APOSTILA

Lei Geral de Proteção de Dados

FM2S
EDUCAÇÃO & CONSULTORIA

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Apostila lei geral de proteção de dados [livro eletrônico] / FM2S Educação e Consultoria. -- Campinas, SP : FM2S Educação e Consultoria, 2023.
PDF

Bibliografia.
ISBN 978-65-80624-90-4

1. Compliance 2. Governança corporativa 3. Proteção de dados - Leis e legislação 4. Segurança da informação I. Título.

23-187826 CDU-342.721

Índices para catálogo sistemático:

1. Proteção de dados pessoais : Direito 342.721

Eliane de Freitas Leite - Bibliotecária - CRB 8/8415

Quem somos

Uma empresa de Educação e Consultoria criada para compartilhar conhecimento de excelência na prática. A FM2S foi escolhida para ocupar o Parque Tecnológico da UNICAMP, uma das universidades mais conceituadas do país. Já são mais de 70 mil profissionais que aceleraram suas carreiras conosco.

Como um dos maiores centros de aperfeiçoamento do Brasil, contamos com diversos cursos nas áreas de: Gestão de Processos; Lean; Visualização de Dados; Gestão de Projetos; Carreira & Liderança e Lean Six Sigma.

Nossos instrutores têm experiência prática para projetar e conduzir aulas e projetos essenciais, com ensinamentos técnicos, de liderança e outros fatores importantes para o seu crescimento. Eles são formados nas melhores universidades do país e já atuaram em cargos de liderança e de consultoria em grandes projetos.

Com essa bagagem, queremos ajudar você a alcançar seus objetivos profissionais, conquistando a posição que almeja na carreira. E isso é muito mais do que oferecer cursos, entregamos nossa experiência para que os profissionais sejam respeitados na sua empresa, na comunidade e na sociedade como um todo.

13 anos de mercado

75491 alunos

80 cursos

135 projetos realizados

45562 certificados emitidos

Nosso propósito

Acelerar o crescimento profissional de nossos alunos por meio de uma experiência educacional única, fundamentada em conceitos sólidos, linguagem simples, ferramentas e exemplos práticos.

Site FM2S | EaD FM2S | LinkedIn | Facebook | Instagram | YouTube | Soundcloud | Spotify | Twitter

Sumário

Lista de Figuras

Lei Geral de Proteção de Dados - LGPD

1. Boas vindas

Sejam bem vindos ao curso de Lei Geral de Proteção de Dados - LGPD da FM2S! Durante as aulas, entenderemos o que é esse sistema e como implementá-lo na empresa, seguindo os seguintes tópicos:

- O que é LGPD?
- Case Construções;
- Vantagens e desafios para implementação;
- Contexto HIstórico;
- Apresentação dos Conceitos:
    - Dado x Informação x Conhecimento;
    - Privacidade e Segurança da Informação;
    - Ciclo de vida de tratamento de dados;
    - Governança e Compliance;
    - Stakeholders;
    - Avaliação de Impacto à Proteção de Dados;
    - Autoridade Nacional de Proteção de Dados;
    - Direitos e Casos Particulares;
    - Agentes no tratamento de dados;
    - DPO;
    - Transferências internacionais, responsabilidades e sanções;
- Passo a Passo;
- Dicas e Boas Práticas;
- Revisão.

2. O que é LGPD?

Antes de abordar a Lei Geral de Proteção de Dados, é preciso pensar em dados e, consequentemente, em tecnologia. Ela desempenha um papel central nas nossas interações em sociedade, mas, de forma ampla, ela representa toda evolução científica, biológica, tudo aquilo que é novo. Aqui, falaremos sobre tecnologia digital, aquilo que possibilita o acesso à informação e dados, que são a maneira que as conexões são criadas.

Os dados são hoje considerados uma commodity, ou seja, um produto ou matéria prima usada para desenvolver algo fundamental dentro da sociedade. Eles são comparados ao petróleo por ser valor financeiro para empresas de tecnologia. Por isso, é importante pensar na importância desses dados no sistema e na interação que eles permitem.

Apesar de anteriormente existirem normas setoriais sobre dados, a LGPD é a primeira lei geral nacional sobre o tema. Ela estabelece regras para o tratamento de dados **pessoais** e inaugura uma nova cultura de privacidade e proteção de dados no país.

Ao se falar em cultura, a LGPD é comparável ao Código de Defesa do Consumidor, que existe a mais de duas décadas, mas que passou por um processo até ser internalizado na sociedade. Era difícil ter, por parte do consumidor inclusive, o reconhecimento de qualquer tipo de direito seu. Por isso, a lei vem antes e a partir da lei é que se cria uma cultura de implementação. E ocorre da mesma forma com a LGPD, já que, a partir de 2019, iniciou-se às sanções, por isso o foco em estabelecer essa cultura.

Dados são, como veremos mais adiante no curso, o que precede a informação: um dado é uma informação ou conjunto de valores que podem ser armazenadas, processadas e analisadas, como números, palavras, imagens ou qualquer outra forma de representação simbólica que contenha significado. Posteriormente, quando interpretados, eles geram informações, o que representa poder para obter resultados. Os dados podem

ser usados pelos meios tecnológicos para mandar informações, fazer propagandas, oferecer serviços, enfim.

A Lei Geral de Proteção de Dados Pessoais é uma lei geral, ou seja, que se aplica a múltiplas situações (no setor público ou privado), que tem como objetivo proteger as informações pessoais dos cidadãos. Justamente por ser uma lei geral, ela não contempla todos os casos, logo ela não trará uma linguagem específica, como por exemplo "como coletar dados de **clientes"**. Por isso ela traz, no artigo 1º da LGPD o seu objetivo: "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". Esse objetivo se relaciona com o fato de que os dados são uma forma de individualizar o ser humano: seja pelo CPF, nome da mãe, pai, data de nascimento, entre outros. E através disso e as combinações possíveis (ou seja, passíveis de manipulação) é que se pode transformar e prever ações de um indivíduo único.

Sobre a disposição da lei, ela sempre começa com um preâmbulo que a justifica; segue para o primeiro artigo, que abarca o seu objetivo e depois vêm seus capítulos e princípios. A LGPD possui 65 artigos distribuídos em 10 capítulos, que contemplam:

- Disposições preliminares: entender a lei no geral;
- Do tratamento de dados pessoais: o que são dados pessoais e como eles estão entendidos na lei;
- Dos direitos do titular: direitos da pessoa natural, titular do dado;
- Do tratamento de dados pessoais pelo poder público: divisão entre poder público e privado;
- Da transferência internacional de dados: entender o funcionamento da transferência de dados entre países;
- Dos agentes de tratamento de dados pessoais: quem são as pessoas responsáveis por tratar os dados;
- Da segurança e das boas práticas;
- Da fiscalização;
- Da autoridade nacional de proteção de dados (ANPD) e do conselho nacional de proteção de dados pessoais e da privacidade;

- Disposições finais e transitórias: como a lei passa a ter vigência no tempo e espaço.

Os seus fundamentos, ou seja, o que dá base para a lei, são:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - à inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Uma das principais consequências da falta de conformidade com a LGPD é a possibilidade de enfrentar sanções administrativas. A Autoridade Nacional de Proteção de Dados (ANPD), encarregada de supervisionar o cumprimento da LGPD, tem a autoridade para impor penalidades financeiras que podem chegar a 2% do faturamento da empresa, com um teto máximo de R$50 milhões por cada violação.

A LGPD deve observar a boa-fé e os seguintes princípios, ou seja, a lógica que o texto segue, uma lente de leitura:

Figura 1 - Princípios norteadores da LGPD pelo Art. 6º

Princípio	Definição
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
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
Livre Acesso	Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais
Qualidade dos Dados	Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento
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
Segurança	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão
Prevenção	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais
Não discriminação	Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos
Responsabilização	Demonstração, pelo agente, da adoção de medidas eficazes e

e prestação de contas	capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas

A abrangência da LGPD está como direito de pessoas naturais, ou seja, os titulares dos dados enquanto pessoas físicas enquanto os deveres em relação ao tratamento dos dados se aplicam para pessoas físicas ou jurídicas enquanto agentes de tratamento. Quanto à territorialidade se restringe às operações realizadas em território nacional; dados coletados no Brasil e que se refiram a pessoas que estão em território brasileiro. Ela também abrange tratamentos internacionais, desde que tenham origem no Brasil.

Por outro lado, não se aplica quando o tratamento for realizado por pessoa natural (pessoa física) para finalidades particulares e sem intenção econômica; ou ainda se forem utilizados para fins exclusivamente jornalísticos, artísticos, acadêmicos ou de grande interesse público. Apesar da LGPD proteger todos os dados, uma pessoa pública, como um cantor, tem o seu nome (enquanto forma de individualização) divulgado sem proteção. Vale ressaltar também que quando dados forem utilizados para fins de grande interesse público, quais sejam, segurança pública e do Estado, defesa nacional, operações de investigação, atividades de repressão de infrações penais, a LGPD não se aplica.

Quando discutimos a relação entre a Tecnologia e a LGPD, estamos, sem dúvida, fazendo referência à Inteligência Artificial (IA). A IA desempenha um papel primordial ao acelerar o processamento e a compreensão dos dados. A origem da IA remonta ao professor de ciência da computação de Stanford, John McCarthy (1955), que a definiu como "a ciência e a engenharia de construir máquinas inteligentes". Por exemplo, ao entrar em um site que exige uma dupla verificação com caixa de seleção de imagens, com o dizer “Eu não sou um robô”, os seres humanos estão treinando uma IA por meio de dados, os quais podem ser utilizados futuramente por empresas.

Notamos, claramente, que a Inteligência Artificial está exercendo relações cada vez mais amplas e profundas com o universo do Direito. O Direito vem sendo transformado pelas novas tecnologias, por meio da digitalização da profissão e do Poder

Judiciário, assim como vem transformando a Inteligência Artificial quando exerce função regulatória sobre esses sistemas. Especialistas renomados na área (Richard Susskind, 2017), já faziam previsões sobre os efeitos da IA no Direito (ALENCAR, 2022, p. 10):

> À medida que nos aventuramos mais profundamente na década de 2020, prevejo que o impacto da IA em nossas vidas pessoais e em nossas instituições sociais, políticas e econômicas se tornará generalizado, transformador e irreversível. A lei e os tribunais não serão deixados de fora.

Os tribunais, a área jurídica no geral, são considerados muito tradicionais, consequentemente, são os últimos a aderir a novas tecnologias. Porém, com a pandemia da Covid-19, os tribunais se reinventaram e já são considerados, portanto, um lugar importante para se pensar em relação ao uso de dados, por isso que a Lei Geral de Proteção de Dados representa um avanço na área.

3. Case Construções

Essa história é ilustrativa, mas muitos podem se identificar com o relatado:

Márcia, uma dedicada profissional responsável pelo setor de pós-venda de uma construtora, estava comemorando o sucesso de vendas de um novo condomínio residencial na área nobre da cidade. Seu trabalho era garantir que os clientes ficassem satisfeitos com suas compras e tivessem todo o suporte necessário após receberem as chaves. No entanto, um incidente estava prestes a desafiar Márcia e a empresa.

Márcia começou a enfrentar uma situação peculiar. Vários clientes começaram a reclamar de ligações inoportunas de lojas de planejamento de móveis, oferecendo serviços para seus imóveis recém-adquiridos. Ela estava perplexa e sentia-se impotente diante dessa situação, ainda sem entender como eles se relacionavam. Foi quando um cliente, que por coincidência era advogado, fez uma pergunta intrigante: "Você não acha estranho que a loja tenha meus dados e a informação de que eu acabei de comprar um apartamento se nem a minha mãe sabe?"

Claro que a situação era realmente estranha, especialmente considerando que várias reclamações semelhantes surgiram. Diante disso, Márcia decidiu abordar a questão e procurou Pedro, responsável pelo setor jurídico, pois tinha suspeitas de que o sistema de armazenamento de dados dos clientes poderia ter sofrido uma invasão. Durante a conversa, ela percebeu que seu próprio conhecimento sobre proteção de dados era limitado, enquanto Pedro estava familiarizado com a LGPD. Entretanto, esse conhecimento era por sua formação em Direito, não por incentivo da empresa.

Inicialmente, eles apresentaram a situação à alta gestão. O incidente relatado por Márcia era grave e poderia resultar em processos legais. Para evitar que situações semelhantes ocorressem no futuro, tornou-se evidente que era necessário investir em treinamento, mapear o ciclo de vida dos dados e, possivelmente, implementar medidas de segurança adicionais.

Como parte do processo, eles conduziram análises preditivas, identificando as necessidades da empresa, e procuraram um escritório de advocacia que pudesse orientá-los sobre os custos envolvidos. Em seguida, compararam esse investimento com os gastos que a empresa teria caso todos os compradores optarem por processá-la.

Essa análise revelou que, apesar de ser um investimento significativo, não se equiparava aos custos potenciais de processos judiciais, o que resultou na aprovação do investimento.

O primeiro passo, portanto, foi a realização de um treinamento abrangente com todos os colaboradores, visando conscientizá-los sobre a LGPD e o que realmente envolvia o tratamento de dados. Esse treinamento demonstrou ser eficaz, tendo impactos positivos também em suas vidas pessoais. Poucos deles tinham o hábito de ler os Termos e Condições de uso de aplicativos, por exemplo, e ainda menos tinham plena consciência da quantidade de dados que geram diariamente. Houve ainda a criação de um comitê responsável, com nomeação de um controlador (o supervisor da área jurídica), operadores da área de vendas e pós venda.

Após a conclusão dos treinamentos, deu-se início a uma auditoria interna com o objetivo de mapear os dados atualmente mantidos pela empresa. Durante esse processo, o setor jurídico identificou a possível brecha que poderia ter resultado na invasão: o sistema utilizado para armazenar os dados dos clientes não contava com uma política de

autenticação ou controle de acesso, como uma verificação no celular. Além disso, foram identificados riscos relacionados ao espaço físico da empresa, onde qualquer pessoa tinha acesso aos formulários assinados pelos clientes.

