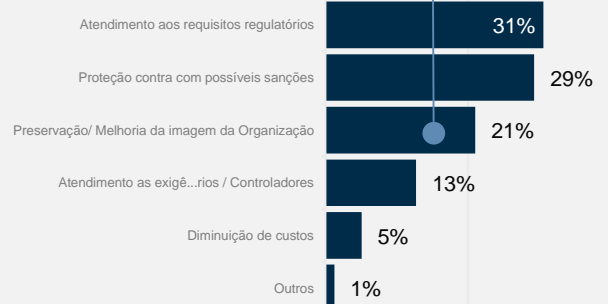


As organizações com maior percepção de maturidade incluem a preservação ou melhoria da imagem como um dos principais benefícios de se adequar a LGPD.

Benefícios de organizações com maturidade de de 61 a 100% dos requisitos atendidos.



Benefícios esperados da adequação à LGPD



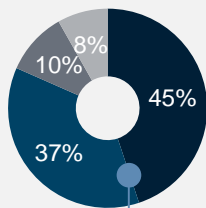
Governança e Cultura de Proteção de Dados

Estabelecer uma governança de privacidade na organização é um importante passo para manter a eficácia e garantir a continuidade das ações após o primeiro esforço do projeto de adequação.

Parte do programa, uma política de privacidade bem escrita, detalhada e devidamente disseminada, reforça a transparência da organização frente aos titulares de dados.

Programa de privacidade e proteção de dados

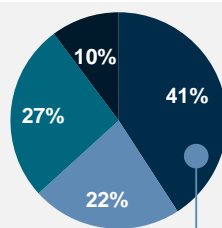
- Sim
- Faz parte do planejamento
- Não
- Não sei informar



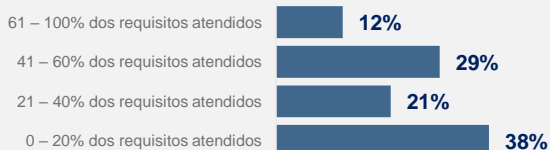
O encarregado ou DPO (*Data Protection Officer*) é uma figura essencial no processo de conformidade à LGPD, além de ser uma designação obrigatória, ele é o responsável por garantir o cumprimento da lei dentro da organização.

A organização já nomeou o DPO?

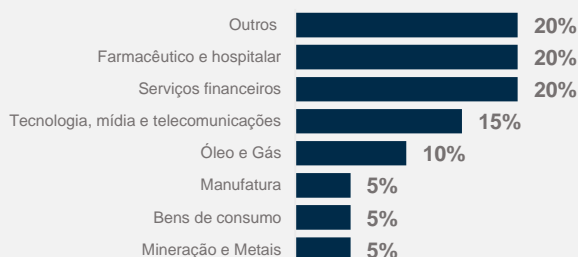
- Sim
- Não
- Faz parte do planejamento
- Não sei informar



Percepção de maturidade das empresas que já possuem ou estão planejando um programa de privacidade e proteção de dados.

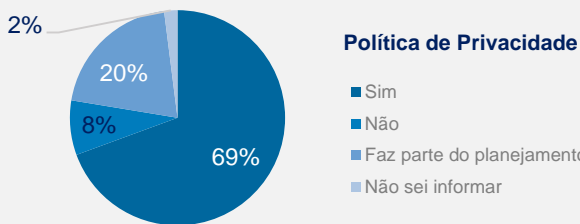


Segmentos que já nomearam o DPO



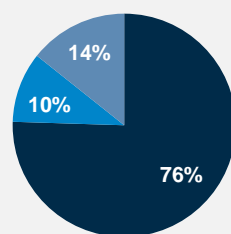
A adequação à LGPD exige uma mudança de cultura e postura das organizações, mas estabelecer a governança em privacidade e proteção de dados, além de promover o compliance, gera impactos positivos na organização, como melhoria no relacionamento com os clientes, aumento da segurança jurídica, valorização do marketing e aumento de sua produtividade, redução de custos, aumento da maturidade de segurança da informação e uma sinergia entre as diversas áreas da organização, pois é um projeto multidisciplinar. Por ser um passo importante na adequação, independentemente do nível de percepção de maturidade, as organizações já possuem em sua grande maioria implementados ou em planejamento um programa, política, ações de aculturação e treinamentos voltados para privacidade e proteção de dados.

