Conformidade com a LGPD por Meio de Requisitos de Negócio e Requisitos de Solução

Diego Menegazzi[1] and Carla Silva[2]

[1]Instituto Federal Catarinense, Luzerna, Brasil
diego.menegazzi@ifc.edu.br

[2]Centro de Informática, Universidade Federal de Pernambuco, Recife, Brasil
ctlls@cin.ufpe.br

Resumo Em agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em setembro de 2020. Segundo a LGPD, as organizações públicas e privadas devem seguir regras para a coleta e o tratamento de informações pessoais, de modo que o não cumprimento dessas obrigações pode acarretar multas que chegam a R$ 50 milhões por infração. As organizações públicas e privadas vêm enfrentando dificuldades para conseguir alcançar essa conformidade. Esse problema pode estar associado à interpretação da Lei, muitas vezes ambígua, e pela falta de conhecimento jurídico dos analistas de sistemas. A extração de requisitos e a sua correta interpretação também são passíveis de erros. Esse problema é comum em pequenas e médias empresas que não possuem um setor ou apoio jurídico. Fornecer técnicas e ferramentas para profissionais de Tecnologia da Informação e Comunicação (TIC) que trabalham com privacidade de dados é fundamental para alcançar a conformidade com a LGPD. Assim, propomos um guia de 6 etapas para apoiar os profissionais de TIC nas atividades de conformidade legal por meio de requisitos de negócio e de solução com foco no artigo 6o da LGPD. O guia foi disponibilizado em um website onde há uma seção descrevendo os seus componentes: o modelo de mapeamento de dados, os requisitos de negócio, os requisitos de solução e o catálogo de controles de privacidade. Por fim, o website conta, ainda, com um vídeo de explicação de todos os componentes e as 6 etapas do guia, além de um exemplo ilustrado da aplicação do método.

Keywords: Engenharia de Requisitos · Engenharia de Software · Lei Geral de Proteção de Dados · Proteção de Dados Pessoais

1 Introdução

A transformação digital trouxe inúmeras mudanças na forma como a humanidade vive, pois hoje é possível fazer compras, realizar pagamento de contas, estudar, trabalhar, praticar atividades de lazer e muito mais de forma totalmente digital [1]. Diante dessa transformação digital, existem diversos dispositivos conectados que acompanham nossas rotinas, coletando, transmitindo, armazenando e compartilhando uma quantidade enorme de dados [7]. É o caso da socialização

Proceedings of the 26th Workshop on Requirements Engineering (WER23), August 15-17, 2023, Porto Alegre, RS, Brazil.
DOI: 10.29327/1298356.26-16

online por meio dos serviços prestados pela Rede Social Virtual, como *Facebook, Messenger, Instagram, WhatsApp, Google, Twitter, LinkedIn*, entre outros, que transformaram as tendências convencionais de amizade e comunicação.

Recentemente houve diversos casos de violação de privacidade de dados dos usuários em várias plataformas, mas o caso mais famoso aconteceu em 2018, relativo à empresa *Cambridge Analytica*, que expôs 87 milhões de dados pessoais de usuários do *Facebook* e os utilizou para fins políticos. Diante de situações como essa, diversos países tomaram medidas para evitar a violação de dados pessoais e, em maio de 2018, entrou em vigor na União Europeia a lei chamada *General Data Protection Regulation* (GDPR). A intenção é proteger a privacidade dos dados pessoais dos cidadãos europeus e evitar o vazamento de informações. No Brasil, em agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados (LGPD) [5], que entrou em vigor em setembro de 2020 e tem como base a GDPR [6].

A extração de requisitos e a sua correta interpretação também são passíveis de erros, um problema que é comum em pequenas e médias organizações que não possuem um setor ou um apoio jurídico. Fornecer técnicas e ferramentas para profissionais de TIC que trabalham com privacidade de dados é fundamental para alcançar a conformidade com a LGPD. Por exemplo, a lei diz que as empresas devem utilizar medidas técnicas para proteger os dados contra acessos não autorizados, situações acidentais ou ilícitas, destruição, perda, alteração, difusão, mas não deixa evidente como devem ser tomadas essas medidas [5].

