PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA
GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO


# Recomendações de Boas Práticas para Implementação da LGPD em Processos de Desenvolvimento de Software

GRASIELLE COSTA SANTOS

GOIÂNIA

2022

GRASIELLE COSTA SANTOS

# Recomendações de Boas Práticas para Implementação da LGPD em Processos de Desenvolvimento de Software

Trabalho de Conclusão de Curso II apresentado à Escola de politécnica, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação.

Orientador: Prof. Ma. Adriana Silveira de Souza

GOIÂNIA

2022

GRASIELLE COSTA SANTOS

# Recomendações de Boas Práticas para Implementação da LGPD em Processos de Desenvolvimento de Software

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Engenharia de Computação, em_____/_____/____.

_____
Prof. Me.

Banca examinadora:

_____
Orientador: Prof. Ma. Adriana Silveira de Souza

_____
Prof. Dr Juliano Lopes de Oliveira

_____
Prof. Esp Leodércio Lima Filho

GOIÂNIA

2022

“Saaaaaaaaaaaaaaaaaaaaasuke.”

Naruto Uzumaki, Naruto

## AGRADECIMENTOS

Agradeço primeiramente a Deus por me conceder a chance de concluir esse curso e por colocar pessoas ao meu redor que me apoiaram durante essa longa jornada.

A meus pais, que concordaram com a ideia de me deixar morar em outro estado para fazer faculdade, e sempre torceram por mim, apesar de até hoje não saberem direito o que eu estudei. Agradeço especialmente a minha mãe que sempre amou aprender e que incentivou minha busca por conhecimento, ela sempre acreditou que eu conseguiria conquistar meus sonhos.

A meus amigos antigos, que me deram suporte emocional durante essa jornada e que ainda esperam ser sustentados por mim. Principalmente minha amiga Daianne Souza que ajudou muito e de todas as formas possíveis durante esses anos, inclusive com esse trabalho.

A meus novos amigos e companheiros de profissão, que me acolheram e auxiliaram durante o curso. Especialmente a minha amiga Amanda Cândido que sempre esteve ao meu lado durante os projetos, aprovações e as reprovações. Também esteve comigo desde o começo desse trabalho, me ajudando com correções e me motivando.

A meus professores e orientadora, que me inspiraram a seguir a área de tecnologia, e me corrigiram para que eu pudesse melhorar.

E finalmente, mas não menos importante, a mim mesma por não desistir no meio do caminho.

## RESUMO

A presente monografia pretende analisar os requisitos da LGPD (Lei Geral de Proteção de Dados) e identificar seu impacto no processo de desenvolvimento de software. Com base nessa análise formular um conjunto de recomendações para que empresas de desenvolvimento de software utilizem para adequarem o seu ciclo de desenvolvimento à LGPD. Para isso, foi estudado os artigos da LGPD, principalmente no que tange as recomendações dadas pelos princípios do *Privacy by design*.



**Palavras-chave**: Dados pessoais. Lei Geral de Proteção de Dados. Desenvolvimento de software.

## LISTA DE SIGLAS

| | |
|---|---|
| LGPD | Lei Geral de Proteção de Dados |
| GDPR | *General Data Protection Regulation* |
| SI | Segurança da Informação |
| DP | Dados Pessoais |
| PbD | *Privacy by Design* |
| SDLC | *Software Development Life Cycle* |
| ANPD | Autoridade Nacional de Proteção de Dados Pessoais |
| RIPD | Relatório de Impacto de Proteção de Dados |
| FIPs | *Fair Information Practices* |

## SUMÁRIO

# 1 INTRODUÇÃO

Os rastros digitais deixados para trás a cada dia revelam mais sobre uma pessoa do que ela imagina e isso pode se tornar um problema de privacidade, ou ser a base de um mundo mais próspero (PENTLAND, 2013). Esses dados gerados, podem ser transformados em informações valiosas para empresas e organizações utilizarem como ativo. Dessa forma, medidas protetivas para resguardar dados se tornam prioridade, pois essas medidas exigem que os negócios se reinventem para garantir adequação aos padrões de segurança impostos.

A transformação digital que vem acontecendo nas últimas décadas, gerou uma grande quantidade de dados por conta da crescente movimentação online. A cultura da sociedade *data driven* (“orientada a dados”) está cada dia mais forte, a utilização de dados pessoais é praticamente obrigatória na maioria das aplicações e serviços online, e essas informações tornam possível a identificação de uma pessoa. Por conseguinte, as empresas estão acumulando uma grande base de dados, e precisam ter maior atenção com segurança e privacidade da informação. Ataques cibernéticos envolvendo violação de dados estão se tornando um problema crescente, no ano de 2009 estima-se que um ataque cibernético acontecia a cada 39 segundos, já em 2021 houve o aumento para um ataque a cada 11 segundos. Além disso, o custo desses ataques também está aumentando (HOFMANN, 2021).

O estudo anual *Cost of a Data Breach* (“Custo de uma violação de dados”) realizado pela IBM *Security* no ano de 2021 em mais de 17 países e regiões, incluindo o Brasil, aponta que o custo médio de uma violação de dados é de US$ 4,24 milhões. Um aumento de 10% em relação ao ano de 2020, o que configura uma diferença considerável de preço. Estima-se que um dos fatores para esse crescimento, seja o trabalho remoto devido a pandemia por COVID-19. O vetor de ataque mais comum foram credenciais comprometidas, abrangendo cerca de 20% das violações. Foram analisados vários fatores de custo, desde investigações técnicas e recuperação até notificações, atividades legais e regulatórias, custo de perda de negócios e reputação.

De acordo com um levantamento feito em 2021 pela empresa Britânica Surfshark, que a atua na área de privacidade e segurança online, o Brasil é o 6º país do mundo que mais sofre vazamentos de dados. Em janeiro de 2022 o Banco Central do Brasil emitiu um comunicado informando um vazamento de dados pessoais vinculados a chaves de PIX, estimando que as informações de 160.147 chaves foram expostas, dentre elas nome, CPF, número de agência e conta. Já em 2021, a Autoridade Nacional de Proteção de Dados (ANPD), solicitou que a polícia

federal investigasse o vazamento de dados como nome, fotos, renda mensal, endereço e CPF de mais de 223 milhões de Brasileiros – incluindo pessoas falecidas.

Inspirada na legislação europeia GDPR (*General Data Protection Regulation)*, em 2018 foi criada a Lei Geral de Proteção de Dados (LGPD), que objetiva regular a forma como acontece a captura e o tratamento de dados pessoais, proporcionando uma maior autonomia e propriedade dos dados aos seus titulares. A lei brasileira cria uma regulação para uso, proteção e transferência de dados no Brasil, em organizações públicas ou privadas. Ela estabelece quem são os envolvidos no processo de tratamento de dados, assim como seus direitos e deveres, incluindo penalidades para o caso de descumprimento (MORAIS, 2021).

Por conseguinte, a legislação orienta que os responsáveis pelo tratamento de dados utilizem de medidas de segurança assim como boas práticas e governança para evitar vazamentos e uso indevido de dados. De acordo com o estudo Cost *of a Data Breach* (2021), o uso de boas práticas de proteção de dados é um dos fatores que faz uma diferença tangível no valor de violação de dados, tal custo depende principalmente da eficiência com que a empresa responde a essa ocorrência – quanto mais rápido as medidas forem tomadas, menos oneroso será o gerenciamento.

Em decorrência a isso, muitos negócios estão na jornada para alcançar conformidade com a lei, sendo a área de TI uma das mais afetadas pela vigência do regulamento, pois é a responsável pelo gerenciamento de dados. Dessa forma, empresas nesse setor tiveram impacto direto das novas normas, é o caso das empresas de desenvolvimento de *software*. Em consequência, medidas mais rígidas de segurança e privacidade de dados precisam ser adotadas nessas organizações, em especial nas empresas que desenvolvem e mantém sistemas de *software*.