Em resposta a essas descobertas, uma análise foi conduzida, resultando na formulação de planos de ação destinados a alinhar os processos da empresa com as diretrizes da LGPD. Como parte dessas medidas, implementou-se a autenticação de dois fatores no sistema, utilizando senha e verificação no celular. Além disso, a empresa eliminou o uso de documentos físicos, armazenando todos os registros na nuvem, o que permitia rastrear qualquer manipulação desses documentos. Será visto ao longo do curso que uma das boas práticas relacionadas à LGPD é que não haja documentos físicos, por serem de mais fácil acesso, por isso, implementou-se o sistema de nuvem. Por fim, com a assistência do advogado da empresa, foi elaborada uma Política de Privacidade e termos de consentimento para cumprir as exigências da LGPD.

O processo foi consideravelmente menos burocrático do que Márcia antecipava, e sua participação desempenhou um papel fundamental na viabilização dessas mudanças.

A adaptação à LGPD representava uma garantia a longo prazo, razão pela qual foi tão valorizada. Além disso, reconheceu-se sua importância para a carreira de Márcia, pois a LGPD é tão crucial quanto o Código de Defesa do Consumidor. Independentemente de sua localização ou cargo, essa expertise se tornou essencial para ela.

4. Vantagens e desafios para implementação da LGPD

A implementação da LGPD pode trazer muitas vantagens para a empresa, as quais incluem:

- Conformidade com as determinações e proteções coerentes com o restante do país;
    - Serve para evitar processos judiciais, demandas, qualquer tipo de penalização pelos agentes; também é importante para obter investimentos, cadastro de fornecedores para alguns tipos de empresa, entre outros;
- Melhorar reputação de uma organização;

- Minimizar riscos em relação à vazamentos e usos inadequados;
- Melhores práticas em transparência e responsabilidade corporativa.

Por outro lado, implementá-la não é simples. São muitos desafios para tal, como a burocratização para revisão e atualização de políticas, por ser uma lei procedimental, é preciso primeiramente olhar o que já existe, quais dados já foram coletados, quais já existem no sistema, quem são os setores envolvidos, entre outros, o que demanda tempo e um time engajado. Outro desafio é a implementação de medidas de segurança robustas e adequadas para cada empresa; além disso, há um custo de manutenção alto para mapeamento, com poucas pessoas qualificadas para realização do serviço e categorização de dados pessoais. Por fim, um grande desafio é a notificação imediata de violações de dados, uma vez que a notificação deve ser feita sempre que se sabe da violação e isso não é rápido.

O cliente e colaborador de uma empresa que segue a LGPD enfrenta alguns desafios também, como a promoção de conscientização e treinamentos, além do advento das *big techs,* as quais concentram os dados. Entretanto, existem outras vantagens, como:

- Conformidade com as determinações e proteções para colaboradores e clientes;
- ANPD produz guias e cartilhas que ajudam na conscientização;
- Consagração do direito à privacidade.

A implementação da LGPD pode gerar oportunidades para colaboradores no geral, uma vez que independente do setor, reclamações sobre segurança e privacidade sempre aparecem, conforme a figura abaixo ilustra. Em primeiro lugar, com o maior número de reclamações, estão os bancos, empresas financeiras e administradoras de cartão, uma vez que esse tipo de vazamento resulta em algum tipo de crime que gera algum tipo de prejuízo financeiro ao consumidor (como compras ilícitas). Assim, esse vazamento é visto com maior rapidez, o que explica o maior número de reclamações.

Figura 2 - Reclamações sobre segurança e privacidade por setor

Bancos, Financeiras e Administradoras de Cartão	26,4%
Operadoras de Telecomunicações (Telefonia, Internet, TV por assinatura)	17,4%
Transporte Aéreo	9,3%
Comércio Eletrônico	8,4%
Viagens, Turismo e Hospedagem	4,4%
Seguros, Capitalização e Previdência	4,4%
Empresas de Pagamento Eletrônico	4,2%
Provedores de Conteúdo e Outros Serviços de Internet	3,2%
Energia Elétrica	3,1%
Operadoras de Planos de Saúde e Administradoras de Benefícios	0,9%

Por outro lado, uma pesquisa realizada pela Dayrus Consultoria demonstra que 80% das organizações no Brasil ainda não concluíram seus projetos de adequação, embora seja dito por 58% das empresas entrevistadas que a proteção de dados pessoais é de alta relevância. Ou seja, embora mais da metade das empresas tenham afirmado a importância, apenas 20% finalizaram o projeto de implementação, por custo alto e pela demora do processo. Portanto, há um mercado considerado importante e relevante, mas não completamente explorado, com poucos profissionais qualificados. Ter condições para fazê-lo é uma grande vantagem competitiva.

5. Contexto Histórico

5.1. Panorama Internacional

Desde sempre produzimos dados e os interpretamos como informação, mas não havia preocupação com sua proteção e compartilhamento de modo amplo. Porém, tudo muda com a Web 2.0: compartilhamento de informações e redes sociais fazem sucesso estrondoso – começamos a viver a Sociedade Informacional, onde a informação é um bem econômico, preponderante, que define muitas das relações humanas e com valor de compra, venda e transferência. Por exemplo, o LinkedIn, plataforma que reúne dados profissionais e redistribui.

O uso de dados pessoais é fundamental para diversos setores da economia e da sociedade, por exemplo, no comércio, o armazenamento de dados pessoais agiliza transações e permite recomendar produtos com base no perfil do cliente, ou seja, é possível criar um perfil de consumo para enviar mais propagandas e informações daquilo que me interessa. Em serviços públicos e privados, o registro de dados melhora o acesso às informações pessoais e personaliza os serviços de acordo com as necessidades de cada usuário.

Casos recentes chocaram o mundo em relação à venda e uso indevido de dados o que acabou por trazer à tona a importância da proteção do uso dos dados, como o da Cambridge Analytica. Dados de mais de 50 milhões de usuários do Facebook foram vazados para fazer propaganda política. Os dados incluíam detalhes sobre a identidade das pessoas – como nome, profissão, local de moradia – seus gostos e hábitos e sua rede de contatos, o que permitia o mapeamento de perfil dessas pessoas. Esse vazamento foi por conta de um teste na rede social, que liberou dados pessoais de quem o fez e das pessoas que mantinham amizades na rede, com objetivo de fazer propaganda política.

A Cambridge Analytica teria comprado acesso a informações pessoais de usuários do Facebook e usado esses dados para criar um sistema que permitiu predizer e influenciar as escolhas dos eleitores nas urnas, segundo a investigação dos jornais The Guardian e The New York Times. Isso aconteceu pela indicação do perfil dos usuários e direcionamento de propagandas específicas de acordo com isso.

Outro marco importante internacionalmente foi a General Data Protection Regulation – GDPR, da União Europeia, aprovada em 2016. Essa é a legislação de referência, a qual tem como objetivo garantir os direitos individuais de privacidade dos indivíduos, provendo transparência no processamento de dados e garantindo que compliance seja uma prioridade.

Ainda no âmbito das leis, mas passando para os Estados Unidos, existem algumas diferenças. Em alguns ordenamentos jurídicos, várias normas relacionadas à privacidade e ao uso de dados podem coexistir e se complementar. Nos Estados Unidos, onde empresas de tecnologia como Google, Apple, Microsoft, Facebook e Amazon estão sediadas, existem diversas normas abordando a proteção de dados em diferentes contextos. No entanto, ao contrário da GDPR europeia, não existe uma norma geral unificada que aborde a proteção de dados de forma abrangente nos Estados Unidos.

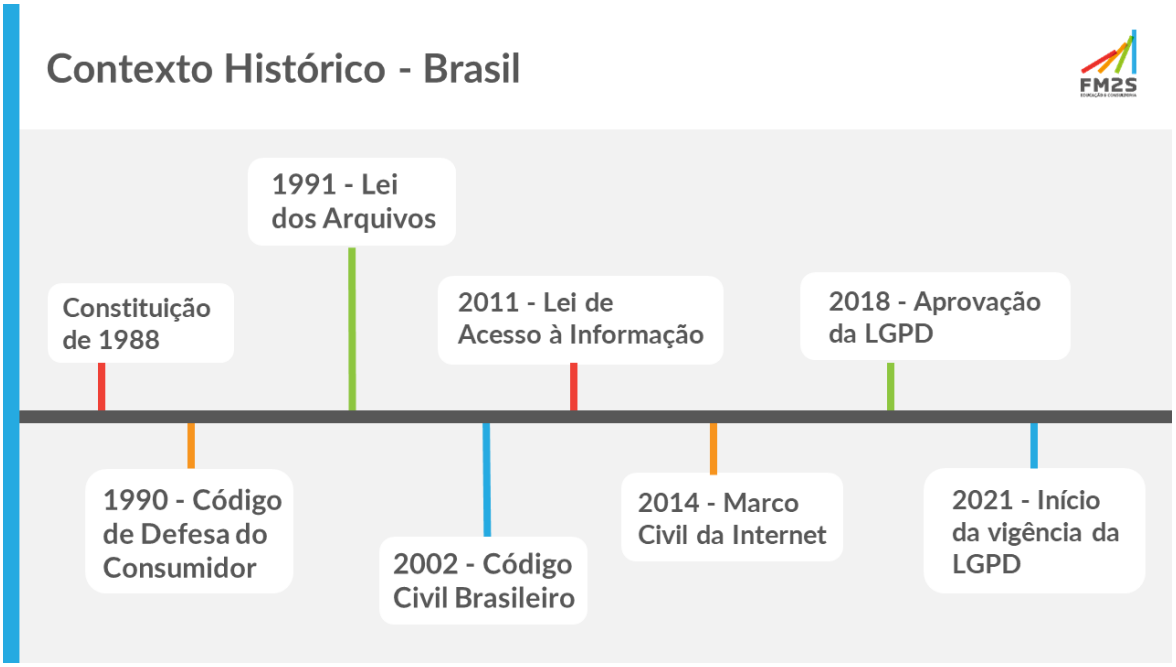
Há, porém, dentro do sistema normativo americano, normas diversas que abordam a proteção de dados em alguns pontos dos seus textos, como a Lei de Modernização Financeira (1999), a Lei de Portabilidade e Responsabilidade de Seguro de Saúde (1996) e a Lei de Privacidade (1974) que regula registros em agências federais.

- Lei de Privacidade (1974): A Lei dos Direitos Educacionais e da Privacidade da Família (FERPA) é uma legislação federal dos Estados Unidos, cujo propósito é resguardar a confidencialidade dos registros educacionais dos estudantes;
- Lei de Portabilidade e Responsabilidade de Seguro de Saúde (1996): HIPAA e as regulamentações derivadas da HIPAA constituem um conjunto de regulamentos de saúde dos Estados Unidos que estabelecem diretrizes para o manuseio, divulgação e preservação de informações pessoalmente identificáveis relacionadas à saúde.
- Lei de Modernização Financeira (1999): A Lei Gramm-Leach-Bliley (GLB) de 1999 nos EUA regula como instituições financeiras tratam informações privadas; ela abrange três principais áreas: Regra de Privacidade Financeira, Regra de Salvaguardas e Disposições sobre Pretexto; instituições financeiras devem fornecer avisos de privacidade por escrito aos clientes explicando suas políticas de compartilhamento de informações.

5.2. Panorama Brasileiro

O Brasil tem a aprovação da LGPD em 2018, mas existem outros marcos que tratam acerca da privacidade, conforme visto na figura abaixo:

Figura 3 - Contexto Histórico - Brasil



Tudo começa com a Constituição de 1988, a chamada Constituição Cidadã, sendo que até a Emenda Constitucional nº115/2022 dela, a proteção de dados não era abordada de forma explícita. Partia-se da ideia que os dados são elemento constituinte da identidade. Ela está na ponta da pirâmide, sendo a lei mais importante, acima das leis e decretos e regulamentos.

O Código de Defesa do Consumidor de 1990 traz algumas regras relativas a banco de dados de consumidores, como manter as informações claras e o direito do cliente de ter conhecimento desse cadastro. É mais específico por se pautar em relações de consumo.

Apenas um ano depois (1991), há a aprovação da Lei de Arquivos, a qual determina que os direitos e deveres relacionados a arquivos privados recaem no poder de agentes públicos. O Código Civil Brasileiro (2002), por sua vez, garante a inviolabilidade da vida privada, que foi uma atualização importante de termos. Por fim, a Lei de Acesso à Informação de 2011 traz transparência de dados públicos, mas também faz alusão à segurança de informações pessoais.

Mais relacionado à LGPD, há o Marco Civil da Internet de 2014, que dá a proteção dos dados pessoais como princípio do uso da internet e determina a proibição dos agentes de internet de fornecer dados pessoais a terceiros. Esse foi um marco importante para a proteção de dados, mesmo que não fossem vistas muitas aplicações práticas. A LGPD, por sua vez, tem o seu projeto de lei proposto em 2012, mas foi um processo conturbado. O projeto só é aprovado em 2018 e só entra em vigor em 2021.

6. Apresentação dos Conceitos

Os conceitos que serão abordados ao longo do curso foram divididos em dois blocos: os essenciais para entender a lei e um segundo que destrincha a lei, tirando todas as dúvidas antes de aplicar no passo a passo. Eles são:

- Conceitos Essenciais:
    - Dado x Informação x Conhecimento;
    - Privacidade e Segurança da Informação;
    - Stakeholders;
    - Governança e Compliance;
    - Ciclo de vida de tratamento de dados: coleta, uso, armazenamento;
    - Impacto e Avaliação de Privacidade (AIPD);
    - Autoridade Nacional da Proteção de Dados.
- Destrinchando a lei:
    - Direitos e Casos Particulares;
    - Agentes no tratamento de dados;
    - DPO;

- Transferências Internacionais, responsabilidades e sanções.