Diante do exposto, existe a necessidade de ajudar as organizações a atingir a conformidade com a LGPD já que, por ser um tema recente, existem poucas abordagens sobre o assunto, sendo a maioria parte da literatura cinzenta (*Grey literature*). Portanto, este trabalho visa definir uma guia para as organizações entenderem as obrigações da LGPD e identificar medidas para alcançar a conformidade dos sistemas de software com a LGPD.

O trabalho apresentado aqui alcança os seguintes objetivos específicos: (i) Analisar na literatura possíveis trabalhos relacionados à Engenharia de Requisitos com o tema de conformidade com leis de proteção de dados; (ii) Propor um guia para alcançar a conformidade de sistemas de software com a LGPD por meio de Requisitos de Negócio e Requisitos de Solução; (iii) Propor um modelo de mapeamento de dados pessoais; (iv) Criar um catálogo de controles de privacidade relacionando os princípios da LGPD; e (v) Definir um website para o guia (https://cin.ufpe.br/ dm5/guia-lgpd/) que pode ser acessado pela Internet.

Não faz parte do escopo deste artigo apresentar o questionário de análise da viabilidade do guia para profissionais de TIC e os resultados obtidos da aplicação do guia proposto e sua avaliação por parte de profissionais de TIC interessados na conformidade com a LGPD.

Este documento está estruturado da seguinte forma: A seção 2 apresenta os trabalhos relacionados. A seção 3 detalha a contribuição deste trabalho - o Guia de Conformidade de Requisitos de Negócio com a LGPD. Por fim, a seção 4 descreve as conclusões e direcionamentos para trabalhos futuros.

2 Trabalhos Relacionados

Em 2020, pouco havia sido tratado sobre como auxiliar as organizações a alcançar a conformidade legal. Diversos pesquisadores e profissionais, então, passaram a investigar diferentes soluções ou abordagens para que as organizações públicas ou privadas pudessem se adequar às leis de proteção de dados. Essas abordagens compreendem guias, roteiros, modelos de processos, software ou soluções de mapeamento de dados. A seguir apresentamos algumas das pesquisas relacionadas ao guia proposto. Utilizamos como critério de escolha os trabalhos que tinham foco em apoiar as atividade de Engenharia de Requisitos para alcançar a conformidade com a LGPD. No entanto, incluimos também o trabalho base que inspirou o guia proposto, o *GuideMe* de Ayala-Rivera e Pasquale [4] que tem como foco a conformidade de requisitos com a GDPR.

O *GuideMe* possui seis etapas que suporta a elicitação de requisitos de solução vinculados às obrigações da GDPR. O guia visa auxiliar as organizações a entender as obrigações da GDPR e identificar medidas para garantir a conformidade legal por meio da utilização de controles de privacidade que devem ser implementados nos sistemas de software da organização. O trabalho trata basicamente da legislação de proteção de dados da União Europeia, que, apesar de ser muito semelhante à LGPD do Brasil, possui algumas diferenças que precisam ser observadas. A presente pesquisa propõe um guia de conformidade com a LGPD adaptado do *GuideMe*.

Araújo et al. [3] propõem um método para obter a conformidade dos processos de negócio em relação à LGPD. Seu método consiste em um catálogo de padrões de modelagem representados com a notação BPMN. O estudo foi avaliado e validado por meio de um questionário respondido por uma turma de pós-graduação na Universidade Federal de Pernambuco (UFPE). O método, chamado de BPMN4LGPD orienta os analistas na avaliação da conformidade dos processos de negócio com a LGPD. Os resultados da avaliação demonstraram que a modelagem do processo de negócio é a etapa mais difícil.

Alves e Neves [2] realizaram entrevistas com cinco analistas de requisitos de uma organização do poder judiciário para entender os principais desafios enfrentados por eles para especificar requisitos de privacidade em conformidade com a LGPD. Com base nos resultados das entrevistas foram propostos padrões de privacidade omo parte de uma abordagem para especificar requisitos de privacidade de forma ágil e que contém diretrizes simples em formato de templates ou checklists. O trabalho apresenta a definição de um padrão de requisitos de privacidade e não um guia extensivo e detalhado para alcançar a conformidade com a LGPD, como o guia aqui proposto.

