Revista Boletim do Gerenciamento

Site: www.nppg.org.br/revistas/boletimdogerenciamento

Adequação da Lei Geral de Proteção de Dados via "Projetos Ágeis Scrum"

[1]CARDOSO, Domingos; CARDOSO, Thiago[2]
domsepol@gmail.com[1]; tlop2000@gmail.com[2].

[1]Analista de Sistemas, Pós-graduando em Gestão de Projetos, NPPG.
[2]Bacharel em Filosofia, Esp. em economia política, Unisul.

Informações do Artigo

Palavras-chave:
LGPD
Agile Scrum
Proteção de Dados

Resumo:

O objetivo deste artigo é apresentar um guia prático para que as empresas brasileiras consigam se adequar a LGPD (Lei Geral de Proteção de Dados, Lei 13.709 de 14 de Agosto de 2018). O modelo abordado será a metodologia SGPD – Sistema de Gestão de Proteção de Dados, via framework Agile Scrum. A LGPD foi inspirada na GDPR (General Data Protection Regulation). O SGPD é um dos métodos utilizados para gerenciamento de processos, implementação e governança de privacidade e proteção de dados. Cada etapa, das suas cinco fases do SGPD, seguem o ciclo da metodologia do PDCA - Plan (planejar), Do (fazer), Check (checar), Act (agir), que garante um controle mais eficaz dos processos e promove a melhoria contínua em cada fase planejada do projeto, para facilitar a tomada de decisão do gerente de projetos no dia a dia. Como cada empresa possui uma realidade particular, é imprescindível ter um método de trabalho adaptável; Nesse sentido, o framework Scrum demonstra, com sua robustez em ferramentas e técnicas, as quais facilitam o gerenciamento e implantação de cada uma das cinco fases do SGPD, que irá servir como um guia de boas práticas para atingir o objetivo do projeto de implementação da LGPD.

1. Introdução

1.1. A Lei Geral de Proteção de Dados e o ciclo de vida de desenvolvimento de Software

Concebida para oferecer aos cidadãos brasileiros melhor proteção aos direitos de privacidade e liberdade, a Lei Geral de Proteção de Dados está em vigor desde agosto de 2021. Este diploma legal está dividido em 10 capítulos e 65 artigos, em que se encontram os princípios que fundamentam a proteção de dados pessoais. Aplica-se a todas as organizações, que oferecem bens ou serviços, sejam elas públicas ou privadas, dentro do território nacional. Além disso, a LGPD prevê que não importa se a matriz de uma organização ou o centro de processamento de dados dela estão localizados no Brasil ou no exterior, posto que se houver a coleta e ou processamento de conteúdo de dados pessoais, de brasileiras ou estrangeiros, dentro do território nacional, a norma deverá ser cumprida em sua integralidade.

As Organizações que não estiverem adequadas à LGPD estarão sujeitas a penalidades legais como advertências e sujeitas a multas de até R$ 50 milhões ou 2% do faturamento anual [1]. Além de comprometer a sua reputação no mercado e com seus clientes e parceiros. Nesse sentido, uma vez que a insegurança cibernética assola frequentemente os noticiários com notícias de vazamentos de dados pessoais que impactam diretamente as vidas dos cidadãos de forma socioeconômica, fez-se necessária a elaboração do presente artigo.

A Lei Geral de Proteção de Dados, por sua vez, reformula a proteção de dados pessoais com o entendimento de que o processamento de dados pessoais é benéfico para a sociedade e que deve ser equilibrado com os direitos e liberdades fundamentais da pessoa humana.

O regulamento atribui a responsabilidade pela proteção de dados pessoais às organizações e espera que elas incorporem a proteção de dados em seus sistemas desde a concepção dos níveis técnicos ao âmbito organizacional.

Além disso, para o processamento de dados pessoais que representam um risco para os direitos dos indivíduos, como o caso da coleta de dados associada a novas tecnologias, um dispositivo de proteção de dados para a avaliação de impacto é obrigatório, dada a potencialidade lesiva presente.