7. Dado x Informação x Conhecimento

Para começar, é essencial entender a diferença entre dados, informação e conhecimento.

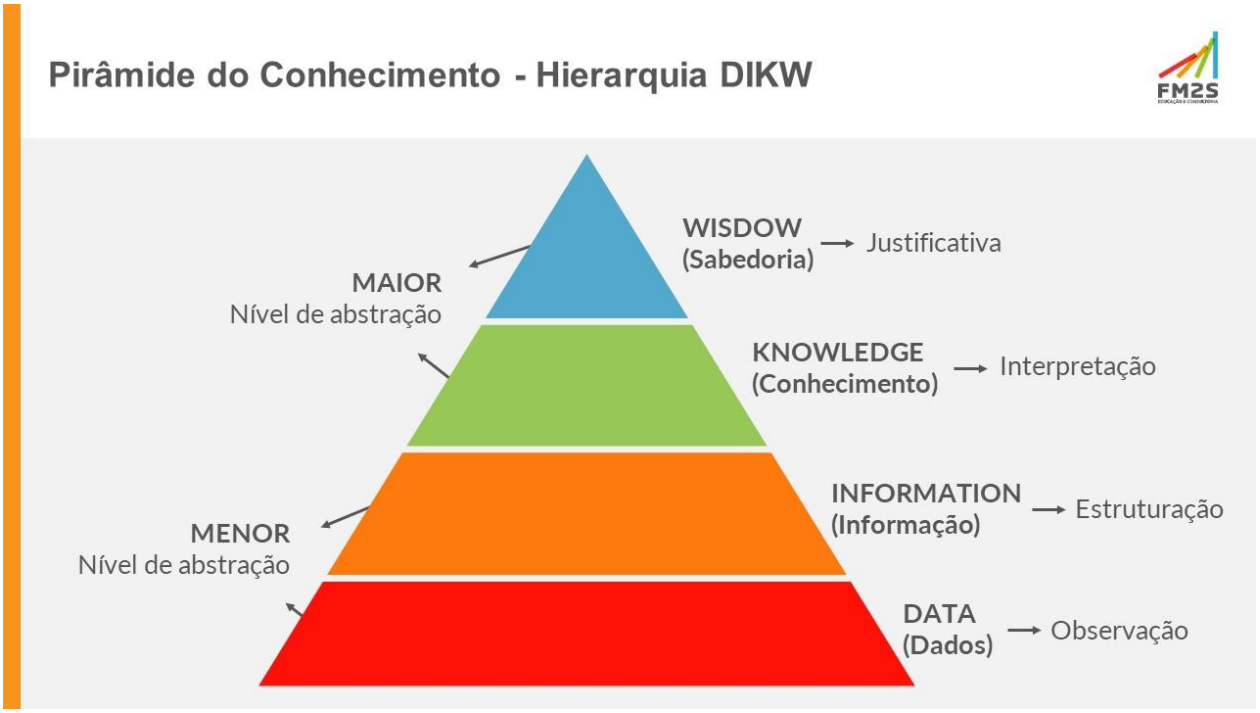
Não existe uma definição de dado que seja fora da área da tecnologia, o que pode limitar a teoria. Por isso, trazemos uma definição simples: o dado é, essencialmente, o que acontece, sendo a menor parte desses três elementos, mas a base deles, por isso que é o foco da lei. A LGPD faz a separação entre:

- Dados pessoais: aqueles que possibilitam a identificação, direta ou indireta, da pessoa natural;
- Dados sensíveis: revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde, a vida sexual de uma pessoa ou dados de pessoas menores de idade.

A informação, por outro lado, é um passo a mais, ou seja, o dado interpretado por alguém. Seguidamente, o conhecimento, que é a informação absorvida e que permite ser sintetizada a partir de conhecimentos prévios, possibilitando algum tipo de ação. Por fim, a sabedoria: Tomar uma atitude no mundo a partir do conhecimento. Essa é a chamada

Pirâmide do Conhecimento ou Hierarquia DIKW (*Data, Information, Knowledge and Wisdom* – dado, informação, conhecimento e sabedoria), conforme a figura abaixo:

Figura 4 - Pirâmide do Conhecimento



Sempre começamos com a base da pirâmide, que tem um menor nível de abstração, uma vez que os dados são mais concretos. A informação é mais abstrata, já que pode depender de conhecimentos prévios. Assim sucessivamente, mas vale ressaltar que a sabedoria não é a mesma para todos os indivíduos, já que depende de históricos e conhecimentos prévios.

Um exemplo comum para o dia a dia é:

- Estamos em uma sala escura e há um clarão.
    - O clarão é o dado.
- Você, ao ver o clarão, pensa: Se em seguida vier um estrondo, provavelmente foi um relâmpago.
    - Essa é a informação.

- Veio um estrondo e você pensou: Está chovendo.
    - Esse é o conhecimento
- A partir disso, você se levanta para fechar a janela.
    - Essa atitude é a definição de sabedoria.

Outro exemplo, mas dessa vez relacionado à LGPD:

- Dados:
    - Um cliente teve a sua última compra no dia 04/09;
    - Essa compra incluía um medicamento de uso contínuo com 30 drágeas;
    - Email;
    - Telefone;
- Informação:
    - Se a última compra foi dia 04/09 e a caixa tem 30 comprimidos, dia 04/10, o cliente precisará de outra caixa;
- Conhecimento:
    - Pelos outros dados da farmácia, a maioria das pessoas compra apenas uma caixa ao mês e deixa para a última hora;
    - Todo mundo quer comprar mais barato;
- Sabedoria:
    - Orientar os colaboradores a ligar para esse cliente entre dia 29 e dia 02/10 oferecendo desconto para esse medicamento específico para aumentar a chance de compra.

Outro exemplo para a LGPD:

- Dados:
    - Coleta de Dados de Navegação: Uma empresa de publicidade online coleta informações sobre os hábitos de navegação de usuários da web, incluindo os sites que eles visitam e o tempo gasto em cada página;
- Informação:

- Análise de Comportamento de Navegação: A empresa processa esses dados de navegação para criar perfis de usuários, identificando interesses e comportamentos de navegação;

- Conhecimento (Knowledge):
  - Segmentação de Audiência: Com base no conhecimento adquirido sobre os usuários, a empresa segmenta os perfis em grupos com características semelhantes, como interesses em viagens, esportes ou tecnologia;

- Sabedoria (Wisdom):
  - Publicidade Direcionada: Usando a sabedoria adquirida da segmentação da audiência, a empresa exibe anúncios direcionados a grupos específicos de usuários. Por exemplo, anúncios de equipamentos esportivos para o grupo interessado em esportes.

Portanto, é importante ressaltar que a LGPD vem para resguardar todo o processo, desde a coleta de um dado até qual atitude no mundo será tomada. Os agentes envolvidos nesse processo são os titulares de dados, controladores e operadores, que são:

- Titular de dados é, portanto, a pessoa natural “dona” dos dados; “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”;
- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, ou seja, quem tem poder de mando sobre os dados;
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018).

8. Privacidade e Segurança da Informação

No artigo 5º da Constituição Federal, especificamente no inciso X, encontramos a garantia de proteção à Privacidade. Este dispositivo assegura que a intimidade, a vida

privada, a honra e a imagem das pessoas são invioláveis, e que aqueles que tiverem seus direitos violados têm o direito a receber indenização por danos materiais ou morais resultantes dessa violação. Essa disposição constitucional consagra o direito à privacidade em um sentido amplo, abrangendo todas as manifestações da esfera íntima, privada e da personalidade das pessoas.

Existem diferentes perspectivas em relação à Privacidade na Internet. Alguns acreditam que a internet é um ambiente onde a privacidade é inexistente e seu uso é por conta e risco do usuário, ou seja, ele deve estar ciente dos riscos ao se expor. Por outro lado, há quem defenda que as empresas que mantêm websites devem implementar rigorosos procedimentos de privacidade e serem responsáveis por qualquer invasão de privacidade. Vale ressaltar que existem *websites* em que não é possível controlar o fornecimento de dados, embora tenhamos mais conhecimento sobre *cookies.*

Aqueles que buscam acessar informações privadas podem variar, desde criminosos hackers até empresas de marketing. Logo, a Privacidade tornou-se uma das principais preocupações no desenvolvimento de *software*, principalmente devido às incidências sobre a exploração não autorizada de dados, uso indevido de informações armazenadas em aplicativos de mídias sociais e divulgação de informações pessoais para terceiros sem o consentimento ou até mesmo conhecimento dos titulares.

Um estudo sistemático realizado por Anthony Samy (2017) identificou quatro categorias principais de requisitos de Privacidade, cada uma relacionada à compreensão da natureza e da perspectiva do usuário. Essas categorias são:

- Conformidade: questões legislativas;
- Controle de acesso: etapas de segurança, como verificação em duas etapas;
- Verificação: aplicação de métodos convencionais;
- Usabilidade: como os usuários utilizam das informações que estão em bancos de dados.

Por outro lado, a Segurança da Informação (SI) abrange um conjunto de princípios, técnicas, protocolos, normas e diretrizes com o objetivo de assegurar um elevado grau de confiabilidade. Essa necessidade surgiu em decorrência do amplo intercâmbio de informações entre sistemas computacionais, que engloba desde

transações financeiras até simples trocas de mensagens. A importância da SI é ainda mais evidente devido à vulnerabilidade inerente aos sistemas nesse cenário de troca intensa de dados.

Os ativos são elementos fundamentais da Segurança da Informação, e podem ser divididos em:

- Informações: toda e qualquer informação que a empresa possui, digitalizada ou não;
- *Software*: programas de computador utilizados nos processos de acesso, leitura, transmissão e armazenamento das informações;
- *Hardware*: todos os elementos físicos que apresentam valor importante para uma empresa no que diz respeito à informação; por exemplo, computadores e servidores;
- Usuários: engloba os indivíduos que lidam com as informações no seu dia a dia de trabalho.

A Norma Técnica ISO 27001:2022 tem como finalidade assegurar a confidencialidade, integridade e disponibilidade de um sistema de segurança, sendo: confidencialidade a garantia de que as informações serão acessadas apenas por usuários autorizados; integridade, a garantia de que a informação não foi alterada durante a transmissão, ou seja, ela está exata e completa; por fim, disponibilidade, que é é a garantia de que a informação esteja disponível sempre que necessário.

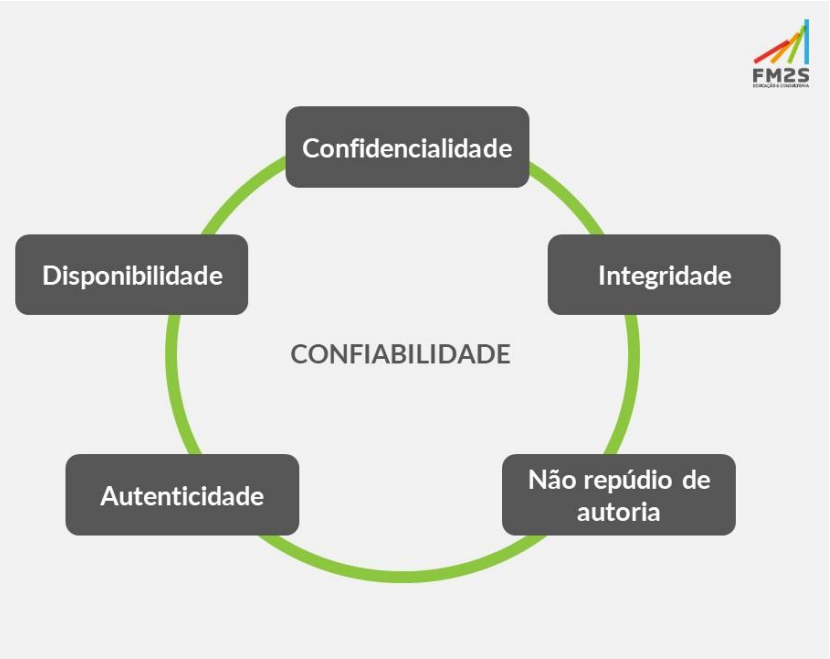
Além dos 3 princípios anteriores, muitos autores também citam a autenticidade e conformidade:

- Autenticidade: é a garantia de que as informações fornecidas são verdadeiras ou que o usuário é o usuário legítimo;
- Não repúdio de autoria: o usuário que gerou ou alterou a informação, não pode negar o fato.

A proteção da informação se faz necessária para qualquer tipo de organização que tem o objetivo de definir os requisitos de privacidade e prover um modelo para

estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI).

Figura 5 - Sistema de Gestão de Segurança da Informação



A LGPD surge, portanto, para garantir tanto o direito à privacidade quanto a segurança da informação. É importante ressaltar que esse cidadão digital, com direito à privacidade e fronteiras não mais definidas apenas pela territorialidade, precisa ter consciência sobre seus direitos em relação aos dados. Aqui entra o papel essencial da conscientização da população. Entra também o conceito de autodeterminação informativa: possibilidade de o indivíduo decidir a quem, quando e em que limites compartilhará aspectos da sua vida privada, incluindo os seus dados pessoais.