Nesse cenário, o modelo privacidade por design *(privacy by design* - PbD) adotado como padrão internacional em 2010 por vários países, tornou-se indispensável pois tem como base a privacidade desde a concepção de um produto, mantendo a preocupação com a segurança presente em todas as fases do ciclo de vida de desenvolvimento de um sistema. O PbD ganhou destaque com o surgimento da GDPR e é construído por princípios que ajudam a prevenir incidentes de privacidade, através de especificação de design, práticas de negócios e infraestrutura física (OMORONYIA, ETUK, INGLIS, 2019).

Diante do exposto, o presente trabalho preocupa-se em responder o seguinte quationamento: Quais recomendações embasadas na LGPD são indicadas ao utilizar a abordagem *privacy by desing* em empresas de desenvolvimento de software?

Esse trabalho tem o objetivo de definir um conjunto de recomendações que apoie o *privacy by design* na implementação da LGPD nas empresas de desenvolvimento de software.

**Como Objetivos Específicos encontram-se:**

- Classificar as principais etapas do processo de criação de software.
- Verificar a conformidade do *privacy by design* para com a LGPD.
- Descrever quais as principais recomendações da LGPD sobre proteção e privacidade de dados.

Este trabalho está dividido em quatro partes. O capítulo 2 aborda sobre a LGPD e aponta suas principais características e recomendações sobre privacidade e segurança de dados. O capítulo 3 discute o processo de desenvolvimento de software e o seu ciclo de vida. O capítulo 4 aborda o privacy *by design* e seus princípios, além de instruções de como implementá-lo. O capítulo 5 descreve recomendações que podem ser aplicadas ao *privacy by design* dentro de cada fase do ciclo de vida de um software. E por fim, as considerações finais e trabalhos futuros são apresentados no capítulo 6.

## 2 LEI GERAL DE PROTEÇÃO DE DADOS

A Lei nº 13.709 referente a Lei Geral de Proteção de Dados (LGPD), foi criada em 14 de agosto de 2018 e entrou em vigor em agosto de 2020 no Brasil, baseada no Regulamento Geral de Proteção de Dados na Europa (*General Data Protection Regulation* - GDPR). A LGPD atua sobre o tratamento de dados pessoais (DP), inclusive em meios digitais e tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade do titular de dados (BRASIL, 2018). A LGPD visa aumentar o controle do titular sobre seus dados, gerando assim confiança no processo de coleta, uso e privacidade de dados, aplicando-se a operações de tratamento de dados realizada por pessoa física ou jurídica, seja pública ou privada, sobre dados coletados e tratados no Brasil e pertencentes a cidadãos Brasileiros.

A lei define dados pessoais como aqueles que identificam a pessoa natural direta ou indiretamente. Normalmente imagina-se dados pessoais somente como as informações requeridas em formulários de identificação, porém dados pessoais são muito mais abrangentes, a LGPD divide esses dados em três tipos; o primeiro tipo são os dados pessoais convencionais, que são os mais conhecidos, como o nome, CPF, telefone, entre outros; em seguida existem os dados pessoais sensíveis; e por último têm-se os dados pessoais anonimizados.

Dados pessoais sensíveis podem ser dados biométricos vinculados a uma pessoa como impressão digital, senhas e informações sigilosas, ou dados que podem causar discriminação contra essa pessoa, como origem, religião, prontuário médico, orientação sexual ou até mesmo a opinião política (BRASIL, 2018). Os dados sensíveis exercem grande impacto na vida de uma pessoa, caso sejam violados podem causar prejuízos monetários e danos morais, entre outras perdas.

Por outro lado, os dados anonimizado são definidos como aqueles que passaram por um processo de desvinculação da pessoa natural a quem pertencem, omitindo dessa forma seu titular. Esse tipo de dado é muito utilizado em pesquisas acadêmicas e empresariais, onde os resultados não se alteram pela anonimização. Existem ainda alguns dados podem ser usados para identificar uma pessoa de forma indireta, como localização GPS, retrato em fotografia, hábitos de consumo e endereço de IP, que não são fornecidos de forma consciente, mas são obtidos automaticamente, logo não é perceptível para todos que estes também se enquadrem na lei.

Outro aspecto importante da LGPD é quem ela respalda: o titular de dados, o controlador de dados, o operador de dados, o encarregado dos dados (*Data Protection Officer* - DPO) e o

órgão regulador. O titular é a quem se referem os dados, o dono deles, sendo garantido o direito de:

- Confirmação da existência do tratamento de dados.
- Acesso a todos os dados que estão sendo tratados e os procedimentos realizados com esses dados.
- Correção de dados incompletos ou desatualizados.
- Bloqueio e eliminação de dados considerados desnecessários, ou tratados em desconformidade com a lei.
- Revogação do consentimento para o tratamento de dados.
- Notificação de vazamentos e incidentes envolvendo seus dados.

Essas solicitações devem ser realizadas de forma gratuita e facilitada, sendo cumpridas dentro do prazo estabelecido nos termos de uso do serviço contratado. Esses direitos dão ao titular mais segurança, liberdade e privacidade sobre suas informações, pois o permitem mais autonomia sobre o processo de tratamento de dados (SANTOS; SILVA, 2020).

A lei estabelece a responsabilidade sobre os dados que estão sendo tratados a empresa ou órgão que está em posse dele. É chamada de controlador, a quem foi garantido a permissão de forma expressa pelo titular para o uso de seus dados durante o período e para finalidades estabelecidas. O controlador toma as decisões referentes ao tratamento de dados, como definir regras sobre o tratamento que serão seguidas pelo operador. Tendo ainda o dever de realizar a gestão das informações envolvam dados pessoais relacionados aos clientes, consumidores e colaboradores.

Assim, chama-se agentes de tratamento o controlado e operador, eles devem manter registro sobre todas as operações realizadas com os dados do titular. Processos como armazenamento, coleta, e segurança de compartilhamento de dados devem estar devidamente documentados e resguardados pela política de segurança da empresa. Dessa forma, a LGPD busca impor mais transparência, comunicação e conformidade no relacionamento entre o titular de dados e os agentes de tratamento (SANTOS; SILVA, 2020).

O encarregado pela proteção de dados em se chama DPO, ele é responsável por assegurar que as empresas entejam em conformidade com a legislação, aceita reclamação dos titulares, presta esclarecimento e atende a solicitações da Autoridade Nacional de Proteção de Dados Pessoais (ANPD). O DPO é indicado pelo controlador para atuar como um meio de comunicação entre ele, os titulares de dados e o órgão regulador. (PEREIRA, 2021)

A fiscalização e a regulação da LGPD são responsabilidade da ANPD, que é o órgão regulador. A lei estabelece exigências e determina penalidades para maior segurança no âmbito jurídico, prevendo uma multa de 2% do faturamento até no máximo 50 milhões de reais por infração. As sanções e penalidades buscam incentivar as empresas a melhorar suas políticas e processos direcionados a privacidade e proteção dos dados (SANTOS; SILVA, 2020).

Dessa maneira, o investimento em segurança da informação é indispensável para evitar que eventos relacionados a violação da segurança de dados pessoais aconteçam. Caso ocorra um incidente de DP tais como acesso não autorizado, acidental ou ilícito, que resulte na destruição, perda, alteração ou vazamento de dados, é necessário comunicar ao titular dos dados e a ANPD.

Cada incidente de segurança pode gerar um prejuízo monetário em pequena ou grande escala. Nesse sentido, a longo prazo a adequação a LGPD pode ser mais econômica para o controlador, pois ela contará com uma adequação padronizada de normas e práticas que promovem a proteção de todos os cidadãos que estejam em território nacional (STEFANINI, 2019). Além das perdas monetárias os incidentes de segurança também afetam a credibilidade da empresa, fazendo o público perder a confiança na organização. Portanto, entrar em adequação com a LGPD garante uma vantagem de credibilidade governamental em relação as empresas que não estão em conformidade com a lei.

**Segurança da informação**

A segurança da informação é uma área que sofreu grande impacto com a vigência da LGPD, uma vez que é responsável pela proteção aos dados. Ela visa garantir a confidencialidade da informação, permitindo somente acesso de pessoal autorizado. Também como a integridade e disponibilidade dos dados, para que não haja alteração e obstrução de acesso.

A lei determina que medidas devem ser tomadas para garantir a proteção de dados pessoais. Esses dados dever ser protegidos de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018). Se faz necessário então implementar diretrizes que orientem como entender e tratar a segurança da informação dentro das organizações (SANTOS; SILVA, 2020).