Por conta das atribuições do cargo a preferência é que o DPO seja um colaborador interno, sendo que para quem já nomeou e quem ainda planeja nomear o responsável pelo cargo, os perfis preferidos são profissionais da área jurídica, compliance ou de segurança da informação. O outro perfil comentado na pesquisa é o de um profissional com um mix de conhecimento das três áreas de atuação.



DPO Interno ou Terceirizado?

- Colaborador interno
- Profissional / empresa terceirizada
- Não sei informar

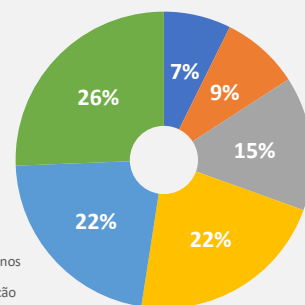


Aculturação e treinamento de privacidade e proteção de dados



Qual é o perfil ideal do DPO?

- Outros
- Profissional da área de riscos e controles internos
- Profissional da área de tecnologia da informação
- Profissional da área jurídica
- Profissional da área de segurança da informação
- Profissional da área de Compliance



Governança e Cultura de Proteção de Dados

O cargo de DPO é de grande responsabilidade e exige múltiplas habilidades. O perfil ideal, citado por diversos especialistas, é um profissional interdisciplinar, com conhecimentos da lei, governança de dados e de segurança da informação e que também seja capaz de ser porta-voz e relacionar com a Autoridade Nacional de Proteção de dados e os titulares de dados.

No Brasil é um profissional ainda em formação e as organizações têm optado por escolher um determinado perfil na estrutura interna e formá-lo nas demais habilidades necessárias. As empresas com percepção média ou alta de maturidade optaram principalmente por profissionais de segurança da informação assumirem o papel.

Segmento de Mercado	Perfil Preferido do DPO
Agroindústria	Profissional da área de compliance
Atendimento Remoto BPO e Educação	Profissional da área de Segurança da Informação
Automotivo	Profissional da área Jurídica
Bens de Consumo	Profissional de Compliance ou Profissional de Riscos e Controles Internos
Consultoria	Profissional da área Jurídica ou Profissional da área de Compliance
Farmacêutico e Hospitalar	Profissional da área Jurídica ou Profissional da área de Compliance
Jurídico	Profissional da área Jurídica ou Profissional da área de Compliance
Manufatura	Profissional da área de Segurança da Informação
Mineração e Metais	Profissional da área de compliance
Óleo e Gás	Profissional da área de Segurança da Informação
Serviços Financeiros	Profissional da área de Compliance ou Profissional da área de Segurança da Informação
Setor Público	Profissional da área de Segurança da Informação
Tecnologia, Mídia e Telecomunicações	Profissional da área Jurídica ou Profissional da área de Segurança da Informação
Transporte	Profissional da área de Compliance Profissional a área de tecnologia da informação.

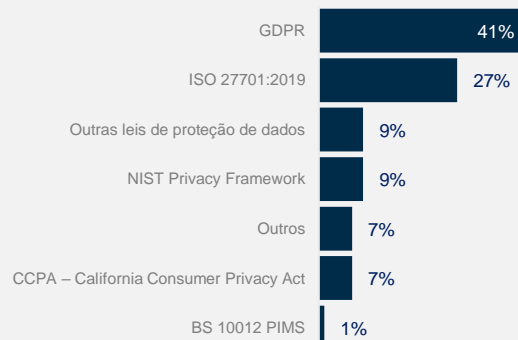
A maioria das organizações tem utilizado, além do GDPR, a nova ISO 27701 como referência acadêmica para planejar as ações de adequação. Como a lei brasileira se assemelha ao GDPR, é possível encontrar muito conteúdo com experiências práticas, já a ISO é muito utilizada pois fornece as diretrizes de como implementar um programa de privacidade, além de se relacionar com outras normas da família 27000 que dão suporte para implementação da conformidade.