9. Ciclo de vida de tratamento de dados: coleta, uso, armazenamento

Considerando o Art. 5º da LGPD, o qual diferencia os tipos de dados e os agentes de tratamento, também é levantado o conceito de tratamento, considerado como: “toda operação realizada com dados pessoais, como as que se referem a coleta, produção,

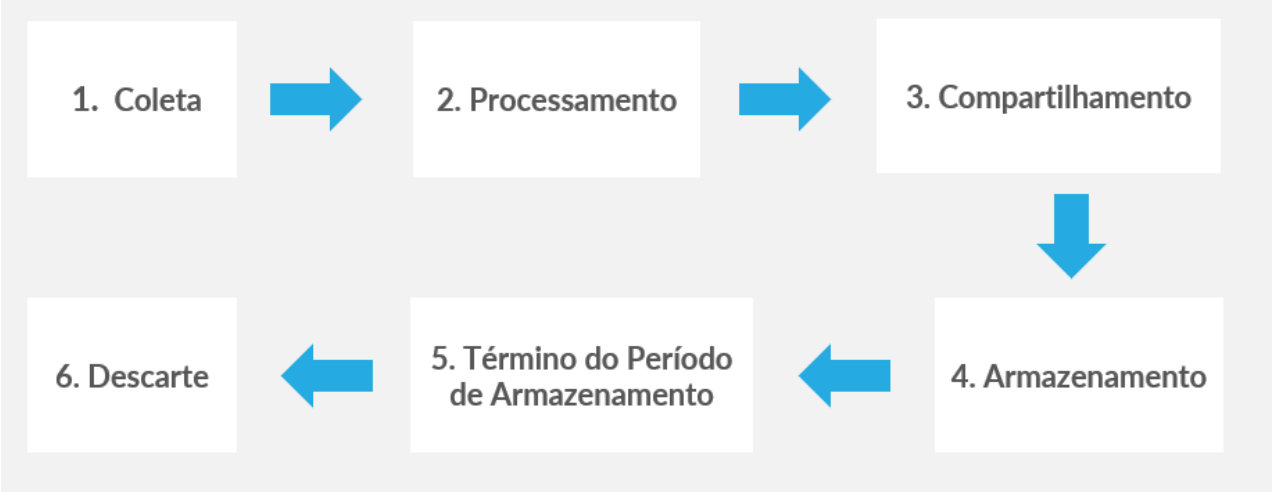
recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (BRASIL, 2018). Ou seja, nesse conceito, não há distinção de tratamento.

Relembrando que:

- Dado pessoal: Informação relacionada a pessoa natural identificada ou identificável;
- Dado pessoal sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- Dado anonimizado: Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- Banco de dados: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Nesse cenário, o Ciclo de Vida do Tratamento de Dados inicia-se com a coleta e se encerra com o descarte, seguindo as etapas ilustradas na figura abaixo. Não necessariamente todas as fases irão ocorrer, mas certamente terá coleta e descarte – fora eles, qualquer operação citada na definição de tratamento poderá ocorrer.

Figura 6 - Ciclo de Vida de Tratamento de Dados

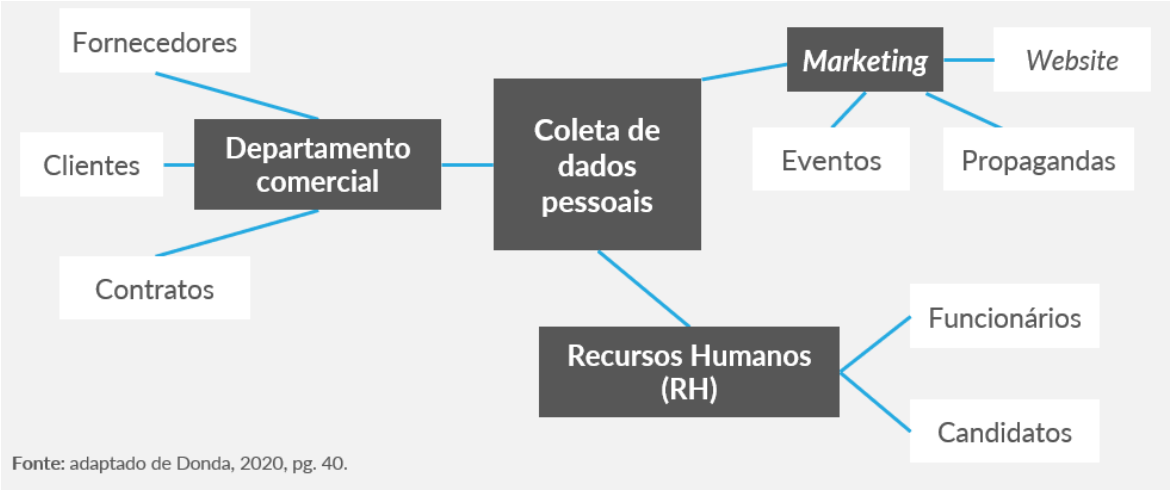


9.1. Coleta de Dados

A coleta de dados são formas pelas quais os dados pessoais são inseridos na empresa. É importante que sejam recolhidos de forma legal (ou seja, com o consentimento do titular) e com transparência com os titulares, seja em formato físico ou digital. Além disso, é necessário identificar os pontos de entrada e os métodos utilizados na coleta dessas informações dentro de sua corporação.

Uma tarefa importante para estar em conformidade com a LGPD envolve a etapa inicial de identificação da Coleta de Dados, que serve como base para a elaboração de um plano de gerenciamento abrangendo todo o Ciclo de Vida dessas informações. A figura abaixo é um exemplo de coleta:

Figura 7 - Fluxograma para coleta de dados



Fonte: adaptado de Donda, 2020, pg. 40.

A figura demonstra que os dados podem entrar a partir de diferentes canais e passar por diferentes áreas, como entrada no departamento comercial e passar para o *marketing* ou Recursos Humanos, cada um com seus interlocutores. Identificar todos os agentes envolvidos é essencial para iniciar a implementação da LGPD.

9.2. Processamento

A fase de processamento se refere à como a empresa irá utilizar os dados, seja qualquer etapa que envolva: classificação, reprodução, processamento, avaliação e controle das informações. É necessário saber quem tem acesso aos dados durante a fase de processamento e se essas pessoas possuem conhecimento de sua responsabilidade em relação às obrigações que a empresa possui.

O processamento pode modificar ou gerar novos dados, por isso a importância relacionada ao cuidado e responsabilidade envolvidos.

9.3. Compartilhamento

Para que ocorra o compartilhamento, deve haver permissão legal para isso (casos de crime ou requisição do poder público justificada), seja porque está previsto por lei ou porque o titular deu o consentimento. O compartilhamento equivale a qualquer operação

de: transmissão, distribuição, comunicação, transferência, difusão e uso compartilhado de dados pessoais.

9.4. Armazenamento

O armazenamento é uma etapa que requer muito cuidado, porque devem ser tomadas cautelas para evitar incidentes de segurança.

O término do período de armazenamento só ocorrerá em determinadas hipóteses, que são:

I. verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II. fim do período de tratamento;

III. comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV. determinação da autoridade nacional, quando houver violação ao disposto na lei.

9.5. Descarte

O descarte deve ser irreversível e extensivo às cópias de segurança. Os dados a serem eliminados podem estar em bases de dados, documentos, equipamentos ou sistemas, mas é importante identificar as unidades organizacionais responsáveis pelo armazenamento dos dados a serem eliminados. Também é necessário considerar os locais físicos onde esses ativos estão localizados para garantir que não haja uma cópia guardada, por exemplo. Se a eliminação ou descarte envolver serviços de armazenamento em nuvem, é necessário considerar os provedores de serviços contratados ou utilizados para descartar inclusive com eles.

Por exemplo:

Imagine a seguinte situação: você possui um comércio de roupas e ao criar a ficha de uma nova cliente, você pede o número de celular. Começam a ser enviadas promoções e novidades para o cliente através desse número informado. Certo dia, cansada com o volume de informações, a cliente solicita a remoção de seu contato, da sua lista de contatos. Você remove o contato, porém, não sabe de uma informação: a

colaboradora que atendeu a cliente em questão, também possui o contato em seu celular. A colaboradora continua enviando informações sobre a loja, pois não foi feita uma varredura adequada para remoção desse contato. É criada uma situação ruim com a cliente, que, agora já não está com a mesma paciência da primeira solicitação.

9.6. Elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

A LGPD prevê a elaboração do Relatório de Impacto à Proteção de Dados Pessoais:

> XVII - relatório de impacto à proteção de dados pessoais (RIPD): 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.
>
> - Brasil, 2018

Esse documento será abordado mais adiante. Porém, já é importante destacar que esse documento é elaborado pelo controlador, quem deverá seguir esse documento à risca.

10. Governança e *Compliance*

Compliance é o conjunto de processos e controles que visam garantir que uma empresa ou organização esteja em conformidade com as leis, normas, regulamentos e padrões éticos aplicáveis à sua atividade e no local que se encontra. O termo *compliance* tem origem no inglês e significa "conformidade".

O *compliance* é um conceito amplo que abrange não apenas a adesão estrita às leis e regulamentações, mas também a adoção de padrões éticos e boas práticas empresariais. Ele envolve a implementação de políticas, procedimentos e controles internos que promovem a transparência, a integridade e a responsabilidade dentro da organização.

Além disso, o *compliance* busca estabelecer uma cultura corporativa que valorize a ética e a conformidade, sendo apenas com isso que ele faz sentido. Isso significa que a conformidade não deve ser apenas uma obrigação imposta de cima para baixo por meio de uma política ou apenas em uma área, mas uma mentalidade compartilhada por todos os membros da organização. É importante criar um ambiente em que os funcionários entendam a importância da conformidade, sejam incentivados a relatar violações e tenham confiança de que suas preocupações serão tratadas de forma adequada.

Complementar a isso, há a governança corporativa, ou seja, o conjunto de práticas e processos que visam garantir a transparência, a prestação de contas e a responsabilidade das empresas em relação aos seus *stakeholders*, como acionistas, clientes, funcionários, fornecedores, comunidade e governo. Por isso, a Governança Corporativa está mais relacionada com a gestão. Essas práticas e processos têm como objetivo proteger os interesses dos *stakeholders*, assegurar que a empresa seja gerida de forma eficiente e ética, e que os resultados financeiros e operacionais sejam alcançados de maneira sustentável a longo prazo.

O *compliance* está relacionado à governança corporativa, pois ambos compartilham o objetivo de garantir a transparência, a ética e o cumprimento das leis e regulamentações nas organizações. Enquanto a governança corporativa abrange a estrutura de tomada de decisões e a supervisão dos processos, o *compliance* está focado em garantir que essas decisões e processos sejam conduzidos de acordo com os requisitos legais e éticos.

Levando para o âmbito da LGPD, pelo seu art. 49, o tratamento dos dados pessoais deve ser estruturado de forma a atender aos padrões de boas práticas e de governança, aparecendo de forma explícita na lei. As diretrizes estabelecidas pela LGPD são essenciais nas operações das empresas, e para garantir sua aplicação adequada, recorre-se ao *compliance*, que tem a responsabilidade de manter as atividades empresariais em conformidade com os parâmetros legais. Em outras palavras, o *compliance* age como o guia para a aplicação da LGPD.

O *compliance* em LGPD, portanto, deve ser um programa que existe para além do papel, mas que também é colocado em prática. Deve ser composto de ações planejadas para evitar violações das informações pessoais. Ademais, a LGPD frequentemente gera dúvidas e complexidades burocráticas, tornando indispensável um departamento de

compliance vigilante e competente, capaz de interpretar e aplicar as normas de forma eficaz. Portanto, para otimizar os processos organizacionais e garantir a continuidade das operações em conformidade com a lei, é crucial que a LGPD e o *compliance* atuem de maneira harmoniosa e complementar.

11. *Stakeholders*

Stakeholders, também conhecidos como partes interessadas, são indivíduos, grupos ou organizações que possuem interesse ou são afetados pelas atividades, decisões e resultados de uma empresa ou organização. Os *stakeholders* podem ter diferentes níveis de envolvimento e influência, e incluem uma variedade de atores, como funcionários, clientes, fornecedores, acionistas, comunidade local, sociedade civil organizada, ONGs, órgãos públicos, entre outros. Eles podem ser classificados de acordo com a Matriz de Classificação de *Stakeholders* a seguir:

Figura 8 - Matriz de classificação de *stakeholders:* interesse x poder

Em relação à LGPD, temos interesse dos funcionários em proteger seus próprios dados e garantir que eles protegem os dados dos clientes; clientes em garantir o uso correto e cômodo de seus próprios dados; gestores em garantir conformidade; assim sucessivamente. Vale-se pensar também nos fornecedores de tecnologias, já que, às vezes, para garantir o cumprimento da LGPD se usa um sistema, que também acaba entrando em contato e armazenando dados.

12. Avaliação de Impacto à Proteção de Dados Pessoais (AIPD)

Avaliação de Impacto à Proteção de Dados Pessoais (AIPD) tem como objetivo auxiliar na identificação e minimização de riscos à proteção de dados por meio da documentação da descrição dos processos de tratamento de dados. Claro que ela não pode ser apenas um documento, ele deve funcionar na prática. Ela orienta os controladores para as soluções mais adequadas, já que é conduzido pelo controlador e beneficiado pela consultoria dos *stakeholders* e *experts*.

O processo de AIPD é caracterizado também como forma de autorregulação e demonstração voluntária de *compliance* com princípios gerais de privacidade (WRIGHT, 2012), o que possibilita aos agentes envolvidos capitanear o desenvolvimento de procedimentos nacionais baseados em boas práticas discutidas na literatura. Vale ressaltar que a Avaliação de Impacto à Privacidade (AIP) ou *Privacy Impact Assessment* ou RIPD são sinônimos da AIPD.

A LGPD define o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como a documentação dos riscos aos direitos fundamentais resultantes do tratamento de dados pessoais e das medidas de mitigação. O processo e obrigatoriedade não são detalhados na LGPD, deixando a ANPD responsável por orientar e solicitar o RIPD quando necessário.

Conforme o art. 38 da LGPD, o RIPD deverá conter, pelo menos, os seguintes itens aprovados pelo controlador:

- a descrição dos tipos de dados pessoais coletados e tratados de qualquer forma;

- a metodologia usada para o tratamento e para a garantia da segurança das informações; e
- a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Para a sua elaboração, é necessário:

1. Identificar os agentes de tratamento e o encarregado;
2. Identificar outras partes interessadas/envolvidas;
3. Avaliar a justificativa da necessidade de elaborar ou atualizar o relatório;
4. Descrever o tratamento de dados;
5. Analisar a base legal;
6. Analisar os princípios da LGPD;
7. Avaliar os riscos identificados;
8. Estabelecer medidas, salvaguardas e mecanismos de mitigação de risco;
9. Coletar comentários e aprovações;
10. Monitorar e atualizar.