3 Guia de Conformidade de Requisitos de Negócio com a LGPD

O guia proposto pode ser aplicado em sistemas que já estão em modo de produção - ou seja, que já estão sendo utilizados por seus usuários - ou para novos

sistemas que precisam ser desenvolvidos. As etapas do guia são: Auditoria de Dados, Análise de Lacunas, Planejamento e Preparação, Revisão do Plano de Ação, Execução e Revisão Pós-implementação. Para apoiar a execução das etapas, o guia é composto de: Modelo de Mapeamento de Dados, Requisitos de Negócio, Requisitos de Solução e Catálogo de Controles de Privacidade. A próxima seção explica cada etapa. O exemplo de uso do guia no sistema do processo seletivo do Instituto Federal Catarinense (IFC) pode ser encontrado no website (https://cin.ufpe.br/~dm5/guia-lgpd/ ou http://bit.ly/lgpdguide) desenvolvido para disponibilizar o guia para potenciais usuários.

3.1 Etapas

1ª Etapa - Auditoria de Dados. Nesta etapa, é realizado o mapeamento de dados, que ocorreu por meio de entrevista com a pessoa responsável pelo setor que manipula os dados. Para auxiliar na coleta de informações, foi utilizado um modelo de mapeamento de dados construído a partir da experiência em entrevistas realizadas no IFC e do modelo disponibilizado pelo setor de gerenciamento de dados da instituição. Este modelo de mapeamento de dados não existe no trabalho base [4].

2ª Etapa - Análise de Lacunas. Esta etapa requer a realização de uma análise do mapeamento de dados realizado na primeira etapa, objetivando identificar áreas (por exemplo, fluxos, processos, sistemas) que precisam ser aprimoradas por meio de ações corretivas ou preventivas. Em outras palavras, essa atividade permite focar nos princípios da LGPD com os quais o sistema não está em conformidade. Para ajudar nesse processo, o analista de sistemas deve usar os requisitos de negócio para identificar as lacunas. O profissional deve, ainda, responder um questionário de análise de lacunas (reusado de [3]). Assim, com base neste questionário e na experiência do analista, será possível identificar as violações do sistema/organização com relação aos princípios da LGPD.

3ª Etapa - Planejamento e Preparação. Nesta etapa, será realizado o planejamento para solucionar as violações do sistema/organização com relação aos princípios da LGPD. Para isso, são observados os requisitos de negócio, as recomendações de alterações indicadas na 2ª etapa e o catálogo de controles de privacidade, que é necessário para satisfazer as obrigações legais específicas. Como resultado, temos os requisitos de solução, que apoiarão a 4ª etapa do guia.

4ª Etapa - Revisão do Plano de Ação. Nesta etapa, todos os *stakeholders* revisam o plano de ação elaborado na terceira etapa. A revisão antes da execução é necessária, pois é preciso avaliar se as mudanças afetarão o funcionamento do negócio ou do sistema. Embora os controles de privacidade listados no catálogo forneçam um conjunto de mecanismos que já se provaram úteis, conforme estudado na literatura, eles não são a única maneira de satisfazer um requisito de privacidade. Portanto, as partes interessadas devem avaliar os prós e contras dos controles de privacidade sugeridos, de modo a selecionar um ou mais, dependendo sempre do cenário. Por exemplo, como sugestão para atender o princípio da responsabilização e prestação de contas, é recomendado que a organização implemente o registro de logs no sistema, porém, dependendo da situação, a

organização não tem colaboradores suficientes para desenvolver ou implementar essa funcionalidade, de modo que é necessário que ela procure alternativas para cumprir o princípio. É preciso, então, revisar esses requisitos com os *stakeholders*, para que se tenha certeza de que as medidas não afetarão o desempenho ou as funcionalidades do sistema.