Essa referida avaliação determina em que medida o processamento de dados dessas tecnologias pode impactar os indivíduos que as utilizam. Dessa forma, muitas organizações de Tecnologia da Informação terão de reavaliar como criam software para que possam integrar a conformidade da LGPD aos ciclos de vida de seus aplicativos, calcadas no princípio da proteção da pessoa humana.

O ciclo de vida de desenvolvimento de *software* (*SDLC - Software Development Life Cicle*) [3] é dividido nas seguintes seis fases: requisitos, design, desenvolvimento, teste, implantação e manutenção. Com efeito, percebe-se um cenário complexo e dotado de inúmeras metodologias disponíveis no mercado com diferentes abordagens de gestão de projetos para o desenvolvimento de *software*.

Para tanto, implementar uma solução que facilite a conformidade das organizações no desenvolvimento e gerenciamento de software com a LGPD não é uma questão simples. Para enfrentar esse desafio, será usado neste artigo a metodologia SGPD [4] – Sistema de Gestão de Proteção de Dados, via *framework Agile Scrum* [8].

O *Agile Scrum* suporta esse desafio pela sua robustez em ferramentas que facilitam o gerenciamento das diferentes variáveis ambientais e técnicas de um projeto como prazo, qualidade, custo, requisitos, recursos e tecnologias.

O uso do *Scrum* melhora a comunicação da equipe aumentando a produtividade devido aos seus papéis e responsabilidades serem bem definidos. A esse respeito, toda a equipe sabe o que precisa ser feito, de forma a fortalecer a motivação e o comprometimento da equipe pelo sucesso do projeto.

O *Scrum* é usado praticamente em todos os tipos de projetos por ser mais flexível e realista oferecendo um vasto *framework* com um conjunto de boas práticas que permitem auxiliar o gerenciamento do projeto em todas as suas fases.

Essa característica permite que a equipe tenha um planejamento de forma eficaz do seu trabalho que está acontecendo ao longo de todo o tempo de vida do projeto, dando visibilidade para a equipe realizar os devidos ajustes para manter o projeto dentro do escopo, prazo e custo, com o objetivo maior de alcançar os seus objetivos com qualidade e agregar valor ao cliente.

De acordo com uma pesquisa recente sobre a aderência do desenvolvimento ágil na gestão de projetos nas empresas (SCRUM MASTER TRENDS, 2019), 81% dos entrevistados usam o *Scrum* combinado com outras metodologias. Esse dado ilustra a sua importância no mundo de gestão de projetos

em diversos tipos de segmentos organizacionais.

O *Scrum*, todavia, não é uma receita de bolo descrevendo o que deve ser feito em todas as fases de desenvolvimento do projeto, mas sim uma poderosa e versátil ferramenta de tomada de decisão para o gerente de projetos em que ele poderá visualizar, controlar e gerenciar todo o clico de desenvolvimento de software, na nossa missão de adequação de software a LGPD.

2. Desenvolvimento do Texto

2.1. Vantagens da Agilidade

O Agile manifesto [7] é um conjunto de 12 princípios básicos descritos em um documento criado em fevereiro de 2001. Ele, em seu turno, traz novas sugestões para a melhoria continua de princípios, métodos e processos, para as pessoas nas organizações terem um fluxo de trabalho mais ágil, eficaz e robusto. Dentro deste contexto, o uso do *framework Scrum* na gestão de projetos traz vantagens como:

A criação de um ambiente colaborativo que incentiva a abordagem proativa entre os membros da equipe na busca da excelência em cada entrega de produto.

A facilitação no levantamento de requisitos e na gestão de mudanças devido ao envolvimento de toda a equipe em conjunto com o cliente durante as fases do projeto. Gerando entregas com mais rapidez, mantendo sempre a qualidade e escopo aderente à realidade do cliente dentro do prazo e custo.