13. Autoridade Nacional de Proteção de Dados

A Autoridade Nacional de Proteção de Dados (ANPD) é o principal órgão regulador brasileiro. A criação dela não estava prevista na redação original do projeto de lei, ou seja, não havia nenhuma previsão sobre quem iria fazer a fiscalização ou monitoramento. E, como se sabe que o que garante a aplicabilidade da lei é o seu caráter coercitivo, foi-se necessário retomar essa discussão.

Assim, devido a debates sobre o formato de funcionamento, embora tenha sido formalmente criada pela Medida Provisória n. 869/2018 em 27 de dezembro de 2018, a ANPD só começa a operar em novembro de 2020, quando foram empossados seus primeiros diretores.

As suas funções trazidas pela Lei são:

I - zelar pela proteção dos dados pessoais, nos termos da legislação;

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

XII - elaborar relatórios de gestão anuais acerca de suas atividades;

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para

os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

- Brasil, 2018

14. Direitos e Casos Particulares

De acordo com a LGPD, o tratamento de dados pessoais é permitido apenas nas seguintes hipóteses:

- Consentimento do titular dos dados;
    - Fornecer por livre e espontânea vontade uma autorização prévia e expressa;
- Cumprimento de obrigação legal ou regulatória;
- Execução de contrato;
    - Efetivação do contrato sendo o titular um dos contratantes;
- Exercício regular de direitos em processo judicial, administrativo ou arbitral;
    - Vale a observação de que um processo pode ocorrer por uma Câmara Arbitral, menos conhecido por conta do custo aqui no Brasil, que é um tipo de judiciário privado;
- Proteção da vida ou da incolumidade física do titular ou de terceiros, desde que justificado e comprovado;
- Tutela da saúde, em procedimento realizado por profissionais de saúde ou por entidades sanitárias;
- Interesse legítimo do controlador ou de terceiro, desde que prevaleçam os direitos e liberdades fundamentais do titular, que exijam a proteção dos dados pessoais.

Além disso, a lei prevê uma série de direitos aos titulares de dados, ou seja, aqueles que são donos dos dados. Eles são:

- **Direito de Acesso:** os titulares têm o direito de obter informações sobre o tratamento de seus dados pessoais, incluindo quem está tratando, para quais fins e quais dados estão sendo utilizados, sendo amplo e irrestrito;
- **Direito de Retificação**: os titulares podem solicitar a correção de dados pessoais imprecisos ou desatualizados;
- **Direito de Exclusão**: também conhecido como "direito ao esquecimento", os titulares podem solicitar a exclusão de seus dados pessoais, a menos que haja uma justificativa legal para sua retenção.
- **Direito à Portabilidade**: os titulares têm o direito de receber seus dados pessoais em um formato estruturado e de uso comum, permitindo a transferência para outro controlador, se desejado;
- **Direito de Oposição**: os titulares podem se opor ao tratamento de seus dados pessoais em algumas situações específicas, como *marketing* direto;
- **Direito à Revogação de Consentimento**: os titulares podem retirar seu consentimento a qualquer momento, sem que isso afete a legalidade do tratamento realizado antes da retirada;
- **Direito à Informação**: os titulares têm direito a informações claras e acessíveis sobre o tratamento de seus dados pessoais;
- **Direito à Revisão de Decisões Automatizadas**: quando as decisões são tomadas com base unicamente em processamento automatizado de dados pessoais, os titulares têm o direito de revisar essas decisões.

A LGPD estabelece restrições especiais para o tratamento de dados sensíveis, que são categorias especiais de dados pessoais que exigem maior proteção. Isso inclui informações como raça, origem étnica, crenças religiosas, orientação sexual, saúde, entre outras. Dessa forma, o tratamento de dados sensíveis pode ocorrer em hipóteses de conflito de direitos, ou seja:

- Quando o titular der consentimento explícito, para finalidades específicas;
- Para o cumprimento de obrigações legais ou regulatórias;

- Em casos de tutela da saúde, em procedimento realizado por profissionais de saúde ou entidades sanitárias;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiros, quando o titular estiver incapacitado de dar consentimento;
- Para a realização de estudos por órgãos de pesquisa, desde que garantidas medidas de anonimização dos dados.

15. Agentes no tratamento de dados

A Lei determina tipos de agentes de acordo com as suas responsabilidades e níveis de controle em relação aos dados. Agentes de tratamento incluem o controlador e o operador de dados pessoais, podendo ser pessoas naturais ou jurídicas, tanto de direito público quanto privado. A definição deles deve considerar seu caráter institucional, ou seja, em determinado banco de dados um agente pode ser considerado controlador; em outro, não poderá atuar como tal.

Não são considerados controladores ou operadores os indivíduos subordinados, como funcionários ou servidores públicos. Isso ocorre porque eles atuam sob o poder diretivo do agente de tratamento.

15.1. Controlador

Controlador é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento de maneira autônoma. De acordo com a Lei:

> Art. 5º, VI, da LGPD: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
>
> - Brasil, 2018

É responsável por elaborar relatório de impacto à proteção de dados pessoais, comprovar que o consentimento obtido do titular atende às exigências legais e comunicar

à ANPD a ocorrência de incidentes de segurança. Ou seja, o controlador tem um poder diretivo em relação ao controle dos dados e responde por isso.

A seguir, alguns exemplos que demonstram quem pode assumir o papel de controlador a depender do cenário:

- Exemplo 1 - Médica profissional liberal
    - Uma médica, profissional liberal, armazena os prontuários e os demais dados pessoais de seus pacientes no computador de seu consultório. A médica, pessoa natural, é a controladora dos dados pessoais;
- Exemplo 2 - Médica colaboradora de um hospital
    - Uma médica é colaboradora de um hospital, constituído sob a forma de associação civil sem fins lucrativos;
    - Nessa condição, atua como principal representante do hospital junto a um serviço de armazenamento de dados de pacientes em nuvem, inclusive assinando os contratos correspondentes;
    - O hospital, isto é, a associação civil, pessoa jurídica de direito privado, é o controlador na hipótese. A médica, por atuar sob o poder diretivo da organização, não se caracteriza como agente de tratamento;
- Exemplo 3 - Órgão público contratante de um serviço de inteligência artificial
    - Um órgão público, vinculado à União, contrata uma solução de IA fornecida por uma sociedade empresária com a finalidade de realizar o tratamento automatizado de decisões com base em um banco de dados gerido pelo órgão;
    - Seguindo o estabelecido em contrato, a sociedade empresária realiza as operações necessárias para viabilizar o tratamento dos dados em questão. A União é a controladora na hipótese. O órgão público responsável detém obrigações legais específicas, conforme previsto na LGPD;
    - A sociedade empresária é a operadora, uma vez que realiza o tratamento dos dados conforme as instruções fornecidas pelo controlador. Por fim, o gestor público responsável, por atuar como servidor público subordinado à União, não se caracteriza como agente de tratamento.

15.2. Operador

Em relação ao outro agente de tratamento de dados, a LGPD traz as seguintes definições:

> Art. 5º, X, da LGPD: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> Art. 39 da LGPD: o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.
>
> - Brasil, 2018

Por isso, o operador não pode agir de maneira autônoma, devendo sempre seguir as instruções do controlador. Suas obrigações incluem: (i) seguir as instruções do controlador; (ii) firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador; (iii) dar ciência ao controlador em caso de contrato com o sub operador.

A seguir, veremos alguns exemplos:

- Exemplo 1 - E-commerce
    - Em um canal de venda online de livros, que conta com diversas formas de pagamento, o canal que realiza a venda é o controlador dos dados pessoais,
    - Cada serviço de pagamento disponível será um operador diferente, como, por exemplo, a empresa de cartão de crédito, uma fintech, o banco em caso de transferência bancárias, dentre outros.
    - O operador dessa transação, seja ele qual for, não poderá utilizar os dados fornecidos para novas finalidades que não aquelas determinadas pelo controlador.
- Exemplo 2 - Call center

- A empresa XRAY tem sob sua responsabilidade os dados de seus clientes e repassa para uma empresa terceirizada de call center, ZULU, que recebe as informações.
- A empresa XRAY é a controladora e o call center terceirizado ZULU, o operador, que executará o tratamento de dados dos clientes a mando da empresa XRAY.
- Caso realize o tratamento de dados fora do que foi orientado pelo controlador, a empresa ZULU poderá ser responsabilizada.

15.3. Sub Operador

Formalmente, a LGPD, no que se refere aos agentes de tratamento, definiu apenas as figuras do controlador e do operador (art. 5º, incisos VI, VII e IX). Muito embora não exista um conceito de Sub Operador na LGPD, o tema pode ser utilizado como parâmetro de análise para compreensão de cadeias mais complexas de tratamento de dados.

O Sub Operador é aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador, como se fosse a terceirização dos serviços, conforme pode ser observado no exemplo a seguir:

- Exemplo - Sorteio de Loja
  - A loja KILO organiza um sorteio e, para concorrer, os clientes preenchem um cadastro com algumas informações pessoais. Os dados e a finalidade do tratamento foram definidos pela loja KILO, que é a controladora.
  - A guarda e a coleta desses dados são realizadas, por funcionários da loja KILO, no sistema da empresa LIMA. A empresa LIMA é a operadora.
  - Ao fim do período de inscrição, a loja OSCAR contrata a empresa LIMA para realizar o sorteio usando os dados guardados pela empresa LIMA. A empresa OSCAR também é uma sub operadora.

16. *Data Protection Officer* (DPO)

O *Data Protection Officer* (DPO) ou encarregado de dados possui a função de atuar como canal de comunicação entre a instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). As informações sobre essa função devem constar no site da organização, sendo que, no caso de repartições públicas, devem ser oficializadas por meio de uma publicação.

Pelo Art. 41. da LGPD, o controlador deverá indicar encarregado pelo tratamento de dados pessoais, sendo o indivíduo (pessoa física ou jurídica) responsável por garantir a conformidade de uma organização, pública ou privada, à LGPD. A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

O encarregado pelo tratamento de dados pessoais Suas atribuições incluem, pelo Artigo 41, §2º, da LGPD:

> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
>
> II - receber comunicações da autoridade nacional e adotar providências;
>
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
>
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
>
> - Brasil, 2018

Importante ressaltar que nem toda empresa precisa de um DPO, apenas as de grande porte. Por uma resolução CD/ANPD nº 2/2022: agentes de tratamento de pequeno porte não precisam indicar DPO, mas sim disponibilizar um canal com o titular de dados, porque isso tem a ver com natureza e porte da entidade ou volume de operações de tratamento de dados. Entretanto, a indicação de encarregado por parte dos

agentes de tratamento de pequeno porte será considerada política de boas práticas e governança.

Um DPO é diferente de uma ouvidoria, uma vez que essa é uma função ou departamento em uma organização, seja pública ou privada, que atua como um canal de comunicação independente entre a organização e o público em geral. O principal objetivo de uma ouvidoria é receber, investigar e resolver reclamações, sugestões, elogios, críticas e outras manifestações dos clientes, usuários, cidadãos ou partes interessadas que estão interagindo com a organização.

Vale a pena ressaltar que, por se tratar de um canal de comunicação direto com o público, a ouvidoria também deve se adequar à LGPD. Algumas empresas colocam o ouvidor como DPO, mas vale ressaltar que receber reclamações e feedbacks dos titulares de dados é apenas uma das funções do DPO. O canal de comunicação do ouvidor é mais amplo.

17. Transferências Internacionais

Vamos explorar os Artigos da Lei Geral de Proteção de Dados (LGPD) que se relacionam com a 'transferência internacional de dados', começando pela definição básica: “transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro” (BRASIL, 2018). Ou seja, organismos públicos e privados também podem realizar a transferência de dados.

Essas transferências são permitidas nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - 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;

III - 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;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - 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;

VIII - 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

IX - quando necessário para atender às hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

- Brasil, 2018.

Por outro lado, em relação ao nível de proteção do país que receberá as informações de origem brasileira, a Autoridade Nacional deverá levar em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

18. Responsabilidade e Ressarcimento de Danos

Passando para a Seção III da LGPD, a qual aborda a Responsabilidade e Ressarcimento de Danos, há algumas diretrizes caso haja dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, sendo obrigado a repará-lo. Vale ressaltar que, no Direito, quem alega, deve provar. Ou seja, para que haja um processo, é necessário que o titular prove o dano.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

Seção I - Das Sanções Administrativas

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;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

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;

X - 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;

XI - 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;

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

- Brasil, 2018

19. Apresentação do passo a passo

Apresentaremos a seguir o passo a passo que será visto nesta parte do curso para a implementação da Lei Geral de Proteção de Dados:

1. Treinar os colaboradores com campanhas de conscientização
2. Realizar auditoria Interna
3. Criar um Comitê
4. Identificar os riscos
5. Analisar os riscos
6. Tratar os riscos
7. Monitoramento e Manutenção das práticas de proteção de dados

20. Passo 1 - Treinar os colaboradores com campanhas de conscientização

Para se iniciar um projeto de implementação da LGPD, é preciso criar uma cultura de proteção de dados para evitar qualquer resistência dos colaboradores e demonstrar seriedade. Além disso, é preciso ter avaliação inicial de abertura; compromisso da alta gerência; recursos e orçamentos adequados e controle de documentos.

Para se iniciar um projeto de treinamento, o Controlador deve entender qual é o nível de maturidade atual da organização. Para isso, Humberto de Jesus Ortiz Rodrigues elabora 10 questionamentos:

1. A empresa tem uma cultura de privacidade e proteção de dados desenvolvida?
2. A empresa tem uma política de privacidade e proteção de dados?