Uma das vantagens da LGPD é a riqueza de conteúdo e discussões que a lei trouxe para o mercado brasileiro, mas 42% das organizações ainda entende que não há conteúdo acadêmico ou profissional suficiente, o que pode indicar que por ser uma lei que se aplica a todos os tipos de organização, a maioria dos conteúdos é mais genérico enquanto as organizações buscam conteúdo mais voltados aos desafios do mercado brasileiro e de seus segmentos de atuação.

Disponibilidade de conteúdo acadêmico e profissional



Material utilizado como referência para as ações de adequação à LGPD



Segmento de Mercado	Referência acadêmica mais utilizada
Agroindústria	GDPR
Atendimento Remoto BPO e Educação	GDPR, ISO 27701
Automotivo	GDPR, ISO 27701
Bens de Consumo	GDPR
Consultoria	GDPR, ISO 27701
Farmacêutico e Hospitalar	GDPR, Outras leis de proteção de dados
Jurídico	GDPR, ISO 27701
Manufatura	GDPR, ISO 27701
Mineração e Metais	GDPR, NIST
Óleo e Gás	GDPR
Serviços Financeiros	GDPR, NIST, ISO 27701
Setor Público	NIST
Tecnologia, Mídia e Telecomunicações	GDPR, ISO 27701
Terceiro Setor	GDPR, ISO 27701
Transporte	Outras leis de proteção de dados

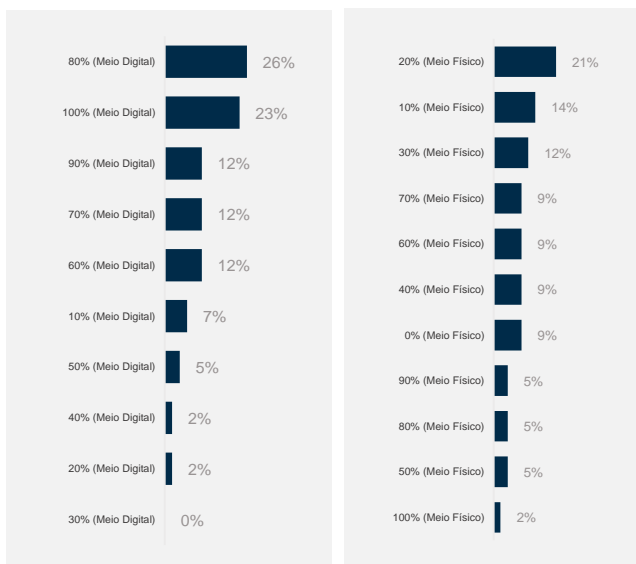
Atendimento aos Direitos dos Titulares

Seus dados pertencem a você. Essa é a principal mensagem da LGPD quando falamos dos direitos do titular de dados. O titular dos dados deve sempre ser informado sobre o modo como eles serão utilizados. Fora das situações impostas pela lei, os dados pessoais somente serão utilizados com consentimento. Os direitos do titular incluem:

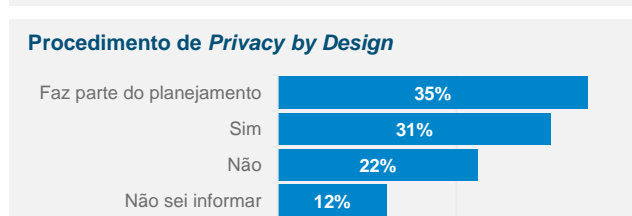


A maioria das organizações com maturidade de 0 a 60% focou em fazer o mapeamento do tratamento dos dados pessoais e assegurar uma forma de atendimento ao titular de dados, enquanto ações como a garantia dos direitos e a gestão do consentimento ainda estão em planejamento ou com ações parciais.

Quanto ao meio em que ocorre o tratamento dos dados pessoais e sensíveis nas organizações, 49% tratam de 80% e 100% das informações por meio digital, e todas possuem alguma porcentagem de tratamento por meio físico, sendo que 7% afirmam que trata 80% e 100% das informações por meio físico.