O investimento em segurança é essencial para que exista privacidade de dados, o ideal é que segurança e privacidade andem juntas. As melhorias necessárias para que a SI suporte a

adequação a lei ficam a cabo das empresas e organizações, elas devem fazer o mapeamento das mudanças necessárias de acordo com seu estado atua. Essas mudanças podem ocorrer também por meio de controles integrados de acesso para segurança física do local em que serão tratados os dados, criptografia dos dados para a proteção dos ativos, revisão e adequação da arquitetura de sistemas da empresa, assim como a separação de bancos de dados e demais ações preventivas (TENBU, 2021).

A segurança do dado a ser tratado é de responsabilidade de cada pessoa que tiver contato com ele. Cabe aos agentes de tratamento utilizarem dos meios e salvaguardas que sua organização disponibiliza para manter esse dado confidencial e seguro. Segundo o previsto pelo caput do art. 46º da LGPD, a proteção dos dados pessoais é alcançada por meio de medidas de segurança, técnicas e administrativas (GUIA DE BOAS PRÁTICAS LGPD, 2020).

> "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito (Brasil, 2018).

Além disso, o Art. 46, § 2º menciona que as medidas de segurança e sigilo de dados devem ser adotadas desde a da concepção do produto ou serviço ao invés de serem adicionadas na fase final do produto. Dessa forma surge a necessidade de integração entre as medidas de segurança e privacidade de dados.

Criar uma cultura de privacidade e conscientização para a proteção de dados é a chave para implementar um sistema de SI em conformidade com a lei. Pode-se utilizar conceitos como o de *privacy by design* (privacidade desde a concepção, em português - PbD), considerado uma boa prática nas operações de tratamento de dados pessoais, esse método traz a privacidade e proteção como foco. Sendo elas implementadas como um padrão de uso, e não opção a ser escolhida.

**Boas Práticas de Governança**

As boas práticas de governança de dados são ferramentas base que visam gerenciar, utilizar e proteger os dados, elas auxiliar as organizações a cumprir regulamentos de conformidade com a lei. As boas práticas referem-se ao conjunto das melhores técnicas para se realizar uma tarefa, já a governança no contexto de dados e tecnologia da informação é um conjunto de diretrizes, habilidades, competências e responsabilidades assumidas pela alta direção da empresa e pelos agentes de tratamento para guiar as ações organizacionais, de modo

a controlar processos, otimizar a aplicação de recursos, dar suporte para a tomada de decisões e garantir a segurança das informações (FLOWTI, 2021).

A governança de dados utiliza os dados como ativos e os mantem sobre controle e organizados, facilitando assim a utilização desses dados e a garantia de privacidade para eles. Dessa forma, ela facilita a proteção contra incidentes de dados, pode também reduzir os custos de gerenciamento de dados e tornar o gerenciamento um papel de toda a organização. Segundo o previsto pelo do art. 50º da LGPD, os agentes de tratamento podem definir regras de boas práticas e governança para o tratamento de dados.

> "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 (Brasil, 2018).

Dessa forma, as boas práticas e governança são estabelecidas de acordo com os tipos de dados que serão processados, bem como o segmento do serviço ou produto oferecidos, levando em consideração a condição da organização, sua forma de funcionamento, as normas de segurança necessárias. Uma empresa de desenvolvimento de software tem que levar em conta ao desenvolver suas boas práticas e governança quais tipos de dados seus softwares vão utilizar, o local em que ficarão armazenados e como será feito o tratamento. Assim como, a finalidade dos dados, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento desses dados.

Assim, reuniu-se alguns exemplos de boas práticas em governança de dados provenientes da LGPD sendo elas:

- Fazer o mapeamento de dados: Conhecer os tipos de dados, quantidade e complexidade das operações realizadas com ele fazem do mapeamento de dados uma etapa indispensável para o processo de adequação a LGPD. Também, identificar o ciclo de vida dos dados e por onde essas informações passam, geram uma visualização da situação geral de tratamento, permitindo criar um plano de governança e adequação a lei. Sem esse mapeamento não tem como identificar os riscos que a empresa ou organização está exposta, nem criar um plano de mitigação de risco, afinal só é possível proteger o que se conhece (GET PRIVACY, 2021).

- Manter registros das operações de tratamento: O registro de operações de tratamento de DP é essencial para a política de transparência e segurança. Ele deve conter as operações de acordo com sua base legal e finalidade. Dessa forma se houver uma solicitação do titular para um relatório de atividade, ou a necessidade de fiscalização pelo órgão regulador, o registro provará que o tratamento de dados é feito de forma legal.
- Anonimizar dados quando possível: A anonimização de dados é uma técnica considerada boa prática quando puder ser aplicada, realizada em casos específicos no qual o titular não precise ser identificar, ela feita pelo operador de dados. A lei afirma que o processo de anonimização tem que ser irreversível, ou seja, uma vez anonimizados os dados não podem voltar a identificar seus titulares (GET PRIVACY, 2021).
- Criar protocolos de resposta a incidentes: Mesmo com todas as medidas de segurança e recomendações citadas acima, um incidente de dados pode ocorrer. Portanto, devem existir protocolos criados para responder rapidamente esses incidentes, diminuindo os danos sofridos. Os protocolos de segurança são ações que os agentes de tratamento devem tomar quando uma falha de segurança ocorre.
- Elaborar o relatório de impacto à proteção de dados pessoais: Um relatório de impacto de impacto à proteção de dados pessoais (RIPD) é uma recomendação a LGPD. Sendo um documento que conta com a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, assim como as medidas de mitigação para esses riscos (BRASIL, 2018).

A criação do programa de governança se dá com base no Relatório de Impacto de Proteção de Dados (RIPD previamente levantado e avaliado pela empresa. Dessa forma, deve-se incluir respostas a incidentes e remediações, sendo necessária a atualização do sistema de gestão constantemente para melhor desempenho da empresa (BRASIL, 2018). A Governança de dados é o foco central para as demais funções de dados, sendo preciso uma grande atenção a esse sistema. A criação de uma cultura de segurança é primordial para essa nova fase de adequação (SANTOS; SILVA, 2020).

Para implementar um sistema de governança em privacidade com base na lei é necessário ter o comprometimento dos agentes de tratamento e da alta gestão, para cumprir as políticas de segurança e boas práticas formuladas. O sistema de governança deve priorizar a

confiança do titular, sendo transparente e apresentando agilidade resolutiva aos incidentes, além de estar sempre atualizado e aprovado pela ANPD (BRASIL, 2018).

# 3 PROCESSO DE DESENVOLVIMENTO DE SOFTWARE

De acordo com Sommerville (2011), processo, para a engenharia de software, é um conjunto de atividades e resultados associados que geram um produto de software. O objetivo de um processo é construir um software com mais qualidade (deve atender aos requisitos estabelecidos), previsibilidade (se comportar de forma esperada) e economia (poupar recursos materiais).

Um software é um programa virtual criado por códigos de instruções e sua documentação associada, seus sistemas são abstratos e intangíveis (SOMMERVILLE, 2011). Eles são usados para realizar ações em sistemas computacionais físicos, chamados de hardware, como computadores, celulares, impressoras, entre outros. O profissional responsável por projetar e criar esses sistemas é chamado de engenheiro de software, para isso ele utiliza os princípios da engenharia de software, que é um ramo da ciência da computação, sobre design, desenvolvimento, testes e manutenção de aplicativos de software (COURSERA, 2022).

O ciclo de vida de desenvolvimento de software (*Software Development Life Cycle* - SDLC) é um processo de construção ou manutenção de sistemas de software, ele descreve as fases necessárias no desenvolvimento (BENG *et al*, 2012). Ele considera modelos e metodologias que formam a estrutura para planejar e controlar o processo de desenvolvimento. Como a metodologia tradicional que consiste em modelos do tipo cascata, espiral, entre outros. E a metodologia ágil, que considera modelos como o SCRUM. A identificação do SDLC desejado leva em consideração a complexidade, tipo e tanho do projeto e da equipe, estratégias de negócio, capacidade de engenharia e outros (BENG *et al*, 2012). Formado por um fluxo estruturado, a construção de um software envolve a fase de planejamento que é realizada antes do desenvolvimento do software. As fases de análise de requisitos, design, implantação e teste, que são realizadas durante o desenvolvimento. E as fases de implantação e manutenção que são realizadas depois que o software está pronto.