A capacidade de gerenciamento do projeto, tendo como princípios reuniões frequentes permitindo uma melhor organização e divisão do trabalho. As equipes de trabalho possuem um perfil de serem auto gerenciadas facilitando o desenvolvimento da capacidade criativa e inovadora de seus membros promovendo a motivação no time.

O aumento significativo da satisfação do cliente por estar envolvido em todas as fases de desenvolvimento do projeto, com a contribuição no projeto, por meio de diversas demonstrações e melhorias implementadas em tempo real.

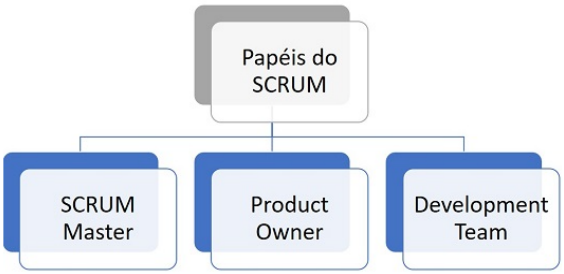
A participação grupal benéfica da equipe em relação às mudanças, posto que se inaugura o entendimento e a maturidade de que o planejamento inicial poderá sofrer mudanças ao longo da evolução do projeto. Nesse prisma, objetiva-se que o cliente esteja satisfeito com as entregas, agregando valor na operação da empresa no dia a dia.

2.2 Papéis e Responsabilidades do Scrum

O reconhecimento de cada papel e suas respectivas responsabilidades no *Scrum*, proporciona um entendimento muito maior desse *framework* para se escolher adequadamente quem deve ocupar cada um desses papéis dentro de cada time do projeto na sua empresa.

Nesse contexto, a figura número 01 visa ilustrar os Papéis do Scrum, conforme se pode observar:

Figura 1 - Papéis do Scrum



Fonte: Adaptado de DUARTE [9]

O *ScrumMaster* é o responsável por gerenciar todo processo do *framework Scrum*, já que possui características de um líder. Age como um facilitador na colaboração técnica e burocrática entre as diversas áreas envolvidas no projeto, com a construção da ponte da equipe com o cliente, com a meta de eliminar os possíveis impedimentos que possam travar a produtividade do time.

Além disso, protege a equipe de interferências externas, com a participação das reuniões diárias, revisão da Sprint, e planejamento. Assim, o *ScrumMaster* é um

verdadeiro líder-servidor, totalmente diferente de um chefe, com ênfase na disseminação das melhores práticas e valores do *Scrum* para todos os envolvidos no projeto.

O Líder-Servidor é aquele que permite e semeia no time uma cultura de cooperação mútua e contínua, no qual o líder e a equipe têm o mesmo poder de fala e influência nas decisões, possibilitando a adoção de práticas e políticas mais eficientes. Ainda assim, urge o questionamento acerca de qual forma o como o *ScrumMaster* deverá agir para atingir tal êxito laboral.

Para tanto, verifica-se que o Líder-Servidor precisará desenvolver a competência de saber escutar e valorizar as ideias e opiniões do time. Ser uma referência no time, sempre buscando e incentivando a inovação e a criatividade, bem como construir uma relação forte de confiança e respeito na diversidade de cada membro da equipe.

O Líder-Servidor precisa estar atento o tempo todo ao andamento do projeto, uma espécie de radar, identificando possíveis gargalos nas atividades do dia a dia do projeto. Dessa forma precisa desenvolver habilidades de comunicação e persuasão que alinhados com um bom relacionamento, mantendo a imparcialidade e a ética, com a equipe, clientes e parceiros serão grandes ferramentas na desobstrução de impedimentos durante a evolução do projeto.

O Líder-Servidor precisa estar atento aos sinais transmitidos pela sua equipe, para isso precisa conhecer cada membro individualmente, essa postura ajuda a perceber mudanças comportamentais e de performance no individuo no dia a dia, que podem afetar o andamento do projeto, dessa forma o quanto antes identificados esses desvios e dando o devido tratamento, melhor será o andamento e a saúde do projeto como um todo.