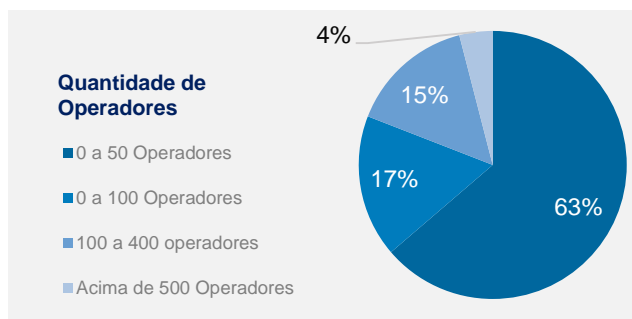
Tratamento de dados inclui toda operação realizada com dados pessoais, e todo tratamento deve ter finalidade, respeitando os 10 princípios existentes na Lei de forma específica, legítima, explícita e informada. O cumprimento de obrigação legal ou regulatória e execução de contrato ou procedimento relacionados ao contrato, teve a máxima de concentração de 100% de classificação de tratamento.



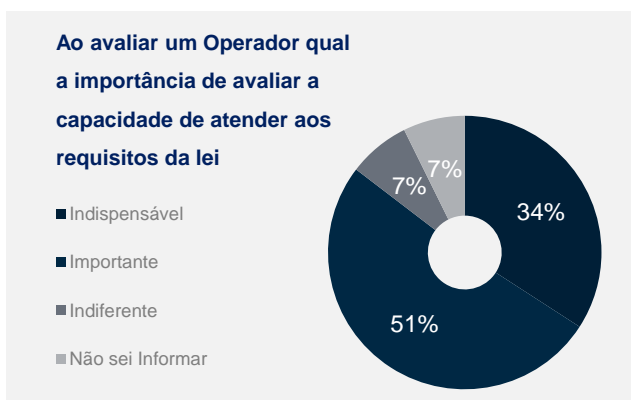
Considerando as bases legais para tratamento de dados pessoais, qual percentual que a sua organização aplica em cada uma, segundo os critérios abaixo?	0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
1. Consentimento pelo titular	23%	16%	11%	7%	0%	9%	9%	0%	7%	5%	14%
2. Cumprimento de obrigação legal ou regulatória	20%	5%	11%	9%	2%	7%	7%	5%	5%	9%	20%
3. Administração pública para execução de políticas públicas	50%	5%	5%	7%	7%	7%	5%	2%	0%	2%	11%
4. Estudos por órgãos de pesquisa	48%	5%	0%	11%	5%	5%	9%	0%	0%	5%	14%
5. Execução de contrato ou procedimentos preliminares relacionados ao contrato	16%	7%	5%	2%	5%	7%	11%	14%	7%	9%	18%
6. Para exercício regular de direitos em processo judicial, administrativo ou arbitral	25%	9%	2%	7%	5%	7%	11%	11%	7%	9%	7%
7. Para proteção da vida ou incolumidade física do titular ou terceiro	41%	7%	5%	7%	5%	7%	7%	5%	5%	7%	7%
8. Para tutela da saúde (profissionais de saúde)	50%	2%	2%	5%	2%	9%	5%	2%	2%	11%	9%
9. Para atender aos interesses legítimos do controlador	27%	11%	5%	9%	2%	9%	9%	5%	5%	11%	7%
10. Para proteção do crédito	34%	11%	0%	5%	2%	7%	5%	5%	7%	11%	14%

Relação Entre Controlador e Operador

Na LGPD, além do titular de dados e do encarregado (DPO), existem dois outros papéis, o do controlador e do operador. O Controlador é a pessoa física ou jurídica a quem compete tomar as decisões quanto ao tratamento dos dados pessoais, e o operador é quem realiza o tratamento dos dados em nome do controlador. A diferença dos papéis está no poder de decisão, o controlador é quem está no topo da cadeia de tratamento de dados e deve passar instruções claras ao operador de como tratá-los, e avaliar se o mesmo possui medidas de segurança para proteger os dados que serão compartilhados com ele.