3. A empresa tem mecanismos de segurança da informação?
4. A empresa tem uma arquitetura de dados implementada?
5. As atividades em que são tratados dados pessoais e a finalidade, adequação e necessidade desses tratamentos estão identificadas pela empresa?
6. A empresa tem um protocolo para agir perante a ocorrência de um incidente com dados pessoais?
7. A empresa tem um comitê de direção ou orientação para gerir o tratamento de dados pessoais?
8. A empresa tem planos de comunicação e treinamentos sobre privacidade e proteção de dados estabelecidos?
9. Quais obrigações tem a empresa com a entrada em vigor da LGPD?
10. A empresa conhece todas as adequações e mudanças que tem que implementar em seus processos para agir de forma adequada no tratamento de dados pessoais? (OLIVEIRA, 2022, apud RODRIGUEZ, 2020)

Existem dois tipos de treinamentos necessários para a implementação:

- Treinamentos para fornecedores e partes interessadas;
- Treinamento de conscientização sobre LGPD e Segurança da Informação.

20.1. Exemplo 1 - Treinando os colaboradores

Em uma indústria de roupas esportivas em fase de crescimento, a privacidade e a proteção de dados estavam começando a se tornar uma prioridade. A empresa estava no processo de implementação da Lei Geral de Proteção de Dados (LGPD), mas ainda havia muito trabalho a fazer. Para isso, eles decidiram usar um checklist para identificar suas necessidades de treinamento e desenvolvimento.

- ☐ A empresa tem uma cultura de privacidade e proteção de dados desenvolvida?
- ☑ ~~A empresa tem uma política de privacidade e proteção de dados?~~
- ☑ ~~A empresa tem mecanismos de segurança da informação?~~

- ☑ ~~A empresa tem uma arquitetura de dados implementada?~~
- ☐ As atividades em que são tratados dados pessoais e a finalidade, adequação e necessidade desses tratamentos estão identificadas pela empresa?
- ☐ A empresa tem um protocolo para agir perante a ocorrência de um incidente com dados pessoais?
- ☐ A empresa tem um comitê de direção ou orientação para gerir o tratamento de dados pessoais?
- ☐ A empresa tem planos de comunicação e treinamentos sobre privacidade e proteção de dados estabelecidos?
- ☐ A empresa conhece todas as adequações e mudanças que tem que implementar em seus processos para agir de forma adequada no tratamento de dados pessoais?

O primeiro desafio era estabelecer uma cultura de privacidade e proteção de dados dentro da empresa. O checklist revelou que essa cultura ainda não estava bem desenvolvida. Para enfrentar esse desafio, a alta administração decidiu que era hora de conscientizar todos os colaboradores sobre a importância da privacidade e dos dados pessoais.

Para criar uma cultura de privacidade, a empresa organizou palestras e workshops para todos os funcionários. Eles compartilharam histórias reais sobre violações de dados e explicaram como cada colaborador desempenhava um papel crucial na proteção das informações pessoais dos clientes. Isso começou a criar uma compreensão mais profunda e um senso de responsabilidade em toda a organização.

O próximo desafio era a falta de um protocolo claro para agir em caso de incidente com dados pessoais. A empresa percebeu que precisava ter diretrizes claras sobre como lidar com violações de dados, conforme apontado no checklist.

A equipe de segurança da informação trabalhou duro para criar um protocolo abrangente de incidentes com dados pessoais. Eles treinaram pessoal de todas as áreas da empresa sobre como identificar, relatar e mitigar incidentes de privacidade. Isso deu à equipe a confiança necessária para lidar com qualquer problema que surgisse.

O checklist também destacou a falta de um comitê de direção ou orientação para gerenciar o tratamento de dados pessoais. A empresa sabia que era fundamental envolver a liderança para garantir o sucesso na proteção de dados.Por isso, alta administração decidiu formar um comitê de direção dedicado à gestão de dados pessoais. Eles escolheram membros com conhecimento especializado em privacidade e dados, garantindo que a empresa tivesse a orientação adequada.

Com uma política de proteção de dados interna e uma arquitetura de dados parcialmente implementada, a empresa queria estruturar treinamentos eficientes para seus colaboradores. Eles definiram objetivos de treinamento claros, focando em conscientizar os funcionários sobre como implementar a política de proteção de dados. Em vez de palestras teóricas, eles optaram por demonstrações práticas, usando a arquitetura de dados da empresa como exemplo. Isso tornou o treinamento mais envolvente e relevante para a equipe.

No final dessa jornada, a indústria passou de uma empresa que estava apenas começando a entender a importância da proteção de dados para uma organização comprometida em garantir a privacidade de seus clientes. A proteção de dados se tornou uma parte essencial do DNA da empresa, garantindo a confiança dos clientes e o contínuo sucesso nos negócios.

21. Passo 2 - Realizar auditoria Interna

Auditoria é um processo sistemático, independente ou não e documentado para obter evidência objetiva e avaliá-la objetivamente para determinar a extensão na qual os critérios de auditoria são atendidos. Esses critérios podem ser abrangentes, mas como o objeto do curso é a Lei Geral de Proteção de Dados, em sua maioria se considera os dados pessoais. Os elementos fundamentais de uma auditoria incluem a determinação da conformidade de um objeto, de acordo com um procedimento realizado por pessoal não responsável pelo objeto auditado, ou seja, se, por exemplo, a área jurídica de uma empresa for auditada, o advogado dela não pode ser responsável pela auditoria.

De acordo com a norma ABNT NBR ISO 9000:2015, auditorias internas são algumas vezes denominadas auditorias de primeira parte e são conduzidas pela própria organização para análise crítica pela direção ou para outros propósitos internos e podem

formar a base para uma declaração de conformidade da organização. A independência pode ser demonstrada pela ausência de responsabilidade em relação à atividade que está sendo auditada.

O papel da Auditoria Interna é servir à alta administração, auxiliando no controle de ativos, o acompanhamento de processos e o cumprimento de normas internas; fazer recomendações para melhorias quando necessário; ser os "olhos e ouvidos" da alta administração e ter acesso livre a todas as áreas da empresa. Tudo isso permite que apoiem as operações financeiras e administrativas e inspecionem outros processos transacionais e não transacionais da empresa. A tabela a seguir ilustra os diferentes tipos de auditoria:

Figura 9 - Tipos de Auditoria - Fonte: Fonte: Santos, 2019, pg. 10.

Tipo de Auditoria	**Natureza das afirmações**	**Critérios estabelecidos**	**Natureza do parecer do auditor**
De demonstrações contábeis	Dados das demonstrações contábeis.	Princípios contábeis geralmente aceitos.	Opinião a respeito da adequação das demonstrações contábeis.
De Compliance	Direitos ou dados relacionados com obediência a políticas, leis, regulamentos etc.	Políticas da administração, leis, regulamentos ou outras exigências por terceiros.	Resumo dos resultados ou segurança a respeito do grau de obediência
Operacional	Dados operacionais ou de desempenho.	Objetivos estabelecidos pela administração ou pela legislação.	Eficiência e eficácia observadas; recomendações

			para aperfeiçoamento.

O auditor realiza as seguintes funções operacionais:

- Realizar o exercício inicial de coleta de informações de dados pessoais;
- Realizar auditoria de dados pessoais por área de negócios;
- Identificar base Conselheiro Jurídico para o tratamento de dados pessoais em cada caso;
- Realizar avaliações de interesse legítimo quando necessário;
- Identificar requisitos e procedimentos de manutenção de registros.

No material do curso tem um arquivo denominado **[FM2S] Template - Inventário dos dados pessoais** – Este template está disponível para que você possa utilizá-lo para mapear, no passe de auditoria interna, os processos que realizam tratamento de dados pessoais.

22. Passo 3 - Criar um Comitê

Antes da LGPD, poucas empresas estavam preocupadas com o tema “privacidade”, porém essa situação mudou e está mudando aos poucos. Por isso, é essencial definir quem será o responsável pelo assunto, pois, além de ser uma exigência da LGPD, permite centralizar o controle das atividades do projeto de implementação. Assim surgem os Comitês, que devem olhar para esse assunto de forma recorrente e se dedicar para isso.

Esse profissional, deve possuir uma interação entre as áreas de negócios com o jurídico e a TI/SI, visando ao atendimento dos requisitos da LGPD. Mesmo que não haja uma área responsável por esses tópicos, como nos casos de uma empresa de pequeno porte, é necessário que o Comitê faça a interlocução entre os responsáveis por eles. Vale desmistificar que é irrelevante se é um advogado ou técnico: sua maior competência

deve superar o conhecimento tradicional, impondo-se como um integrador de diferentes conhecimentos para obter o resultado desejado.

A criação de um Comitê para atuar em assunto que envolve a privacidade, deve-se levar em conta o seguinte contexto:

- Um grupo de trabalho para atuar no projeto de implementação deve ter um perfil específico para atender ao objetivo do projeto, ou seja, a implementação da conformidade à LGPD;
- Já um comitê definido para tratar do assunto privacidade pode ter outro perfil, com objetivo mais estratégico de viabilizar de fato a proteção dos dados.

Caso a empresa em questão tenha poucos funcionários, alguns questionamentos sobre a relevância de um Comitê devem ser feitos. Como instituir um Comitê em uma empresa com 20 funcionários? Considerando que nossa organização permita a atuação de um comitê de privacidade, qual seria seu papel? Alçada? Responsabilidades? Seus membros participariam de reuniões semanais, mensais, semestrais? Como formalizar e disciplinar o relacionamento entre o comitê, seus membros e a organização?

Embora seja recomendável que o Comitê seja permanente, ou seja, que ele não se dissolva, ele não requer dedicação exclusiva e diária. Uma vez implementadas todas as ações que garantem o cumprimento da LGPD, resta o monitoramento, que pode ser semanal, por exemplo. Vale ressaltar que o Comitê também pode ser rotativo.

Por ser de responsabilidade do Comitê, é importante ressaltar a definição de Política de Privacidade. Uma Política é um documento que define diretrizes, normas e procedimentos para alcançar um objetivo específico. No contexto de proteção de dados e informações pessoais, a Política visa proteger essas informações de clientes, colaboradores, parceiros e fornecedores. A "política de privacidade" esclarece responsabilidades, funções, prazos e processos relacionados à gestão da privacidade na organização. Engloba tudo o que for necessário para orientar as atividades de gestão da privacidade em uma organização.

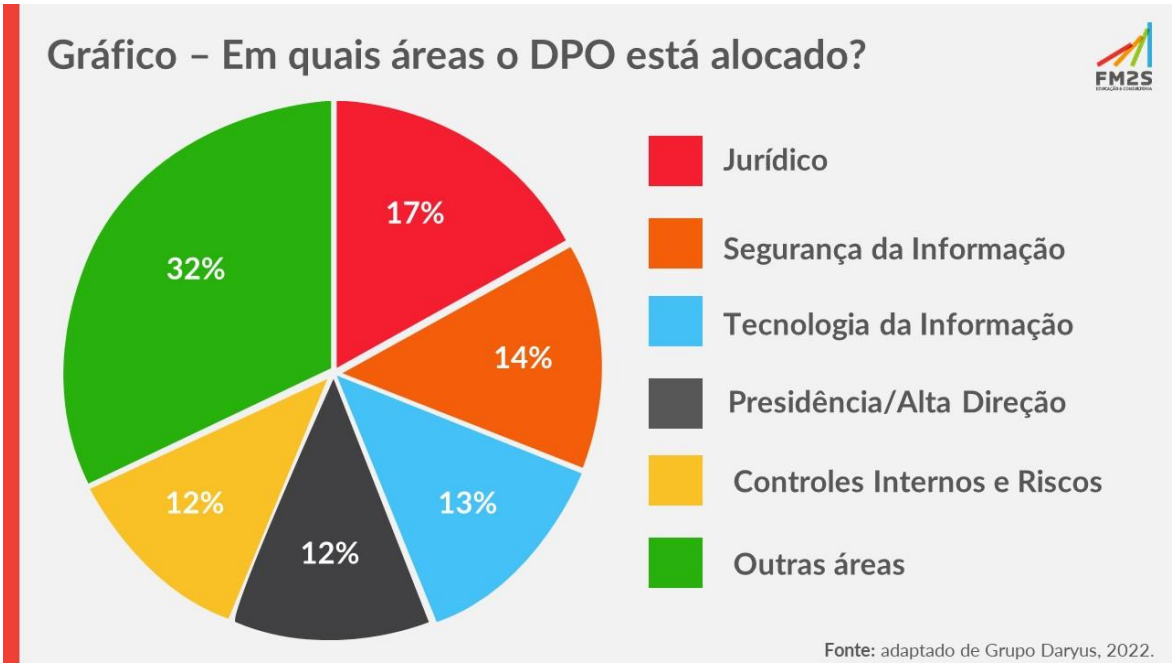
É importante que o Comitê seja composto por:

- O DPO (se necessário);
- Controladores: Pode ser interno, como um RH;
- Operadores: Externo à organização controladora;

- Profissionais da área de TI que lidam diretamente com o armazenamento dos dados;
- Outros setores podem participar, pensando em melhorias dos processos.

A seguir, um gráfico que reúne dados da Pesquisa do Grupo Dayrus acerca das áreas em que um DPO geralmente está alocado, mas isso pode variar de acordo com a empresa:

Figura 10 - Quais áreas que o DPO está alocado? - Fonte: adaptado de Grupo Daryus, 2022.



O Comitê tem como funções:

- Avaliar os mecanismos de tratamento;
- Propor políticas, estratégias e metas;
- Elaborar manual/POP/guia para a consolidação das normas;
- Definir política de privacidade;
- Promover intercâmbio de informações.

É preciso ter em mente, por fim, que nada deve ser feito da noite para o dia. Trata-se da criação de um processo, que será amadurecido à medida que for evoluindo para as próximas fases de adequação à LGPD.