5ª Etapa - Execução. Nesta etapa, após a análise feita pelos *stakeholders* e os requisitos de solução terem sido especificados e aprovados para o cenário em questão, a equipe de desenvolvimento de software deve realizar a implementação das soluções definidas. Nesta etapa, caso a organização possua profissionais de Direito e/ou Privacidade, é importante que eles façam o acompanhamento das implementações das soluções para contribuir no processo de validação dos controles de privacidade escolhidos.

6ª Etapa - Revisão Pós-implementação. Finalmente, as organizações precisam garantir que os requisitos de solução foram atendidos. Isso pode ser verificado por meio da avaliação de processos e procedimentos com especialistas em TI, Direito e conformidade. Além disso, auditorias regulares devem ser agendadas para identificar os requisitos de solução que podem precisar de revisão.

3.2 Requisitos de Negócio

A LGPD possui diversas regras que a organização precisa seguir. Extrair essas regras ou esses requisitos de um texto legal e interpretá-los adequadamente é um processo complexo e passível de erros. A origem da maioria dos problemas está na natureza vaga, ambígua e detalhada da lei. Para tornar os princípios da LGPD mais compreensíveis para o público e com menos detalhes técnicos, eles podem ser expressados como requisitos de negócio. Mais precisamente, foi proposta a associação de cada princípio da LGPD a um requisito de negócio. A Tabela 1 ilustra um dos 10 princípios da LGPD, conforme seu artigo 6º. O modelo inclui um ID do requisito utilizado para realizar a indexação com outro componente do guia, a declaração de exigência - que é o texto legal extraído da lei -, o autor responsável por obter as informações, o número de revisão que pode ser utilizado para rastrear as alterações do requisito, a data de lançamento, as palavras-chave associadas ao requisito e, por último, o atributo conformidade legal, que identifica o artigo e o inciso referenciados. Os requisitos de negócio foram adaptados do trabalho de base [4] para se adequarem à LGPD.

3.3 Requisitos de Solução

Os requisitos de solução vinculam as obrigações da LGPD e os requisitos de negócio relacionados aos controles de privacidade necessários para cumpri-los. Eles foram adaptados do trabalho de base [4] para se adequarem à LGPD.

O modelo de mapeamento de requisitos de solução inclui espaços reservados que podem ser preenchidos com as informações que identificam os requisitos de negócio, o controle de privacidade escolhido e o cenário em que será aplicado. Quando todos os espaços reservados são preenchidos, o resultado é um requisito de solução (Tabela 2).

Tabela 1. Requisito de negócio p/ o Princípio da Finalidade (adaptado de [4])

ID do requisito:	**BREQ-1 (Business Requirement 1)**
Declaração de exigência:	A organização deve indicar pelo menos uma base legal, ou seja, uma hipótese para realizar o tratamento de dados pessoais. Antes de iniciar o processo de tratamento de dados pessoais, é importante realizar a documentação e indicar uma base legal para o princípio da finalidade. Se a finalidade mudar, a organização deve reavaliar a base legal ou pode manter a base legal original somente se a nova finalidade for compatível com a finalidade inicial.
Autor:	Fulano de Tal
Nº Revisão:	1.0
Data de Lançamento:	30/10/2020
Palavras-chave:	Base Legal, Finalidade, Princípio.
Conformidade legal:	Lei 13.709 - LGPD Art. 6º, inciso I; Art. 7º.

Tabela 2. Requisito de solução p/ o Princípio da Finalidade (adaptado de [4])

Modelo de Mapeamento para Requisito de Solução
De acordo com a LGPD, o(a) **[organização]** é obrigado(a) a cumprir o princípio **[princípio_da_LGPD]** podendo sofrer as **[consequência_da_violação].**
Este princípio é expresso pelo requisito **[ID_requerimento]**, mapeado da **[referência_legal_de_conformidade]**. Este requisito especifica **[descrição_do_requisito]**.
Para ajudar a satisfazer **[ID_requerimento]**, no contexto do **[ID_cenário]**, o profissional implementará o controle **[nome_do_controle_de_privacidade]** (identificado pelo ID **[ID_da_entrada_do_catálogo]** do catálogo de controles de privacidade) para resolver o problema **[problema_de_controle_de_privacidade]**.
Esse controle de privacidade envolve **[descrição_dos_controles_de_privacidade]**. Como resultado, **[benefício_do_controle_de_privacidade]**.