## 3.1 Planejamento

A etapa de planejamento deve conter os termos do projeto, isso inclui custos, as metas e feedback das partes interessadas, é preciso definir o escopo do projeto e o propósito do programa (JEVTIC, 2019).

### 3.2 Análise de Requisitos

Na etapa de análise de requisitos são definidos os objetivos e funções de um software, assim como as restrições. Isso acontece através se levantamento de requisitos, classificação de requisitos em funcionais (estão relacionados com as funcionalidades do software, como possibilidade de exclusão e inclusão de informações) e não funcionais (são aspectos gerais do software como acessibilidade, segurança) do software assim como os recursos necessários e os riscos associados ao software. Essa fase gera uma documentação de requisitos que será utilizada nas próximas etapas (MONITORA, 2020).

### 3.2 Design

Depois que os requisitos são definidos eles serão incluídos no design do software, o design define a arquitetura do software, como os componentes de hardware, software, estrutura (como a capacidade de rede) e processamento, também a linguagem utilizada para a codificação, as plataformas em que o software será executado, comunicação de ativos e procedimentos de segurança da informação que serão utilizados **(**JEVTIC, 2019). Essa fase também deve determinar como o usuário irá interagir com o software, um design é considerado bom, se ele leva a um software correto (faz o que deve), robusto (tolerante ao uso indevido), flexível (adaptável a mudanças), reutilizável, eficiente, confiável e utilizável. (OMORONYIA; ETUK; INGLIS, 2019). Essa fase gera um protótipo de como o software deve se comportar e ser implementado.

### 3.3 Implementação

O desenvolvimento é a fase em que a codificação acontece, levando em conta o design do produto, o programa é escrito. Em consequência, encontrar erros no código e corrigir falhas é inevitável e fundamental para a construção de um software. É recomendado que os programadores comentem o código para que a manutenção futura seja facilitada com essas instruções **(**JEVTIC, 2019). Essa fase gera o software criado.

### 3.4 Teste

A validação e verificação do software é realizada através de testes, que são feitos por profissionais e muitas vezes por usuários selecionados. Assim é possível saber se o programa

atende as especificações definidas, como funcionalidades, desempenho, segurança, usabilidade e outros. Os erros encontrados são relatados, rastreados, corrigidos.

### 3.5 Implantação

Uma vez que o software saí da fase de testes ele está pronto para ser implantado, assim o produto é disponibilizado para o usuário final. Algumas vezes o software é lançado em etapas, isso varia de acordo com a intenção do produto. Nessa etapa é importante ter uma equipe de suporte pronta para atender e ajudar os usuários caso seja preciso.

### 3.6 Manutenção

Com base no feedback dos usuários e na necessidade de mercado, o software passa por manutenções para corrigir erros ou atualizar novas funcionalidades para uma nova versão. Todas essas fases têm que ser documentadas corretamente para que haja um melhor controle sobre o processo.

O ciclo de vida de software se implementado de maneira correta, aceita um alto nível de controle de gerenciamento e documentação, pois com a documentação de cada fase fica mais fácil construir, gerenciar e utilizar esse software. A equipe do projeto de software fica ciente dos custos e recursos necessários para o desenvolvimento, assim como os potenciais riscos e formas de mitigação que esse software possa ter.

Saber como foi feito e para que foi feita cada aplicação durante o SDLC facilita também o cumprimento de requisitos estabelecidos pelo cliente do software, garantindo assim que esse produto seja entregue conforme foi solicitado, ou melhor.

# 4 PRIVACY BY DESIGN

A segurança no desenvolvimento de software tem influência tanto na sua disponibilidade quanto na sua qualidade (ZANARDO, 2019). Um software que considera segurança da informação uma prioridade tem menos chances de ter seu sistema inativo indevidamente, além de alcançar um grande nível de satisfação e confiança de seus usuários, provando que a preocupação com a segurança da informação sempre esteve presente no desenvolvimento. Mas com o advento da LGPD, surge a preocupação com sistemas que utilizam dados pessoais de alguma forma para garantir a privacidade de dados além da segurança, sendo a privacidade um direito constitucional e a segurança o grau de proteção que é aplicado aos dados.

As principais características da privacidade são o direito de ser deixado em paz e a capacidade de controlar as informações divulgadas sobre si mesmo, assim pode-se entender privacidade da informação como o direito de um sujeito de controlar ou influenciar quais informações ligadas a ele podem ser coletadas e armazenadas, e quem terá contato com essas informações (STALLINGS, 2020). O termo privacidade geralmente se refere a tornar dados pessoais indisponíveis para quem não deveria ter acesso e os interesses de privacidade de dados estão ligados à coleta, controle, proteção e uso de informações sobre indivíduos (STALLINGS, 2020).

No momento atual, em que a prevenção de incidentes de dados é uma preocupação e a vigência de leis de privacidade está em destaque, a conformidade regulatória é fundamental. As organizações estão mitigando seus riscos, o que gera apreensão para os criadores de software considerarem a privacidade já no início do projeto. Normalmente a fase de design é a mais propicia para a incorporação de privacidade no software, pois é quando os requisitos são transformados em funcionalidades e o principal motivo é que os problemas descobertos no final ciclo de vida do software tornam-se mais difíceis e caros de corrigir (OMORONYIA, 2019).

Apesar disso, existe um conflito entre os requisitos funcionais e a privacidade que muitas vezes é agravado pela pressão organizacional por tempo de produção de software mais curto, de maneira que, uma abordagem de design estruturada e centrada na privacidade geralmente leva tempo, exigindo uma consideração das inconsistências existentes, e comparações de alternativa de design. Geralmente opta-se por sacrificar alguns interesses por conta da privacidade, porém isso costuma gerar problemas futuros, sendo assim, a alternativa é

projetar o software de uma maneira ganha-ganha de soma positiva (OMORONYIA, 2019). Isto é, que a funcionalidade total do sistema não seja prejudicada e se possível que os requisitos sejam otimizados (CAVOUKIAN, 2011).

Como parte dos requisitos para a implantação de privacidade preservando as funcionalidades do software, há a necessidade de ferramentas e técnicas que melhor permitam incorporar a privacidade nos estágios iniciais. Dentro desse cenário, a abordagem do PbD pode ser aplicada ao desenvolvimento de software, levando em consideração os requisitos de privacidade durante todo o processo de desenvolvimento, desde a concepção de um novo sistema, até o design e operação. Princípios como esse, formam a base para leis de privacidade e proteção de dados como a GDPR, eles também servem como alicerce para a criação de programas gestão de dados (OMORONYIA, 2019).

Instituído na década de 1990 pela Dra. Ann Cavoukian, Comissária de Informação e Privacidade de Ontário do Canadá, o PbD aborda sete princípios que foram idealizados sem que exista hierarquia entre eles ou ordem de relevância (MALDONATO, 2019). Cavoukian utilizou as Práticas de Informação Justa (FIPs - *Fair Information Practices)* como base para alguns dos princípios do PbD, elas são medidas de boas práticas para gestão de informação no meio digital, publicadas nos anos 1980 pela Organização para Cooperação e Desenvolvimento Econômico (OCDE), são oito práticas relacionados a uso, coleta e privacidade de dados. As FIPs tiveram grande influência nos regulamentos atuais de proteção e privacidade (GONZÁLEZ, 2019). Os princípios de PbD aplicados ao desenvolvimento de software são:

### 4.1 Proativo não reativo; preventivo não corretivo.

Agir de forma preventiva, antecipar situações que põem em risco a privacidade dos dados do titular e corrigir ou minimizar os danos antes que aconteçam (SILVA,2021). Dessa maneira, espera-se que a equipe de desenvolvimento tome providencias de mitigação de riscos antes que um incidente de dados aconteça, para que não afete a privacidade dos usuários durante a utilização do software (ABREU,2021). Portanto, deve-se adotar práticas fortes de privacidade de forma proativa e consistente no processo de desenvolvimento, assim como práticas organizacionais e de design de produto voltado ao usuário. De acordo com Cavoukian (2011), isso implica em:

- Comprometimento da alta gestão para estabelecer altos padrões de privacidade que vão além de regulamentos e leis. Os requisitos de privacidade dos usuários devem

ser considerados no projeto de software, a fim de obter a aceitação do usuário (CANEDO et al,2020).