Para ilustrar a criação de um Comitê, trazemos como exemplo o Comitê Gestor da Privacidade e Proteção de Dados da Unicamp, que tem como responsabilidade garantir o cumprimento da LGPD e da LAI (Lei de Acesso à Informação). Ele tem como competência e membros:

Artigo 3º - Compete ao Comitê Gestor de Proteção de Dados:

I. propor e implementar a Política de Privacidade, instruções normativas, requisitos metodológicos, cronogramas e planos com objetivo de regulamentar a privacidade e a proteção dos dados pessoais no âmbito da Universidade Estadual de Campinas;

II. avaliar os procedimentos de tratamento e proteção dos dados existentes e propor estratégias e metas em observância a LGPD;

III. revisar a Política de Privacidade e as instruções normativas a cada 3 (três) anos, prazo máximo;

IV. promover ações de sensibilização junto à comunidade universitária, aos órgãos administrativos e aos parceiros da universidade sobre a aplicação da política e normas relacionadas à privacidade e proteção de dados;

V. planejar e coordenar a implantação do Programa de Privacidade, ações e projetos necessários para a adequação à LGPD;

VI. acompanhar a implantação dos planos e o cumprimento das ações regulamentadoras nos diversos órgãos da Universidade;

VII. receber comunicações de descumprimento das normas referentes à Política de Privacidade e Proteção de Dados, instruí-las com os elementos necessários à sua análise e notificar os responsáveis;

VIII. articular o intercâmbio de informação sobre a proteção de dados pessoais com outros órgãos públicos.

Artigo 4º - O Comitê Gestor da Privacidade e Proteção de Dados, de natureza permanente, consultivo-deliberativa, tem responsabilidade estratégica e será composto pelo Encarregado, conforme descrito na Lei Geral de Proteção de Dados Pessoais no artigo 5º inciso VIII, e por representantes dos seguintes órgãos:

I. 01 representante da Coordenadoria Geral da Universidade – CGU;

II. 02 representantes da Gestão Estratégica de Dados;

III. 01 representante da Pró-Reitoria de Pesquisa – PRP;

IV. 01 representante da Diretoria Geral de Recursos Humanos – DGRH;

V. 01 representante da Diretoria Acadêmica – DAC;

VI. 01 representante da Diretoria Geral de Administração – DGA;

VII. 01 representante do Centro de Computação – CCUEC;

VIII. 01 representante do Sistema de Arquivo Central da Unicamp – Siarq;

IX. 01 representante da Comissão de Vestibular – Comvest;

X. 01 representante do Serviço de Informação ao Cidadão – SIC;

XI. 01 representante dos órgãos da Área da Saúde;

XII. 01 representante da Procuradoria Geral – PG.

- Deliberação CAD-A-003/2020

23. Passo 4 - Identificar os riscos

A identificação de riscos envolve a busca, reconhecimento e descrição de potenciais ameaças, sendo guiada pelo contexto estabelecido e envolve comunicação e consulta às partes interessadas. O objetivo principal é criar uma lista abrangente de riscos que possam afetar os objetivos de diversas maneiras, o que inclui riscos que podem aumentar, evitar, reduzir, acelerar ou atrasar o alcance dos objetivos, bem como riscos relacionados à decisão de não buscar oportunidades.

A identificação adequada é fundamental, pois é um pré-requisito essencial para a gestão e tratamento posterior desses riscos. A identificação de riscos pode ser fundamentada em diversos elementos, como dados históricos, análises teóricas, insights

de indivíduos bem-informados e especialistas, além das necessidades das partes interessadas.

Nesta etapa, é imperativo esclarecer os seguintes aspectos:

- O escopo do processo, projeto ou atividade abrangido pelo processo de identificação;
- Os participantes envolvidos no procedimento de identificação dos riscos, já que são eles quem mais conhecem o processo e sabem onde há uma possibilidade de vazamento;
- A metodologia ou abordagem adotada para identificar os riscos;
- As fontes de informação consultadas;
- A elaboração de uma descrição detalhada para cada risco, incluindo a fonte de origem do risco, suas causas subjacentes, o evento potencial e as consequências associadas a ele.

Existem algumas formas de identificar os riscos. A primeira a ser citada é a Lista de Verificação, que é uma ferramenta simples que consiste em uma lista de perguntas ou itens que podem ser usados para ajudar na identificação de riscos em um projeto, processo ou atividade, ajudando a garantir que nenhum risco importante seja esquecido ou ignorado. Há também a classificação: é uma ferramenta que ajuda a categorizar e classificar os riscos identificados com base em sua natureza, origem ou impacto, ajudando a identificar os padrões e tendências dos riscos e a priorizando a alocação de recursos para a gestão de riscos.

Podemos citar alguns exemplos de riscos:

- *Malwares* (códigos maliciosos): termo genérico que abrange todos os tipos de programas especificamente desenvolvidos para executar ações maliciosas em um computador. Alguns exemplos são: Vírus; *Worms* e *Bots*; Cavalos de Tróia; *Spyware; Ransomware*.
    - Vírus: é um programa, ou parte de um programa, que cria cópias de si mesmo e infecta outros programas e arquivos de um computador. Ele não é auto suficiente, precisa de um programa/arquivo hospedeiro;

- *Worms*: programa independente com capacidade de se autopropagar através de redes, de computador para computador. Não necessita ser executado para se propagar e não precisa de hospedeiro como o vírus;
- *Bots*: programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente;
- Cavalo de Tróia (*Trojans*): são programas introduzidos no computador com o objetivo de controlar o seu sistema. Normalmente, recebido como um "presente": cartão virtual, fundo de tela, jogos, etc.;
- *Spyware* (espião): consiste em um programa que recolhe informações sobre o usuário e seus costumes na internet e transmite à uma entidade externa, sem que o usuário saiba;
- *Ransomware*: código malicioso que torna inacessíveis os dados armazenados em um equipamento (geralmente por criptografia), e exige pagamento de resgate para restabelecer o acesso ao usuário.

- *Phishing*: é uma forma de engenharia social, com objetivo de roubar informações valiosas para uso posterior em roubo ou fraude.
  - O golpe de *Phishing* envolve a criação de um *website* falso ou o envio de mensagens eletrônicas falsas;
  - Isso geralmente ocorre por meio de e-mails ou mensagens em redes sociais;
  - Os golpistas se passam por instituições conhecidas, como bancos ou empresas populares;
  - Eles tentam induzir as vítimas a acessar páginas falsas, onde podem roubar informações confidenciais dos usuários.
- Acesso indevido a dados pessoais: Dar acesso a pessoas não autorizadas, seja por ameaça externa ou interna;
- Perda de dados pessoais: Incidentes que envolvam perda de dados, como em mudanças de sistemas e infraestrutura.

Para ilustrar ainda mais os riscos envolvidos, a seguir temos um exemplo de Mariana:

Mariana sempre foi apaixonada por moda e decidiu transformar sua paixão em uma loja de roupas virtual. O negócio cresceu rapidamente, e Mariana estava entusiasmada com seu sucesso. No entanto, ela sabia que, com grande poder vem grande responsabilidade, especialmente quando se tratava da privacidade dos clientes.

Mariana entendia que, como proprietária de um e-commerce, ela tinha acesso a uma grande quantidade de informações pessoais de seus clientes, como nome, CPF, lista de compras e endereço. Ela estava comprometida em garantir que esses dados fossem tratados com o devido cuidado e responsabilidade.

Um dia, Mariana decidiu realizar uma auditoria em sua empresa para avaliar a conformidade com a Lei Geral de Proteção de Dados (LGPD). Ela queria garantir que sua loja estava alinhada com as melhores práticas de privacidade e segurança de dados. Durante a auditoria, Mariana identificou dois riscos potenciais:

1. Risco de Transferência:

Ela percebeu que, como sua loja terceirizava as entregas para outra empresa, precisava compartilhar informações com eles, como nome, endereço, CPF e valor da mercadoria.

No entanto, ela notou que não estava claro para os clientes por que esses dados estavam sendo compartilhados. Mariana decidiu abordar esse problema e implementou um processo transparente de comunicação com os clientes, explicando a necessidade dessas informações para garantir uma entrega eficiente.

2. Risco de Processamento:

Outro risco que Mariana identificou era o processamento de dados para enviar e-mails de promoções com base nos itens comprados pelos clientes. No entanto, ela percebeu que isso também não estava claro para os titulares dos dados.

Para resolver essa questão, Mariana tornou sua política de privacidade mais acessível e fácil de entender, explicando como os dados dos clientes seriam utilizados para melhorar a experiência de compra e fornecer ofertas personalizadas.

Com determinação e responsabilidade, Mariana não apenas se tornou uma empresária de sucesso, mas também uma defensora da privacidade de seus clientes. Ela aprendeu que a proteção dos dados pessoais não era apenas uma obrigação legal, mas também uma maneira de construir confiança e fortalecer seus relacionamentos comerciais.

24. Passo 5 - Analisar os riscos

A análise de riscos consiste em uma avaliação minuciosa das incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, bem como dos controles existentes e sua eficácia. O objetivo principal da análise de riscos é obter uma compreensão aprofundada da natureza dos riscos, incluindo a determinação do nível de risco, quando apropriado.

A condução da análise de riscos pode variar em termos de detalhamento e complexidade, dependendo dos objetivos da análise, da disponibilidade e confiabilidade dos dados e dos recursos disponíveis. As técnicas utilizadas para essa análise podem ser qualitativas, quantitativas ou uma combinação de ambas, conforme apropriado às circunstâncias e ao propósito da análise.

A análise de riscos desempenha um papel fundamental ao fornecer informações essenciais para a avaliação dos riscos, ajudando a tomar decisões sobre se um risco precisa ser tratado, e, em caso afirmativo, como deve ser abordado, afinal, se um risco é baixo, pode ser que a empresa opte por não trabalhá-lo naquele momento. Ela também orienta a definição da estratégia e dos métodos mais adequados para o tratamento dos riscos.

Os resultados da análise oferecem uma visão crítica que se torna valiosa em situações decisórias, quando diferentes opções envolvem diversos tipos e níveis de risco.

Ao conduzir uma análise de riscos, é fundamental considerar os seguintes fatores:

- A probabilidade dos eventos e suas consequências;
- A natureza e magnitude das consequências potenciais;
- A complexidade e interconexões entre os riscos;
- Aspectos temporais e a volatilidade dos eventos;

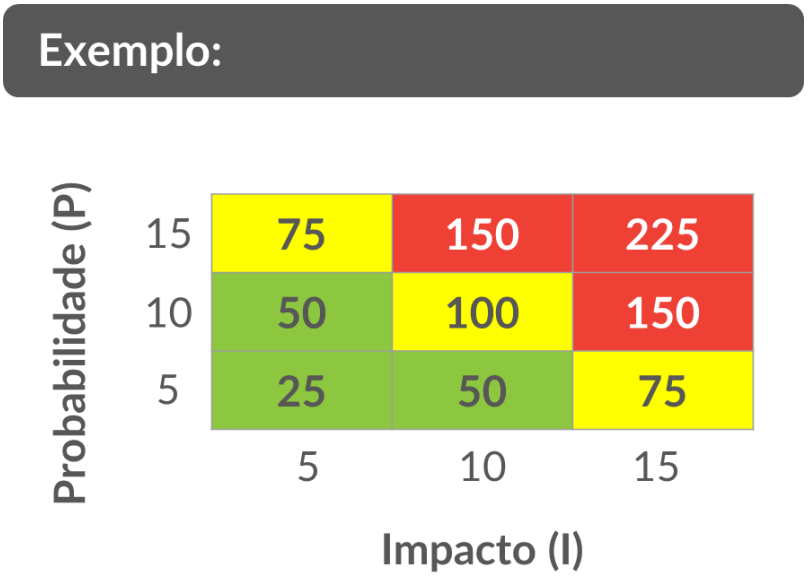
- A avaliação da eficácia dos controles já existentes;
- A sensibilidade dos resultados e os níveis de confiança associados às análises realizadas.

Existem uma série de formas de verificação e análise de riscos. Uma maneira de avaliar é utilizar a matriz de Probabilidade x Impacto, sendo dividida em duas colunas:

- Probabilidade: chance de algo acontecer, em termos gerais ou matemáticos;
- Impacto: como o resultado de um evento afeta os objetivos.

Assim, é possível avaliar se a probabilidade de acontecer algo é baixa, moderada ou alta, assim como o impacto (e classificar de 5 a 15). Em seguida, ao multiplicar o valores (P x I), é possível entender quais riscos devem ser tratados, até mesmo pelas cores da matriz, conforme a figura abaixo. Vale ressaltar que é a combinação dos dois fatores que garantem a análise de riscos, não apenas a probabilidade ou o impacto:

Figura 11 - Matriz de Probabilidade x Impacto



Também trazemos uma tabela de riscos, não exaustiva, ou seja, que não inclui todos os existentes, para ilustrar e ajudar a conscientizar de alguns deles:

Figura 12 - Tabela com lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais - Fonte: Guia de Boas Práticas Lei Geral De Proteção De Dados (LGPD), 2020.

Risco Referente ao Tratamento de Dados Pessoais	**P**	**I**	**Nível de Risco (P X I)**
Acesso não autorizado.	10	15	150
Modificação não autorizada	10	15	150
Perda	5	15	75
Remoção não autorizada.	5	15	75
Coleção excessiva	10	10	100
Informação insuficiente sobre a finalidade do tratamento.	10	15	150
Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
Compartilhar ou distribuir dados pessoais com	10	15	150

terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.			
Retenção prolongada de dados pessoais sem necessidade.	10	5	50
Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dados pessoais com informação equivocada, ausência de validação dos dados de entrada, etc.)	5	15	75
Reidentificação de dados pseudonimizados.	5	15	75

Para trazer um exemplo, será feita uma análise de risco em acesso indevido a dados pessoais, sendo o caso de empresa que terceiriza o sistema de vale-presentes:

- **Riscos identificados**
    - Acesso indevido a dados pessoais;
        - Exposição dos dados aos funcionários da empresa terceira;
    - Ransomware;
        - Exposição externa a hackers;
    - Tratamento sem consentimento do titular dos dados pessoais;
        - Não há consentimento específico da empresa terceira, apenas da loja;
    - Retenção prolongada de dados pessoais;
        - Não ter definido o tempo de descarte.