O *Product Owner* é o responsável por representar os interesses de todos os envolvidos (*Stakeholders*). Ele que detém o conhecimento do negócio, o que precisa ser feito, sendo assim o responsável em definir os requisitos do produto. Ele mantém o *Product Backlog* atualizada e priorizada. Possui autoridade de solicitar mudanças de requisitos e alterar prioridades a cada Sprint. Responsável em validar ou rejeitar o resultado de cada Sprint. Ele é dono do produto, não do processo.

O *Development Team* é o responsável pelo desenvolvimento das funcionalidades, da entrega final do produto. As equipes são geralmente auto gerenciadas, auto organizadas e multifuncionais, o que promove melhores resultados de performance onde cada membro da equipe é capaz de analisar, projetar, testar e documentar suas atividades.

Com esses papéis definidos, já é possível implementar o *Scrum* na empresa.

2.3 Como funciona o Ciclo do *Scrum*

Todo o trabalho é feito em *Sprints*. Cada Sprint é uma iteração bem definida, com duração de 2 a 4 semanas. Cada Sprint é iniciada com uma reunião de planejamento da Sprint (*Sprint Planning Meeting*), onde o *Product Owner* e a equipe se reúnem para priorizar sobre o que será feito para a próxima *Sprint*. Selecionando os itens do *Product Backlog* de maior prioridade, o *Product Owner* informa ao time o que é desejado a ser desenvolvido, e o time informa ao *Product Owner* uma estimativa de entrega do produto que pode se transformar em uma funcionalidade na próxima *Sprint*.

Após decidir o que deve ser feito na próxima *Sprint*, o time desenvolve a *Sprint* Backlog, ou seja, uma lista de tarefas que devem ser executadas para entregar um pacote completo da funcionalidade do produto até o final da *Sprint*. As tarefas na lista surgem à medida que a *Sprint* evolui e devem ser divididas em pacotes menores de modo que cada uma leve cerca de 4 a 16 horas para ser concluída.

Todos os dias a equipe se reúne para uma reunião de 15 minutos chamada *Daily Scrum* (*Daily Meeting*). Na *Daily Scrum*, cada membro da equipe responde a três perguntas básicas: O que você fez neste projeto desde a última reunião *Daily Scrum Meeting*? O que

você vai fazer antes da próxima reunião? Você tem algum impedimento?

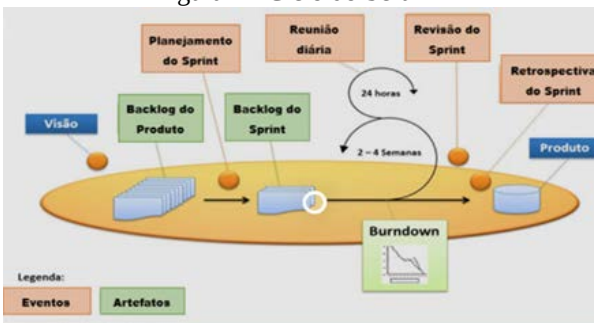
O objetivo da reunião é sincronizar o trabalho de todos os membros da equipe e acompanhar o seu progresso usando ferramentas como o gráfico chamado *Sprint Burndown* e o *Board Scrum*.

Ao final de cada *Sprint*, é realizada uma reunião de revisão do *Sprint* (*Sprint Review*), na qual o time apresenta o que foi desenvolvido durante a *Sprint* ao *Product Owner* e quaisquer outros *stakeholders* que queiram participar.

Após a revisão da *Sprint* e antes da próxima reunião de planejamento da *Sprint*, o *ScrumMaster* também realiza uma reunião de retrospectiva da *Sprint* (*Sprint Retrospective*) para incentivar o time a revisar e aperfeiçoar as melhores práticas, dentro da estrutura do processo *Scrum*, para torná-lo mais eficaz para o próximo *Sprint*.