- Construir uma cultura voltada a privacidade em que o comprometimento seja compartilhado. Toda a empresa deve seguir as normas de privacidade estabelecidas, não somente quem tiver contato direto com os dados.
- Utilizar métodos para reconhecer possíveis erros e consequência geradas pela não utilização da privacidade como fator determinante (GONZÁLEZ, 2019). Como relatório de impacto e avaliação de riscos.

### 4.2 Privacidade como padrão (*Privacy by default)*

A privacidade é o padrão do sistema, ou seja, já está definida normalmente, não é preciso que o usuário realize alguma ação para que seus dados se tornem privados. Sistemas e boas práticas devem proteger os dados pessoais de forma automática. A proteção de dados por padrão exige que se assegure que serão processados apenas os dados necessários para atingir sua finalidade específica (ICO, 2018). O conceito de *privacy by default* tem influência das FIPs, sendo eles:

- **Especificação de finalidade**: o titular de dados deve estar ciente das finalidades do uso de seus dados quando a coleta ocorrer, sendo elas comunicadas de forma clara e objetiva.
- **Limitação de coleta:** a coleta de dados deve ser limitada apenas ao necessário para o uso em suas finalidades.
- **Anonimização de dados:** Sempre que possível, a coleta de dados deve ocorrer de forma anonimizada. Assim como, o uso de dados por padrão deve ocorrer de forma a minimizar a identificação do titular
- **Uso, retenção e limitação de divulgação:** o uso, retenção e divulgação de dados pessoais deve se ater as especificações previamente consentidas pelo titular. Quando o propósito dos dados for cumprido, eles deverão ser descartados com segurança.

### 4.3 Privacidade incorporada ao design

A privacidade deve ser integrada no design, arquitetura do sistema e nas práticas de negócio, não como um complemento, mas como um componente essencial e sem diminuir suas funcionalidades. Essa integração deve ser feita de forma holística, considerando um amplo contexto, integrativa, pois todas as partes interessadas devem ser consideradas e criativa, porque

existem escolhas que precisam de uma resposta diferente do que se espera (CAVOUKIAN, 2011).

### 4.4 Funcionalidade total (soma positiva, não soma zero)

A privacidade é implementada em todo o projeto, mas ela não pode prejudicar a funcionalidade total do sistema, tendo uma soma positiva e não uma soma zero em que privacidade precisa sacrificar algo como segurança ou funcionalidade. Se possível deve haver a otimização de requisitos. A privacidade também deve levar em consideração o objetivo do software e satisfazer os objetivos legítimos da organização (CAVOUKIAN, 2011).

### 4.5 Segurança de ponta a ponta

A privacidade deve ser incorporada ao sistema antes da coleta de dados ser realizada, e deve ser continuamente protegida durante todo o ciclo de vida dos dados. Da coleta, até a total eliminação dessas informações, a segurança desses dados através de medidas, devem garantir a integridade, confidencialidade e disponibilidade da informação (CAVOUKIAN, 2011).

### 4.6 Visibilidade e transparência

As condições de uso e termos relacionados aos dados pessoais devem ser exibidos para os seus titulares de forma clara e simplificada, para que haja entendimento. Visibilidade e transparência são importantes para gerar responsabilidade e confiança. Este conceito também tem influência dos princípios da FIPs, sendo eles:

- **Prestação de contas:** é dever dos responsáveis pela coleta de DP do usuário ter cuidado com a proteção deles. Todos os procedimentos realizados com esses dados devem ser documentados, assim como as políticas de segurança usadas para resguardá-lo. Se houver a transferência de dados pessoais a terceiros, a proteção e privacidade deve ser assegurada por contrato.
- **Abertura:** para assegurar a transparência entre o titular e os agentes de tratamento, as políticas e boas práticas de segurança usadas para garantir a privacidade dos dados pessoais devem estar disponíveis ao titular.
- **Conformidade:** deve haver um canal de reclamação e avaliação para titulares junto a ANPD, dessa forma garantindo através do monitoramento o cumprimento das medidas de segurança e termos de uso previamente estabelecidos (CAVOUKIAN, 2011).

### 4.7 Respeito pela privacidade do usuário

O foco das medidas de privacidade desenvolvida tem que ser o usuário e seus interesses, oferecendo medidas como padrões de segurança adequado ao tipo de dado, avisos e notificações apropriadas tanto em forma quando em localização, e opções amigáveis de interface. É importante capacitar os usuários para que tenham papel ativo no gerenciamento de seus dados, eles devem atualizar suas informações sempre que preciso, e atentar-se se o tratamento de dados está sendo feito da maneira como foi definido. Isso é factível perante a solicitação da documentação sobre seus dados, assim é possível evitar abusos e uso indevido de dados pessoais por parte dos agentes de tratamento. Este conceito também tem influência dos princípios da FIPs, sendo eles:

- **Consentimento:** o titular tem que dar consentimento expresso de maneira clara para a coleta e uso de seus dados. Esse consentimento pode ser retirado a qualquer momento.
- **Acurácia:** os dados pessoais do titular devem estar atualizados e completos para que haja exatidão no cumprimento de suas finalidades.
- **Acesso:** o titular deve ter acesso aos seus dados quando forem solicitados, assim como, conhecimento de como estão sendo usado. Ele também tem o direito a solicitar alterações desses dados se necessário.
- A conformidade também tem que estar presente nesse cenário (CAVOUKIAN, 2011).

Esses princípios fundamentais orientam um programa de privacidade, eles são requisitos para desenvolvimento e implementação de sistemas e devem ser traduzidos em práticas especificas. Embora a implementação desse *framework* (“estrutura”) não garanta a adequação completa a LGPD, ele é considerado como uma boa prática de gerenciamento de dados pessoais e garante um programa de governança de privacidade eficiente, além de ser um diferencial no mercado para o desenvolvimento de software por ser um método focado em privacidade de dados além de segurança.

# 5 RECOMENDAÇÕES PARA A UTILIZAÇÃO DO *PRIVACY BY DESIGN* NO CICLO DE VIDA DE SOFTWARE

De acordo com o referencial teórico abordado nessa pesquisa é possível perceber que a LGPD instaura novos padrões de privacidade para o tratamento de dados, sendo preciso a adequação das empresas de software a lei. Assim, esse trabalho propõe recomendações baseadas no PbD para auxiliar nesse processo de concordância, elas orientam a utilização de princípios e práticas antes, durante e depois do processo de desenvolvimento de um software. Essas recomendações não extinguiram todas as possibilidades possíveis da utilização do PbD em relação a privacidade no desenvolvimento de sistemas, elas também não cobrem toda a LGPD, desse modo é possível uma futura continuidade no estudo da mesma problemática.

Iniciando antes do desenvolvimento estão as recomendações para preparar o ambiente empresarial, tornando a privacidade uma prioridade para a empresa, essa fase será chamada de planejamento. Em seguida, entrando no processo de desenvolvimento as recomendações estão divididas por fases de análise de requisitos, design, codificação e teste. Após a conclusão do software estão as recomendações para implantação e manutenção, dessa forma é possível visualizar quais medidas devem ser inseridas em cada etapa da criação de um sistema.

## 5.1 Planejamento

- Solicitar comprometimento da alta gestão, visando assim garantir que existe atenção e recursos suficientes para serem utilizados na proteção à privacidade quando o software for desenvolvido (BERNSMED, 2016);
- Elaborar um plano de treinamento para funcionários contendo as leis (LGPD), normas, métodos, boas práticas (PbD), ferramentas e procedimentos que serão utilizados para garantir a privacidade durante e após o desenvolvimento do sistema (DATATILSYNET, 2017);
- Nomear um responsável pela privacidade (CAVOUKIAN, 2011);
- Construir uma cultura voltada a privacidade em que a responsabilidade seja compartilhada (CAVOUKIAN, 2011);
- Definir e atribuir responsabilidades concretas para que cada membro da organização esteja claramente ciente de suas tarefas no que diz respeito à privacidade (AEPD, 2019);

- Estabelecer canais de comunicação para colaboração e consulta dos participantes de forma a compreender e reunir múltiplos interesses que, à primeira vista, podem parecer divergentes (AEPD, 2019);
- Realizar auditorias de privacidade dentro da empresa (BERNSMED, 2016).