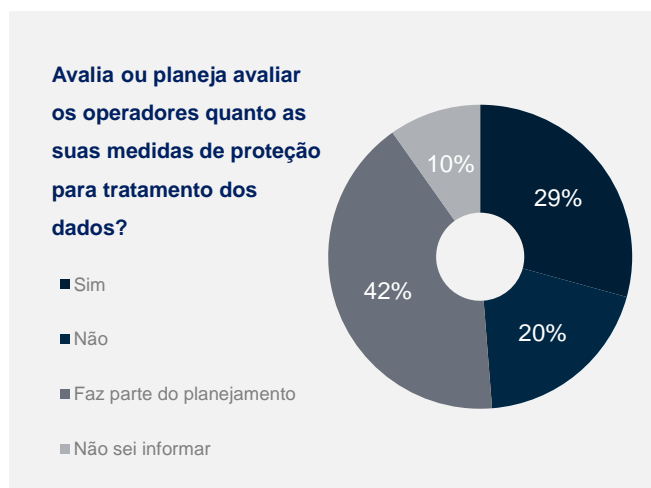
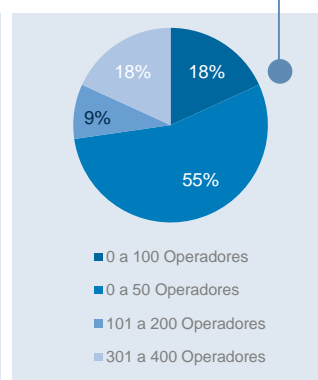
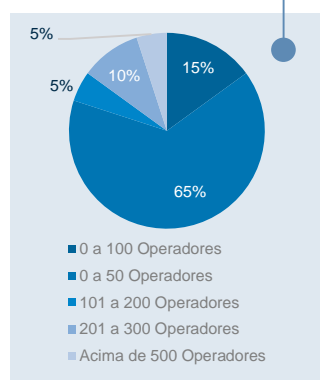
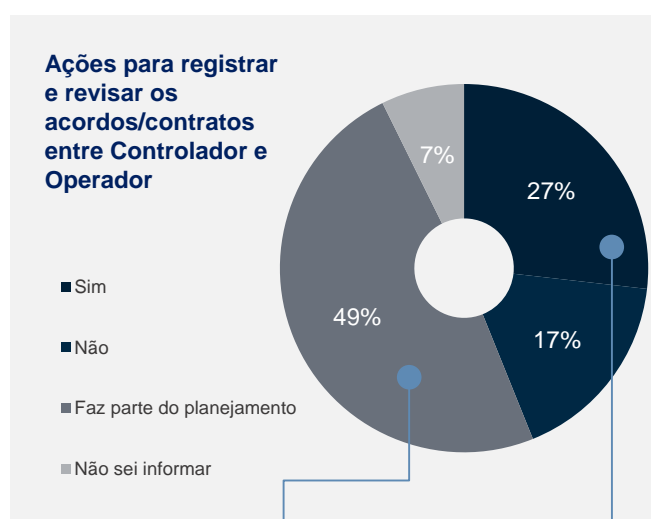


Os setores de Óleo & Gás e Terceiro Setor, são os segmentos que possuem o maior número de operadores (acima de 500), sendo que as organizações de Óleo & Gás, com maior percepção de maturidade quanto ao atendimento dos requisitos da lei, já implementaram as ações para registrar e revisar os acordos/contratos entre controlador e operador, já as organizações do terceiro setor estão em fase de planejamento.



Praticamente todas as organizações contam com parceiros, seja para agilizar ou viabilizar novos negócios, e para isso buscam diversos serviços como: *Hosting* em *Data Center*, serviços de *Cloud*, call centers, processadores de pagamento, sistemas de RH, empresas de cobranças e várias outras atividades.

As organizações (85%) consideram importante ou indispensável avaliar os operadores, com quem pretendem compartilhar os dados pessoais de seus clientes e colaboradores, quanto a sua capacidade de atender os requisitos da lei, mas apenas 27% já implementaram ações para revisar os acordos/contratos; e 29% já implementaram ações para avaliar a capacidade dos operadores de proteger os dados que estão sendo compartilhados pelo controlador.