3.4 Catálogo de controles de privacidade

O catálogo apresenta os controles de privacidade que podem ser usados para atender os 10 princípios da LGPD. Ele serve para mapear a relação entre os controles de privacidade e os princípios da LGPD que eles afetam. O catálogo pode ser consultado no website do guia, que contém uma seção com as 6 etapas do guia para alcançar a conformidade da LGPD, além de um exemplo ilustrado da aplicação do método. Ainda no website, há uma seção com os componentes do guia que são usados na execução das etapas: o modelo de mapeamento de dados, os requisitos de negócio, os requisitos de solução e o catálogo de controles de privacidade. Por fim, o website conta, ainda, com um vídeo de explicação de cada elemento que compõe o guia.

O catálogo de controles de privacidade foi traduzido do trabalho de Ayala-Rivera e Pasquale [4]. Estes controles foram criados com base nas normas internacionais ISO/IEC da Família 27000 e 29100.

4 Conclusões e trabalhos futuros

Este trabalho teve como base a pesquisa realizada por Ayala-Rivera e Pasquale [4], a partir da qual algumas etapas foram replicadas. Os dois trabalhos tratam de um guia com etapas para a conformidade de uma lei de privacidade vigente, com a diferença de que a presente pesquisa trata sobre a LGPD e não sobre a GDPR. Apesar de serem leis parecidas, existem algumas diferenças e contribuições. Uma delas é o modelo de mapeamento de dados, cujo propósito é ajudar a organização a realizar a coleta das informações para cumprir a primeira etapa do guia. Outro artefato é o questionário com perguntas direcionadas aos analistas de sistemas que ajudam a compreender se o sistema atende os princípios legais. Além disso, há os controles de privacidade adaptados do trabalho de base [4] e com base nos princípios da LGPD que os contemplam.

Este trabalho apresenta algumas limitações: (i) o processo de utilização do guia ainda é manual; (ii) o fato de o guia ser extenso; e (iii) necessidade de treinamento para utilizar alguns componentes e etapas do guia.

Como trabalhos futuros temos: (i) a avaliação do guia por desenvolvedores de software; (ii) a avaliação do guia por especialistas em privacidade por meio de um grupo focal; (iii) a avaliação do guia por profissionais que não sejam de TIC, objetivando avaliar se o guia pode beneficiar outra áreas; (iv) o apoio ferramental para automatizar algumas etapas, como o mapeamento de dados pessoais; (v) ampliar o guia para abranger outros artigos da LGPD além do artigo 6º.

Agradecimentos

Este trabalho foi parcialmente apoiado pelo SETEC/MEC e FACEPE.

Referências

1. Agostinelli, S., Maggi, F.M., Marrella, A., Sapio, F.: Achieving GDPR Compliance of BPMN Process Models. In: Information Systems Engineering in Responsible Information Systems. pp. 10–22. Springer International Publishing, Cham (2019)
2. Alves, C., Neves, M.: Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso. In: Anais do WER21 - Workshop em Engenharia de Requisitos, Brasilia, Brasil. Editora PUC-Rio (2021)
3. Araújo, E., Vilela, J., Silva, C., Alves, C.: Are My Business Process Models Compliant With LGPD? The LGPD4BP Method to Evaluate and to Model LGPD Aware Business Processes. In: Proceedings of the XVII Brazilian Symposium on Information Systems. SBSI '21, ACM, New York, NY, USA (2021)
4. Ayala-Rivera, V., Pasquale, L.: The grace period has ended: An approach to operationalize gdpr requirements. In: 2018 IEEE 26th International Requirements Engineering Conference (RE). pp. 136–146 (2018)
5. BRASIL: Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais (2018), https://www.planalto.gov.br/ccivil$_0$3/$_a$*to*2015 − 2018/2018/*lei*/*l*13709.*htm*
6. EU: The EU general data protection regulation (2018), https://gdpr.eu/
7. de Oliveira Cunha, Y.L., Carvalho, M.E., Santos, T.R.R.: Impactos da transformação digital no modelo de negócios. In: Congresso Transformação Digital (2019)