## 5.2 Análise de Requisitos

- Assumir que podem coexistir interesses diferentes e legítimos, os da organização e os dos usuários a quem presta serviços, e que é necessário identificá-los, avaliá-los e equilibrá-los em conformidade (AEPD, 2019);
- Identificar Requisitos de proteção de dados e de segurança da informação (DATATILSYNET, 2017). Os requisitos de proteção de dados são referentes a privacidade de dados pessoais e os requisitos de segurança da informação se referem a proteção de qualquer dado que deva ser protegido.
- Definir políticas de privacidade consistente com os requisitos de privacidade;
- Escolher medidas de segurança que melhor se adequam ao perfil da empresa com base nos requisitos;
- Realizar Avaliação de riscos (DATATILSYNET, 2017);
- Realizar Avaliação de impacto (DATATILSYNET, 2017);
- Definir Níveis de tolerância ao risco que a empresa está disposta a tolerar, baseado na avaliação de risco (DATATILSYNET, 2017);
- Realizar o mapeamento de dados que serão coletados pelo software. Devendo conter o tipo de dados, a quem pertencem, quais informações são possíveis obter sobre o titular através desses dados, quantidade de dados a serem coletados, operações que serão realizadas, quem irá tratar esses dados, onde eles serão armazenados e período de armazenamento. (DATATILSYNET, 2017);
- Deve-se definir a finalidade para que os dados serão coletados (CAVOUKIAN, 2011);
- O tratamento de dados tem que ser lícito, justo e transparente (DATATILSYNET, 2017);
- Para a coleta e tratamento de dados deve-se seguir as práticas de limitação de coleta, anonimização de dados, uso, retenção e limitação de divulgação (DATATILSYNET, 2017);
- A segurança no processo de tratamento dos dados tem que ser garantida, utilizando meios como criptografia e controle de acesso (DATATILSYNET, 2017);
- Tornar os critérios de coleta de dados o mais restritos possível (AEPD, 2019);

- Limitar o uso de dados pessoais aos objetivos para os quais foram coletados e garantir que haja uma base legítima para o processamento (AEPD, 2019);
- Restringir o acesso aos dados pessoais às partes envolvidas no tratamento e de acordo com a função subjacente à criação de perfis de acesso diferenciados (AEPD, 2019);
- Definir prazos rígidos para retenção de dados e estabelecer mecanismos operacionais que garantem o cumprimento (AEPD, 2019);
- Criar barreiras tecnológicas e processuais para a vinculação não autorizada de fontes independentes de dados (AEPD, 2019);
- O software desse ser projetado e desenvolvido a fim de permitir que o controlador e o operador possam documentar e demonstrar como os requisitos da lei estão sendo seguidos (AEPD, 2019);
- Informar ao usuário/titular como o software funciona, usando linguagem simples e clara;
- Garantir que os usuários tenham acesso a configurações de privacidade, permitindo alteração de consentimento para o tratamento de dados, assim como visualizar e modificar ou excluir seus dados (AEPD, 2019);
- Verificar se o mesmo tipo de informação está sendo coletado em vários lugares (funcionalidade duplicada) e avaliar se a funcionalidade pode ser simplificada (DATATILSYNET, 2017).

### 5.3 Design

- Buscar soluções e alternativas para cumprir os requisitos definidos sem que as funcionalidades de privacidade e segurança alterem o proposito do software e sua funcionalidade total (AEPD, 2019);
- Analisar a superfície de ataque do software pré-projetado para reduzir as oportunidades de explorar pontos fracos e vulnerabilidades no software (DATATILSYNET, 2017);
- Após a transformação dos requisitos em funcionalidade é importante realizar uma revisão para simplificar as funcionalidades desnecessárias se possível. Dessa forma é possível reduzir a probabilidade de erros de software (DATATILSYNET, 2017);
- Utilizar imagens, ícones e símbolos no software para tornar as informações sobre privacidade mais claras e legíveis. Animações, vídeos e som podem ser usados para personalizar informações e instruções (DATATILSYNET, 2017);

- Implementar configurações de privacidade “robustas” por padrão e onde os usuários são informados das consequências para sua privacidade quando os parâmetros estabelecidos são modificados (AEPD, 2019);
- Disponibilizar informação completa e adequada que conduza a um consentimento informado, livre, específico e inequívoco que deve ser explícito em todos os casos que o requeiram (AEPD, 2019);
- Implementação de mecanismos eficientes e eficazes que permitem aos titulares dos dados exercer os seus direitos em matéria de proteção de dados, como autenticação multifator para realizar login em perfil, alertas de privacidade e notificações (AEPD, 2019).

É indispensável que o software seja desenhado de forma a:

- Minimizar e limitar a quantidade de dados pessoais coletados e processados. Uma boa regra para essa prática é selecionar os dados antes de coletar;
- Ocultar e proteger os dados pessoais de pessoas não autorizadas, usando técnicas de anonimização parcial, criptografia, entre outros;
- Separar o tratamento ou armazenamento de várias fontes de dados pessoais. Ou seja, alocar esses dados em diferentes locais ou separar as informações durante o tratamento para impossibilitar a criação de um perfil;
- Reduzir o nível de sensibilidade e detalhamento de dados pessoais sempre que possível. Pode-se usar técnicas de anonimização para isso;
- Tornar públicas as políticas de privacidade e proteção de dados que regem o funcionamento da organização;
- Manter registro das operações de tratamento (DATATILSYNET, 2017).

## 5.4 Implementação

- Utilizar uma lista aprovada de ferramentas e bibliotecas. Essa lista deve conter Biblioteca de códigos, linguagem de programação, sistema de controle de versão, ferramentas de teste, infraestrutura, ferramentas de monitoramento, servidor de log, *framework* e APIs de terceiros. Também deve estar incluso ferramentas e componentes de suporte, que ter devem ter seus riscos e vulnerabilidades avaliados e documentados (DATATILSYNET, 2017);
- Verificar vulnerabilidades no código (DATATILSYNET, 2017);

- Realizar revisão de código e análise de código estático com regras de segurança e realizar a desabilitação de funções e módulos inseguros principalmente em APIs, bibliotecas e módulos de terceiros identificados na revisão (DATATILSYNET, 2017).

### 5.6 Teste

- Verificar se as funcionalidades de privacidade não alteram a funcionalidade total do sistema;
- Verificar se todos os requisitos de privacidade foram atendidos da melhor forma possível;
- Verificar se o software coleta apenas os dados pessoais necessários;
- Realizar testes de segurança como o teste dinâmico, teste de fuzz e penetração (DATATILSYNET, 2017);
- Deve-se verificar se as tentativas não autorizadas de aceso são registradas como violação de dados (DATATILSYNET, 2017);
- Realizar análise de vulnerabilidades nas camadas de aplicação de rede, por exemplo realizando testes de senha padrão, senhas armazenadas em arquivos, SQL *injection*, *script injection*, acesso não autorizado de *log*, *backups* e locais (DATATILSYNET, 2017);
- Realizar teste de controle de acesso e acesso real.

### 5.7 Implantação

- Criar protocolos de resposta a incidentes, contendo como classificar um incidente, procedimentos de detecção, análise, reporte e tratamento (DATATILSYNET, 2017);

- Realizar uma verificação final de segurança contendo pelo menos uma verificação de requisitos de proteção de dados e segurança, avaliação de risco e impacto e resultado dos testes;

- Realizar arquivamento de toda documentação realizada durante o desenvolvimento de software para futuro uso (DATATILSYNET, 2017);

- Publicar cláusulas de informação concisas, claras e compreensíveis que sejam facilmente acessíveis e permitam que os titulares dos dados compreendam o âmbito do tratamento dos seus dados, os riscos a que podem estar expostos, bem como a forma de exercer os seus direitos em matéria de proteção de dados (AEPD, 2019).