Tudo que está previsto na LGPD, sejam os princípios de finalidade, necessidade e consentimento, ou a restrição ao uso de dados pessoais estende-se para subcontratantes e parceiros da empresa e, é papel do controlador estabelecer um processo de avaliação constante de fornecedores e parceiros, pois não adianta o controlador adotar todas as medidas de proteção em seu ambiente e compartilhar dados com organizações que não têm a mesma preocupação.

Medidas de Proteção e Gestão de Incidentes de Segurança

Na A LGPD incentiva as organizações a desenvolverem e aprimorarem suas medidas de segurança cibernética. As pessoas estão cada vez mais conscientes sobre seus direitos de privacidade e ao descobrir que uma empresa está os protegendo melhor, e não é parte das constantes notícias de vazamento de dados, confiam ainda mais no relacionamento estabelecido.

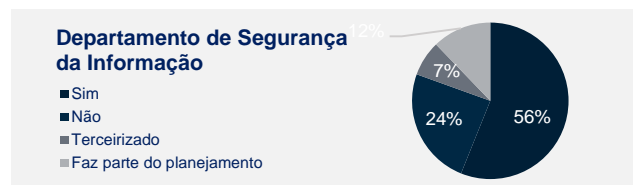
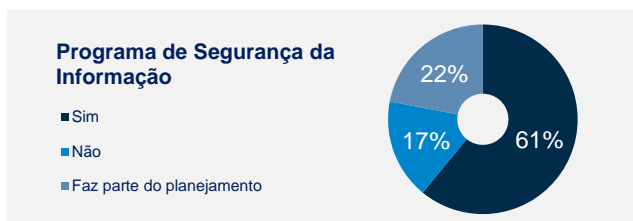
Em um cenário onde as empresas devem estar preparadas para ameaças cada vez mais avançadas, 39% das organizações participantes não possuem ou ainda estão planejando um programa de segurança da informação, e 43% não possuem ou planejam possuir um departamento de segurança informação.

A maioria das empresas que ainda não possuem um programa ou departamento de segurança da informação têm receita de até 100 milhões e até 500 funcionários próprios, sendo dos segmentos de Atendimento Remoto BPO e Educação, Jurídico, Mineração e Metais, Tecnologia, Mídia e Telecomunicação, Construção e Incorporação, Terceiro Setor.