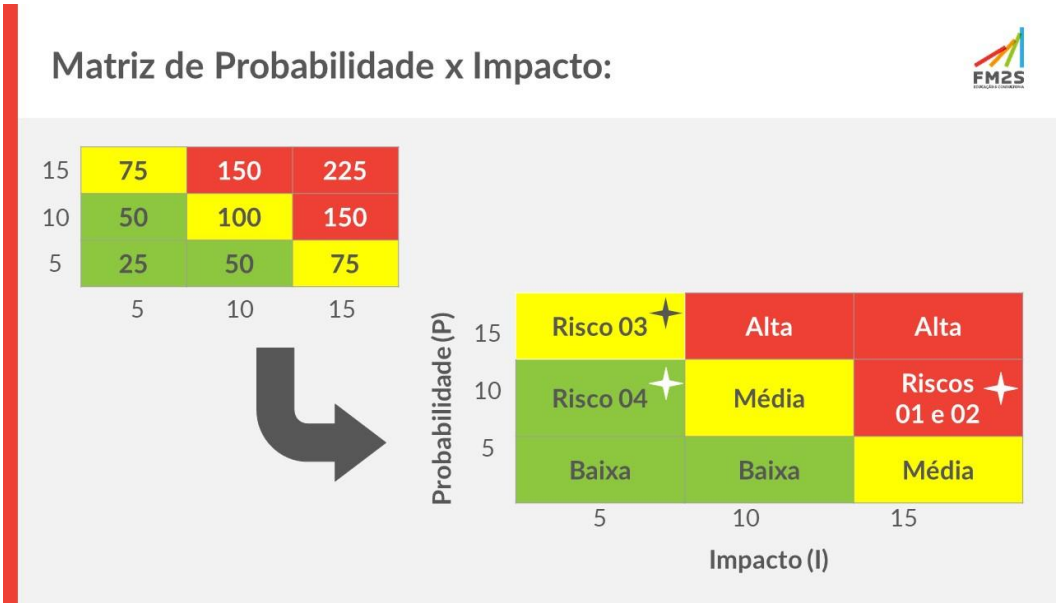
Para fazer a análise dos riscos, utilizou-se a Matriz de Probabilidade x Impacto, conforme visto a seguir:

Figura 13 - Análise de Riscos de uma empresa que terceiriza o sistema de vale-presentes

ID	**Risco Referente ao Tratamento de Dados Pessoais**	**P**	**I**	**Nível de Risco (P X I)**
01	Acesso indevido a dados pessoais	10	15	150
02	Ransomware	10	15	150
03	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	5	15	75
04	Retenção prolongada de dados pessoais	10	5	50

É importante pensar nas duas colunas ao fazer a análise, uma vez que, mesmo que a probabilidade seja pequena, como no caso de vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular, que pode ser que o cliente preencha as suas informações, mas, caso aconteça, o impacto é grande, uma vez que o cliente não receberá seu vale.

Figura 14 - Matriz de Probabilidade x Impacto de uma empresa que terceiriza o sistema de vale-presentes



25. Passo 6 - Tratar os riscos

No decorrer das etapas da Gestão de Riscos, depois de percorrer pela identificação, classificação, análise e avaliação dos problemas, é hora de tratá-los, ou seja, selecionar e implementar ações para abordá-los. Esse processo acontece com a formulação e seleção de opções para o tratamento do risco, seguido do planejamento e implementação. Então, é preciso avaliar sua eficácia e, se houver risco remanescente, verificar se é aceitável. Se não for, haverá necessidade de tratamento adicional.

Os Planos de Tratamento servem para especificar como as opções escolhidas serão implementadas. Eles devem ser integrados aos processos da gestão da organização, sempre consultando as partes interessadas apropriadas, e devem conter a justificativa para a seleção que foi feita, além de informações como:

- Os responsáveis por aprovar e implementar este plano;
- Ações propostas;
- Recursos requeridos;
- Medidas de desempenho;
- Possíveis restrições;

- Relatos e monitoramentos;
- Registros de ações tomadas e concluídas.

A tabela a seguir elenca resumidamente as hipóteses de tratamento autorizadas pela LGPD, informando, em cada caso, a base legal referente ao tratamento de dados pessoais em geral (Art. 7º), bem como a correspondente base legal para o tratamento de dados pessoais sensíveis (Art. 11).

Figura 15 - Hipóteses de Tratamento

Hipótese de Tratamento	**Dispositivo Legal para o Tratamento de Dados Pessoais**	**Dispositivo Legal para o Tratamento de Dados Pessoais Sensíveis**
Hipótese 1: Mediante consentimento do titular	LGPD, art. 7º, I	LGPD, art. 11, I
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, II	LGPD, art. 11, II, “a”
Hipótese 3: Para a execução de políticas públicas	LGPD, art. 7º, inciso III	LGPD, art. 11, II, “b”

Hipótese 4: Para a realização de estudos e pesquisas	LGPD, art. 7º, inciso IV	LGPD, art. 11, II, “c”
Hipótese 5: Para a execução ou preparação de contrato	LGPD, art. 7º, inciso V	Não se aplica
Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, art. 7º, inciso VI	LGPD, art. 11, II, “d”
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular ou de terceiro	LGPD, art. 7º, inciso VII	LGPD, art. 11, II, “e”
Hipótese 8: Para a tutela da saúde do titular	LGPD, art. 7º, inciso VIII	LGPD, art. 11, II, “f”
Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, inciso IX	Não se aplica
Hipótese 10: Para proteção do crédito	LGPD, art. 7º, inciso X	Não se aplica
Hipótese 11: Para a garantia Da prevenção à fraude e à segurança do titular	Não se aplica	LGPD, art. 11, II, “g”

A LGPD estabelece também, em seu art. 6º, que o tratamento de dados pessoais deve observar a boa-fé, ou seja, agir sempre pensando em estar em conformidade com a lei e boas práticas e dez princípios fundamentais específicos. São eles:

- Finalidade;
- Adequação;
- Necessidade;
- Livre acesso;
- Qualidade dos dados;
- Transparência;
- Segurança;
- Prevenção;
- Não discriminação;
- Responsabilização e prestação de contas.

Não basta, portanto, o enquadramento em uma das hipóteses legais autorizativas para se iniciar o tratamento de dados pessoais. É fundamental garantir que os princípios listados acima sejam respeitados. O que será feito para tratar os riscos depende do processo de tratamento em si, mas algumas medidas comuns são:

- Obtenção de consentimento:
    - O consentimento tem que ter uma finalidade clara e ele pode ser revogado;
    - Se a finalidade for alterada, o titular deve conceder o consentimento novamente;
    - Consentimento não pode ser genérico;
- Medidas de segurança e proteção de dados:
    - Tornar anônimo ou pseudônimo;

    - Deixar de ser identificável;
- Notificações obrigatórias;
- Penalidades administrativas;
- Responsabilidade civil;
- Relatório de Impacto de Proteção de Dados (RIPD).

Com intuito de exemplificar esse passo, temos o exemplo de uma empresa do ramo hoteleiro, que estava em processo de implementação da LGPD. Ela identificou os seguintes riscos: retenção prolongada de dados pessoais (ou seja, nunca houve um descarte por não ter um ciclo de vida de tratamento bem estruturado) e informações insuficientes sobre tratamento de dados pessoais.

Figura 16 - Análise de riscos em um hotel

ID	**Risco Referente ao Tratamento de Dados Pessoais**	**P**	**I**	**Nível de Risco (P X I)**
01	Retenção prolongada de dados pessoais	5	15	75
02	Informações insuficientes sobre tratamento de dados pessoais	5	15	75

Portanto, ambos os riscos são considerados moderados. Pensando por exemplo no primeiro deles, a probabilidade de haver um vazamento foi considerada baixa, uma vez que o sistema para acesso desses dados tem senha e verificação de dois fatores, mas o impacto seria grande por terem dados de mais de 20 anos de empresa.

Para eles, as escolhas de tratamento foram: Exclusão dos dados antigos, para isso, eles enviaram um aviso aos titulares dos dados, avisando que a conta seria encerrada e que, caso quisesse, o titular teria que solicitar um novo acesso. Esse novo acesso também daria acesso aos clientes às novas políticas de proteção de dados da

empresa, o que resolve dois problemas. Sobre as informações insuficientes sobre tratamento de dados: reformularam a Política de Segurança de Dados e mandaram aviso aos titulares.

26. Passo 7 - Monitorar e Manter as práticas de proteção de dados

A abordagem pró-ativa da Privacidade desde a Concepção (PdC) é importante e se concentra em antecipar e prevenir eventos invasivos de privacidade antes de sua ocorrência. Em vez de esperar que os riscos de privacidade se concretizem e, em seguida, propor soluções para as violações, essa abordagem visa evitar que tais eventos ocorram. Em suma, a PdC atua de forma preventiva, antecedendo os incidentes, em vez de reagir a eles posteriormente.

Ao ser aplicada às tecnologias da informação, práticas organizacionais, projetos físicos ou ecossistemas de informação em rede, a Privacidade por Design começa com o reconhecimento explícito do valor e dos benefícios associados à incorporação de práticas de privacidade robustas desde uma fase inicial e de forma consistente.

Existe também a abordagem privacidade incorporada ao projeto, onde a privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas de negócios. Isto significa que não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade. (BRASIL, 2022, p. 51)

Por fim, ao entender ambas abordagens, chega-se ao encerramento do projeto. Para que ele ocorra, repita a avaliação de lacunas para identificar áreas remanescentes não conformes; enderece as áreas restantes não compatíveis; e por fim, realize a revisão pós-projeto.

Para ajudar, disponibilizamos no arquivo [FM2S] Template Relatório de Impacto à Proteção de Dados Pessoais (na pasta do curso), um template para que você possa realizar o Relatório de Impacto à Proteção de Dados, do governo federal.

27. Dicas e boas práticas

As boas práticas são previstas na própria LGPD:

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados 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, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação;

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

- Brasil, 2018

28. Revisão dos Conceitos e Passo a Passo

- Conceitos Essenciais:
    - Dado x Informação x Conhecimento;
    - Privacidade e Segurança da Informação;
    - Educação e Cidadania Digital;
    - Stakeholders;
    - Governança e Compliance;
    - Ouvidoria;
    - Ciclo de vida de tratamento de dados: coleta, uso, armazenamento;
    - Impacto e Avaliação de Privacidade (AIPD);
    - Autoridade Nacional da Proteção de Dados;
- Destrinchando a lei:
    - Direitos e Casos Particulares;

- Agentes no tratamento de dados;
- DPO;
- Transferências Internacionais, responsabilidades e sanções;

- Passo a passo:
  - Passo 1 - Realizar auditoria Interna;
  - Passo 2 - Criar um Comitê;
  - Passo 3 - Identificar os riscos;
  - Passo 4 - Analisar os riscos;
  - Passo 5 - Tratar os riscos;
  - Passo 6 - Monitoramento e Manutenção das práticas de proteção de dados;
  - Passo 7 - Treinar os colaboradores com campanhas de conscientização;

Parabéns!

Obrigada pela caminhada até aqui!

Que você consiga aplicar seus novos conhecimentos sobre a Lei Geral de Proteção de Dados!

29. Referências

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

ALENCAR, Ana Catarina de. Inteligência Artificial, Ética e Direito: Guia Prático para Entender o Novo Mundo.Editora Saraiva, 2022.

Consumidor.gov.br. Boletim 2022. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/dia-do-consumidor-senacon-lanca-boletins-com-os-dados-de-reclamacoes-recebidas-em-2022/15-03-2023-boletim_consumidor-gov-br_2022_v6.pdf.

CAMÊLO, M. N. e ALVES, C. G-Priv: Um Guia para Apoiar a Especificação de Requisitos de Privacidade em Conformidade com a LGPD. 2022. Disponível em: https://sol.sbc.org.br/journals/index.php/isys/article/download/2743/2200/13837.

FONTES, Edison Luiz G. Segurança da informação - 1ª edição. Editora Saraiva, 2012.

BARRETO, Jeanine S.; ZANIN, Aline; MORAIS, Izabelly S.; et al. Fundamentos de segurança da informação. Grupo A, 2018.

DONDA, Daniel. Guia prático de implementação da LGPD. 1. ed. São Paulo: Labrador, 2020.

Comitê Central de Governança de Dados. GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf.

GOLDSCHMIDT, Andrea; ROCHA, Thelma V.; CARDOSO, Roberta de C.; et al. Gestão dos Stakeholders - Como Gerenciar o Relacionamento e a Comunicação Entre a Empresa e seus públicos de interesse. Editora Saraiva, 2010.

FERREIRA, H. A. SISTEMA DE ORGANIZAÇÃO DO CONHECIMENTO PARA APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): desenvolvimento de taxonomias para instituições hospitalares. Universidade Federal de Santa Catarina, 2023. Disponível em: https://repositorio.ufsc.br/handle/123456789/247565.

Autoridade Nacional de Proteção de Dados. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf.

RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper.

OLIVEIRA, D. L. AGENTES DE TRATAMENTO DE DADOS PESSOAIS E ENCARREGADO: GUIA PRÁTICO SOBRE SUAS ATRIBUIÇÕES, RESPONSABILIDADES E BOAS PRÁTICAS. Fundação Getulio Vargas. 2021.

Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/31490/TrabalhoDenisLimadeOliveira_2022_final_v1.pdf?sequence=6&isAllowed=y.

MATTOS, João G. Auditoria. Grupo A, 2017.

MARINHO, Fernando. Os 10 Mandamentos da LGPD - Como Implementar a Lei Geral de Proteção de Dados em 14 Passos. Grupo GEN, 2020.