## 5.8 Manutenção

- Criar um central de contato que se encarregue de incidentes e forneça atualizações, diretrizes e informações para usuários e titulares de dados (DATATILSYNET, 2017);
- Utilizar procedimentos de proteção contínua para serviços de manutenção, atualização e operação realizando testes de segurança, análise de vulnerabilidades, testes de penetração de software, infraestrutura e rede, depuração de erros (DATATILSYNET, 2017).

## 5.9 LGPD e as recomendações

As recomendações aqui propostas visam auxiliar no cumprimento dos seguintes artigos da LGPD:

- Art. 6º que fala que as atividades de tratamento devem observar os princípios de finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (BRASIL, 2018);
- Art. 7º a 10º que falam sobre os requisitos para o tratamento de dados pessoais, tais como consentimento, acesso facilitado, finalidade, forma de tratamento e identificação dos agentes de tratamento (BRASIL, 2018);
- Art. 15º e 16º que falam sobre o término do tratamento de dados e suas condições como cumprimento da finalidade, término de prazo especificado, revogação de consentimento e exclusão de dados (BRASIL, 2018);
- Art. 17º a 19º falam sobre os direitos do titular tais como direitos de liberdade, intimidade e privacidade através de confirmação de tratamento, acesso facilitado aos dados coletados e eliminação de dados (BRASIL, 2018);
- Art. 37º e 38º falam sobre os deveres do controlador e operado de dados, tais como manter registro do tratamento e elaborar relatório de impacto (BRASIL, 2018);
- Art. 41º que fala sobre a indicação de um encarregado pelo tratamento de dados pessoais (BRASIL, 2018);
- Art. 46º a 49º falam sobre segurança e sigilo de dados que devem ser garantidas através da utilização de medidas técnicas e administrativas, assim como ações que devem ser tomadas caso aconteça um incidente de dados (BRASIL, 2018);

- Art. 50º e 51º que falam sobre boas práticas e governança, orientando o uso de boas práticas e a criação de um programa de governança em privacidade (BRASIL, 2018).

Para mais detalhes sobre as leis utilizadas deve-se consultar o Anexo A.

# 6 CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados provocou mudanças consideráveis no atual panorama de proteção a dados pessoais, em decorrência ao aumento da utilização de dados como ativos, e da crescente ocorrência de incidentes de dados, medidas de segurança se tornaram uma prioridade. Dessa forma, medidas protetivas com altos padrões de segurança se tornam indispensável para resguardar os dados.

Essas medidas exigem que as organizações que utilizam dados pessoais se reinventem para garantir adequação aos padrões de segurança impostos, em consequência, empresas de software precisam utilizar medidas e práticas de privacidade mais rígidas para garantir a privacidade de seus usuários. Assim, o conceito de *privacy by design* ganha destaque, já que ele garante a privacidade por concepção e por padrão de sistema. Os princípios dessa abordagem orientam a utilização de práticas de privacidade durante todo o processo de desenvolvimento, o que o torna apropriado para a problemática criada pela LGPD. Dessa maneira surge a necessidade de instruções sobre a aplicação do PbD no processo de desenvolvimento de software

Para analisar as recomendações que o PbD empregado a LGPD trazem para empresas de software, foram descritas as principais recomendações da LGPD sobre proteção e privacidade de dados, desse modo foi possível entender a demanda que a lei impõe. Assim também, foi realizada a verificação dos princípios do PbD e as práticas que compões cada um. Em decorrência a isso, se faz entender como a utilização da abordagem PbD torna possível a criação de um programa de gestão de privacidade em conformidade com a LGPD.

Ao analisar as fases do ciclo de vida de desenvolvimento de um software com os princípios do PbD foi possível definir um conjunto de recomendações para implementar essa abordagem de privacidade no processo de criação de um software. Tais recomendações podem ser utilizadas para orientar empresas de software, assim como desenvolvedores a verificarem o nível de privacidade atual de um sistema, assim como facilitar a implementação do PbD.

Os resultados encontrados nesse projeto se classificam como uma série de recomendações sobre o uso de privacidade e sua importância. Apesar da necessidade de adequação de empresas de software ao novo padrão de segurança estabelecido pela LGPD, e do papel de importância o PbD desempenha nessa questão, ainda existe uma dificuldade em utilizar essa abordagem, sendo um dos motivos é a não definição de diretrizes concretas de implementação, o que dificulta sua utilização.

Outro fator é a falta de conhecimento sobre privacidade de dados por parte dos profissionais brasileiros, pois a discussão sobre assunto de privacidade no Brasil anda é escassa devido ao pouco tempo de vigência da LGPD. Existe ainda a dificuldade em utilizar novas práticas, e leva tempo para criar uma cultura de privacidade, porém com paciência, investimento e esforço da alta gestão é possível alcançar a conformidade em relação a medidas técnicas de proteção e privacidade de dados.

As principais dificuldades encontradas na realização desse trabalho foram a carência de bibliografia a respeito da utilização do PbD no desenvolvimento de software, com destaque à falta de pesquisa sobre privacidade de dados no Brasil, as principais fontes sobre esse assunto provém do Reino Unido. Isso permite a identificação de um amplo espaço de pesquisa brasileira em ascensão nessa área.

Diante do exposto, espera-se que os resultados obtidos com este trabalho contribuam para o esclarecimento da importância e crescimento do uso de leis, e medias de privacidade de dados no desenvolvimento de software. Principalmente a abordagem *privacy by design* e a lei geral de proteção de dados.

## 6.1 Trabalhos futuros

Recomendasse que sejam feitas pesquisas sobre:

- As dificuldades de se aplicar privacidade como um requisito essencial no projeto de software;
- Estudo de casos sobre a implementação do *pivacy by design;*
- A implementação de avaliações de impacto de risco no desenvolvimento de software.

# REFERÊNCIAS


AEPD. **A Guide to Privacy by Design**. Agencia Española Protección Datos, 2019

ALTVATER, Alexandra. **What Is SDLC? Understand the Software Development Life Cycle**. Stackify, 2020. Disponível em: <https://stackify.com/what-is-sdlc/>. Acesso em: 24 abr. 2022.

ARAGÃO, Alexandre. **5 grandes vazamentos de dados no Brasil — e suas consequências.** Jota, São Paulo, 2022. Disponível em: < https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022> Acesso em: 2022.

BARROS, Laura. **Privacy by design e LGPD: impactos e desdobramentos.** Consultor juridico, 2021. Disponivel em: < https://www.conjur.com.br/2021-jul-04/publico-pragmatico-privacy-by-design-lgpd-impactos-desdobramentos > 7 maio. 2022.

BENG et al. Software Development Life Cycle AGILE vs Traditional Approaches. **International Conference on Information and Network Technology**, Singapore, IPCSIT vol. 37, 2012.

BERREDO, Lucas. **Banco Central confirma vazamento de 160 mil chaves Pix**. Olhar digital, 2022. Disponível em: < https://olhardigital.com.br/2022/01/21/seguranca/banco-central-confirma-vazamento-de-160-mil-chaves-pix/> Acesso em: 1 jun. 2022.

BERNSMED, Karin. **Applying Privacy by Design in Software Engineering - An European Perspective**. SOFTENG, p. 1-8, 2016.

BIG WATER. **Software Development Life Cycle (SDLC)**. 2019. Disponível em: < https://bigwater.consulting/2019/04/08/software-development-life-cycle-sdlc/ > Acesso em: 21 Jan. 2022.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018.

CANEDO *et al.* Perceptions of ICT Practitioners Regarding Software Privacy. **Entropy** (Basel, Switzerland), V. 22.4, No 429, 2020.

CARVALHO, Thaís A. **Aplicabilidade da lei geral de proteção de dados e da metodologia privacy by design nos termos de uso e de política de privacidade**. TCC (Graduação) - Curso de direito, Faculdade De Direito De Vitória, Vitória, 2019.