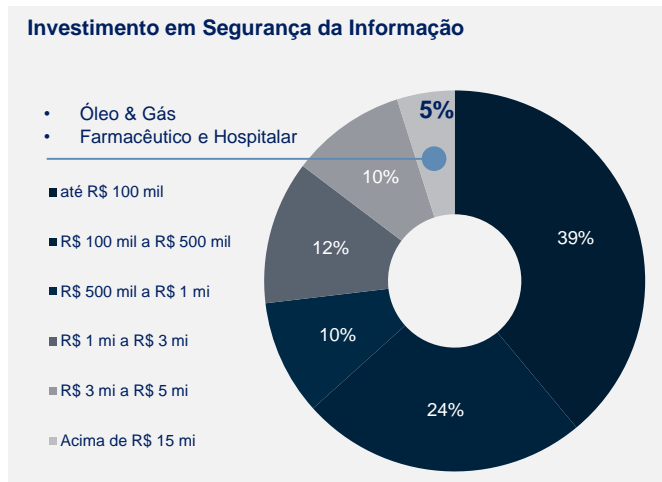
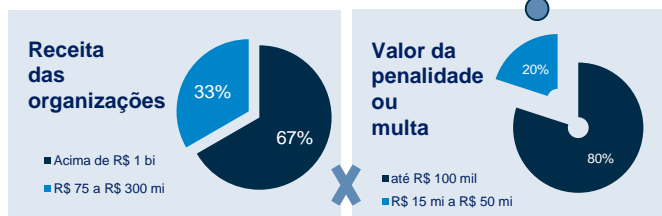
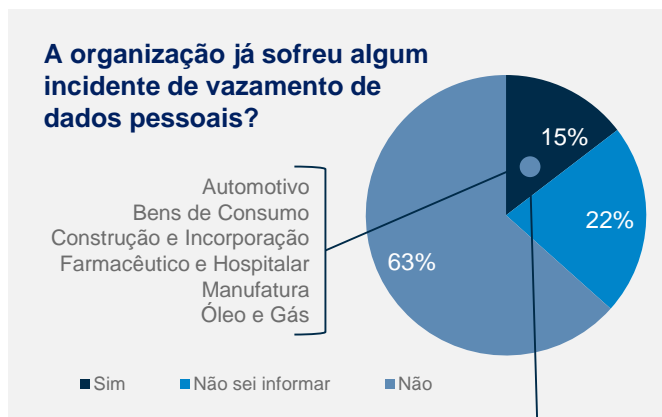
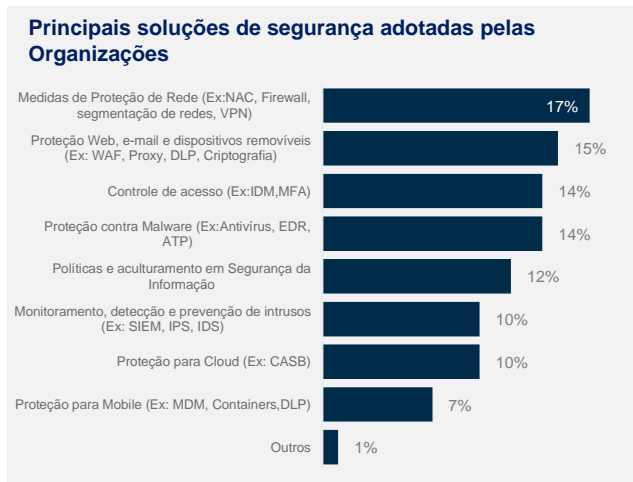
As notícias de vazamento de dados infelizmente se tornaram constantes e após o cenário de pandemia e a aceleração do trabalho remoto de forma repentina, o número de ataques e vazamento de dados aumentou com aceleração no Brasil.

Tanto as organizações que mais investem em segurança (acima de R\$ 15 milhões) quanto às demais organizações com diferentes níveis de maturidade e investimento estão entre os 15% que afirmaram já ter sofrido algum incidente de vazamento de dados, sendo que as penalidades ou multas aplicadas foram até R\$ 100 mil e entre R\$15 a R\$50 milhões.

Os dados pessoais dos consumidores sempre foram atraentes para o mercado e estão presentes em diversas fases do relacionamento do consumidor com a organização. Da mesma forma que as empresas utilizam estes dados para customizar e planejar melhor suas campanhas, produtos e serviços, os criminosos cibernéticos também utilizam com o intuito de sofisticar seus ataques, obter ganho financeiro ou destruir a reputação de uma empresa, portanto, a LGPD confirma o alto benefício de se investir em segurança da informação.



A LGPD determina a adoção de medidas técnicas de segurança para proteger as informações de processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, mas não define quais medidas devem ser adotadas. É uma abordagem holística e de escopo amplo, e cada organização deve adotar e priorizar as medidas baseadas em seus riscos e pensar em privacidade desde a concepção de seus serviços e produtos.



Conclusão

Com a LGPD nasce uma nova cultura e deve ser encarada pelas empresas como um aspecto diferenciador para competitividade no mercado, capaz de transmitir uma imagem de confiança perante os titulares.