O *ScrumMaster* ao final de cada reunião de retrospectiva (*Sprint Retrospective*) deve documentar todas as lições aprendidas em uma base dados, na intranet, visível para todos os envolvidos no projeto com a finalidade de servir como base de conhecimento de apoio nas *Sprints* seguintes e projetos futuros.

Figura 2 - Ciclo do Scrum



Fonte: Adaptado de Barbosa et al. [6]

2.4 Gerenciando o Risco

No *Agile Scrum*, a definição de um impedimento *Agile* (*Impediment Backlog*) é qualquer coisa que diminua ou dificulte a produtividade de uma equipe, afetando a entrega bem-sucedida de um produto, geralmente estão associados a riscos. Enquanto que impedimentos são uma ocorrência normal em uma equipe *Agile Scrum* e podem ocorrer a qualquer momento devido à complexidade e dinâmica envolvida no processo de desenvolvimento do produto.

Um impedimento ocorre de diferentes formas, podendo se expressar como um recurso ausente ou um *bug* que aparece durante o desenvolvimento ou teste de um produto. Também podem estar relacionados a outros obstáculos relacionados a negócios, infraestrutura, clientes e parceiros.

É notável que a maioria dos impedimentos atrasa o progresso do projeto. Por isso, nota-se a importância do *ScrumMaster* para identificar, rastrear e remover as possíveis problemáticas. Outras vezes, os membros da equipe também podem desempenhar um papel na identificação de impedimentos e reportar ao *ScrumMaster*.

O primeiro passo é identificar os impedimentos e fazer com que todos os membros da equipe entendam o impacto dentro do projeto.

Uma vez identificados os impedimentos, devemos criar um registro no quadro de tarefas (*Board Scrum*) para que toda equipe possa visualizar claramente os obstáculos no caminho do trabalho.

O próximo passo é identificar a causa raiz dos impedimentos. Isso é mais eficaz do que se concentrar numa solução de contorno pontual. A solução de contorno pode ser usada em casos específicos e de forma controlada.

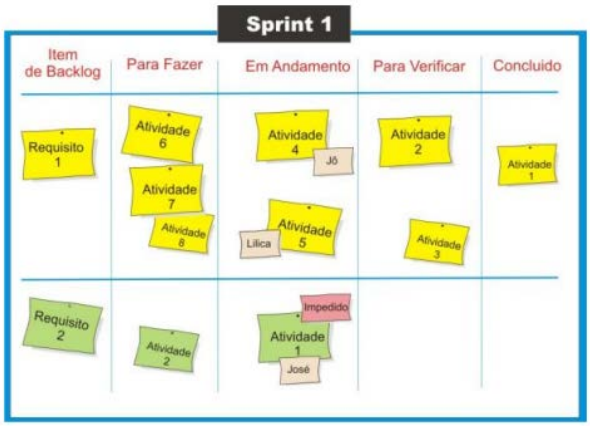
Ao final da observação minuciosa, com a solução da causa raiz, o *ScrumMaster* deve atualizar o *Board Scrum*.

2.5 Ferramenta de Controle *Board Scrum*

O *Board Scrum* é usado basicamente para organizar e acompanhar o andamento das tarefas em tempo real da equipe, para monitorar a fila priorizada do *Backlog* da *Sprint*, identificar possíveis gargalos ou picos

de demandas na fila de cada membro do time e pode-se indicar se existe algum impedimento em alguma tarefa. O *board Scrum* tem uma identidade visual objetiva, em que basta olhar para o quadro e ter uma leitura detalhada de como estar o andamento do projeto.

Figura 3 - Ilustra um quadro de trabalho Scrum (board Scrum).