CAVOUKIAN, Ann**.** Privacy by design, The seven foundational principles. Implementation and mapping of fair information practices. **Information and Privacy Commissioner of Ontario**, Toronto, v. 2, p. 1-12, 2011.

COURSERA. **What Does a Software Engineer Do?**. 2022. Disponível em: <https://www.coursera.org/articles/software-engineer> Acesso em: 10 jun. 2022

CLOUDFLARE. **O que são Práticas de Informação Justa?| FIPPs**. 2021. Disponível em: <https://www.cloudflare.com/pt-br/learning/privacy/what-are-fair-information-practices-fipps/> Acesso em: 7 maio. 2022.

DATATILSYNET. **Software development with Data Protection by Design and by Default**. 2017. Disponível em: <https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true> Acesso em 15 maio 2022.

FLOWTI. **Governança de TI: saiba tudo sobre este conceito**. 2021. Disponível em: < https://flowti.com.br/blog/governanca-de-ti-saiba-tudo-sobre-este-conceito > Acesso em: 4 fev. 2022

GET PRIVACY. **Entenda o conceito de Privacy by Design e sua relação com a LGPD**. 2021. Disponível em: <https://getprivacy.com.br/privacy-by-design-lgpd/#:~:text=ou%20outro%20objetivo.-,5.,armazenamento%20at%C3%A9%20o%20seu%20descarte.> Acesso em: 22 maio. 2022.

GET PRIVACY. **Adequação à LGPD: por que investir em Segurança da Informação?** 2021. Disponível em: < https://getprivacy.com.br/lgpd-seguranca-da-informacao/> Acesso em: 22 maio. 2022.

GUIA DE BOAS PRÁTICAS - Lei geral de proteção de dados (LGPD). **Gov**, Brasil, v.2, 2020.

HOFMANN, **Sarah. New IBM Report - The Real Cost Of A Data Breach In 2021**. Cyber pilot, 2021. Disponível em: < https://www.cyberpilot.io/cyberpilot-blog/new-ibm-report-the-real-cost-of-a-data-breach-in-2021> Acesso em: 14 abr. 2022.

IBM Security. Cost of data breach report. **IBM Corporation**, New York, 2021.

IBM Security. **Estudo IBM: Gastos com violações de dados caem no Brasil, mas país é o mais provável a ter ataques de hackers entre os pesquisados**. 2018. Disponível em: < https://www.ibm.com/blogs/ibm-comunica/estudo-ibm-gastos-com-violacoes-de-dados-caem-no-brasil/ > Acesso em: 14 abr. 2022.

IOC. **Data protection by design and default.** Information Commissioner's Office, 2018. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> Acesso em 10 Jun. 2022

PENTLAND, Alex S. The data-driven dociety. **Scientific American**, US, v. 79, 2013

JEVTIC, Goran. **What is SDLC? Phases of Software Development, Models, & Best Practices**. PhonixNAP, 2019. Disponível em: <https://phoenixnap.com/blog/software-development-life-cycle#:~:text=Software%20Development%20Life%20Cycle%20is,%2C%20Test%2C%20Deploy%2C%20Maintain.> Acesso em 10 jun. 2022

KROENER, Inga; WRIGHT, David. A Strategy for Operationalizing Privacy by Design. **The Information Society**, 2014.

LANGEN, talita da S. C. **Lei geral de proteção de dados: diagnóstico do grau de conformidade de micro e pequenas empresas**. Dissertação (Mestrado) - Mestrado profissional em administração das micro e pequenas empresas, Centro Universitário Campo Limpo Paulista, Campo limpo paulista, 2020.

LIMA, Lindamaria**. A Lei Geral de Proteção de Dados Pessoais e o Privacy by Design e Privacy by Default.** Tripla, 2021. Disponível em <https://tripla.com.br/a-lei-geral-de-protecao-de-dados-pessoais-e-o-privacy-by-design-e-privacy-by-default/> Acesso em: 7 maio. 2022.

LG LUGAR DE GENTE. **Controlador e operador na LGPD: qual o papel da sua empresa?** 2021. Disponível em: < https://blog.lg.com.br/controlador-operador-lgpd/> Acesso em: 9 Mar. 2022.

MANCUZO, Ronnie. **Brasil é o 6º país com mais vazamentos de dados no planeta, aponta levantamento**. Olhar digital, 2022. Disponível em: <https://olhardigital.com.br/2022/03/17/seguranca/brasil-e-o-6o-pais-com-mais-vazamentos-de-dados-no-planeta-aponta-levantamento/> Acesso em: 1 jun. 2022.

MORAES, Thamiris. **Marco Civil e LGPD: Qual a diferença entre as leis e o que muda na prática**. Mambo, 2021. Disponível em: <https://mambowifi.com/marco-civil-e-lgpd-diferencas/#:~:text=Enquanto%20o%20Marco%20Civil%20da,de%20dados%20(inclusive%20offline). > Acesso em: 4 fev. 2022.

NOVAIS, Gustavo G. A.; ARAÚJO, João P. S.; SOUZA, Júlio A. M. **ESTUDO TAXONÔMICO ENTRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A ABNT NBR ISO/IEC 27001.** TCC (Graduação) - Curso de Sistemas de Informações, Centro Universitário do Planalto Central Aparecido dos Santos. Brasília, 2020.

NUNES, Gabriela V. M. **Governança e boas práticas na lei geral de proteção de dados pessoais: dos programas de compliance.** TCC (Graduação) – Curso de Direito, Universidade De Brasília Faculdade De Direito, Brasília, 2019.

OMORONYIA, Inah. Why Is Baking Privacy into Software Design Hard? **ITNow**, Web, v. 61.3, p. 44-45, 2019.

OMORONYIA, Inah; ETUK, Ubon; INGLIS, Peter. A Privacy Awareness System for Software Design. **International Journal of Software Engineering and Knowledge Engineering**, Vol. 29, No. 10, 2019.

PEREIRA, Aline de S. DPO: o papel do Data Protection Officer na LGPD. SajAdv , 2021. Disponível em: < https://blog.sajadv.com.br/o-papel-do-dpo-na-lgpd/> Acesso em: 19 maio 2022.

SANTOS, Elcio. **Governança de Dados: a LGPD vai estar no calcanhar de muitas empresas.** Alway on, 2021. Disponível em: <https://aodigital.com.br/governanca-de-dados-lgpd/> Acesso em: 1 abr. 2022.

SANTOS, Juliana G.; SILVA, Sabrina L. C. **Análise dos impactos da lei geral de proteção de dados pessoais sobre a governança e segurança de dados**. Tcc (Graduação) – Curso De

Sistema De Informação, Centro De Ciências Exatas E Tecnologia, Escola De Informática Aplicada, Universidade Federal do Estado do Rio de Janeiro, Rio De Janeiro, 2020.

SILVA, Camila. **Privacy by Design: o que é, princípios e como implementar essa metodologia em sua empresa.** Unico, 2021. Disponível em: <https://unico.io/unicocheck/blog/metodologia-privacy-by-design/ > Acesso em: 7 maio. 2022.

SOMMERVILLE, Ian. **Engenharia de Software.** 10ª ed. São Paulo: Pearson, 2019.

STEFANINI. **Você sabe o que é a gestão em segurança da informação?** 2019. Disponível em: < https://stefanini.com/pt-br/trends/artigos/gestao-em-seguranca-da-informacao> Acesso em: 4 fev. 2022.

TENBU. **Princípios Gerais da LGPD e Exemplos de Boas Práticas**. 2021. Disponível em: < https://www.tenbu.com.br/principios-gerais-da-lgpd-e-exemplos-de-boas-praticas/ > acesso em 3 maio 2022.

VASCONCELOS, Esther. **Como o setor de TI será impactado diretamente pela LGPD?** Rede jornal contábil, 2020. Disponível em: < https://www.jornalcontabil.com.br/como-o-setor-de-ti-sera-impactado-diretamente-pela-lgpd/ > Acesso em: 2022.

ZANARDO, Paulo. **Segurança nossa de cada dia para o desenvolvimento de software**. Imasters, 2019. Disponível em: < https://imasters.com.br/desenvolvimento/seguranca-nossa-de-cada-dia-para-o-desenvolvimento-de-software > Acesso em: 21 Jan. 2022.