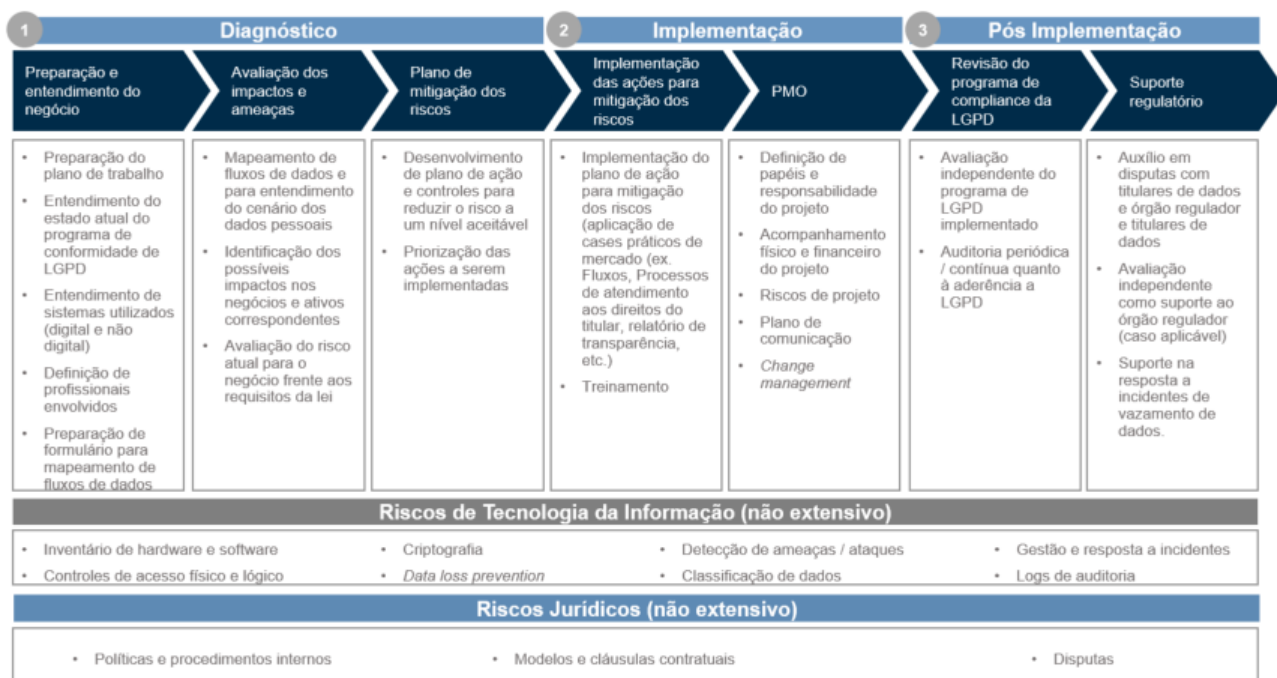
Durante os meses de realização da pesquisa (entre junho e agosto), a LGPD passou por algumas reviravoltas, porém agora conta somente com a sanção ou veto presidencial para passar a valer. Com a LGPD entrando em vigor ainda este ano, a maioria das empresas ainda tem uma baixa maturidade e considera cumprir só até 40% dos requisitos da lei, enquanto existem organizações que ainda estão discutindo e iniciando suas ações de adequação, sendo o período esperado de adequação é de no mínimo 6 meses.

Por outro lado, as empresas mais maduras, que já cumprem de 60% a 100% dos requisitos da lei são setores já bem regulados, com estruturas e receitas mais robustas e que já investem parte da receita em segurança da informação, deixando a liderança do tema e o cargo do DPO em grande parte para um colaborador interno do departamento de Segurança.

A dificuldade é maior para as pequenas e médias empresas, que ainda estão construindo as estruturas de governança e de segurança e tendem a sofrer grandes mudanças. As maiores dificuldades na adequação estão nos processos de mapeamento dos fluxos de dados pessoais, gestão de consentimento e garantia dos direitos do titular, além da falta de uma Agência Nacional de Proteção de Dados (ANPD), que vai fiscalizar o cumprimento da lei. Essa dificuldade foi finalmente solucionada com a publicação no dia 27/08 da estrutura da Agência que contará 36 cargos, sendo 16 em comissão remanejados e 20 funções comissionadas do Poder Executivo. Embora as sanções só estejam previstas para agosto do ano que vem, a adequação à LGPD é uma jornada que deve ser aproveitada, pois exige comprometimento, envolvimento de toda a organização e muito aculturação, mas é também um processo de amadurecimento, de auto conhecimento e melhoria de diversos processos internos onde todos ganham com os avanços.



Nossa abordagem para a LGPD



MARCOS GANUT - MANAGING DIRECTOR
mganut@alvarezandmarsal.com



EDUARDO MAGALHÃES - DIRECTOR
emagalhaes@alvarezandmarsal.com