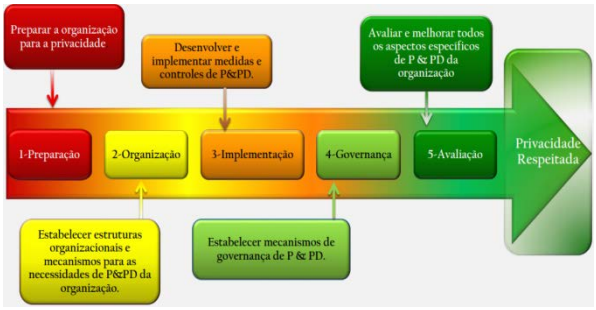


Fonte – Elaborado pelo autor.

2.6 A metodologia SGPD

A metodologia SGPD (Sistema de Gestão e Proteção de Dados) proposta pelo autor John Kyriazoglou [4] é um dos métodos, dentre outros, utilizados para gerenciamento de processos, implementação e governança de privacidade e proteção de dados, que tem como objetivo propiciar o melhor controle e gestão dos dados pessoais nas organizações, de forma que seja possível mapear as operações de tratamento de dados pessoais.

Figura 4 - Ilustra as fases de uma SGPD.



Fonte: Adaptado de KYRIAZOGLOU [4]

O SGPD é um framework internacional também aplicável a implementação da LGPD, possui cinco fases sequenciadas: (1) preparação, (2) organização, (3) implementação, (4) governança e (5) melhoria. Com o *Scrum*, gerenciaremos todo o projeto, entregando-o gradualmente de acordo com a priorização do *Backlog* do produto (*Product Backlog*) em fases bem definidas chamadas de *Sprints*.

O *Scrum* visa eliminar a possibilidade de frustração de entregar algo não solicitado pelo cliente, aumentando o valor agregado do produto, pois cada fase (*sprint*) do projeto é previamente selecionada do *Backlog* do produto, uma lista de histórias de usuários que expressam os requisitos de software de forma objetiva, conforme alinhamento na reunião (*Sprint Planning Meeting*) com a participação do *Product Owner* responsável pela priorização das tarefas, o que garante que os requisitos mapeados sejam atendidos de acordo com a criticidade do negócio, agregando valor para o cliente, antes de se prosseguir para a próxima fase, garantido a satisfação do cliente.

Cada etapa, das cinco fases da SGPD será entregue entre duas até quatro semanas, chamadas *sprints*, de modo que, se algo tiver que ser mudado em qualquer fase, isso poderá ser feito dentro da própria *sprint*, diminuindo o tamanho do retrabalho caso o projeto fosse entregue de uma vez só (o que acontece na metodologia tradicional, “Cascata”).

Essa abordagem permite a geração de tarefas (*Sprints*) com base em histórias de requisitos de usuários. Embora a LGPD esteja estruturada em 10 capítulos, com 65 artigos, iremos implementar somente o que legalmente se aplica ao negócio do cliente de acordo com sua necessidade e prioridade.

2.7 Descrição do estudo de caso do projeto

A SIGA Sistemas empresa fictícia, foi fundada em 1979 na cidade do Rio de Janeiro, com o objetivo de desenvolver sistemas para gestão de empresas (ERP). A empresa foi idealizada com o objetivo de otimizar e

integrar os processos de gestão de empresas, oferecendo o mais alto nível de qualidade e segurança em desenvolvimento de software.

A SIGA Sistemas é umas das principais empresas no ramo de desenvolvimento de *softwares* para diversas áreas, com atividade nacional, a SIGA Sistemas está presente em diversos estados brasileiros, suas filiais estão espalhadas em vários estados brasileiros, como a Bahia, Goiânia, São Paulo e Rio Grande do Sul.

A empresa é reconhecida por atuar na resolução de problemas complexos, com a tecnologia como pilar estratégico e inovação, eliminando assim problemas que evitam o crescimento das organizações de seus clientes.

O ERP SIGA Sistemas possui vários módulos integrados (Recursos Humanos, Faturamento, Compras) que coletam dados pessoais e informações de saúde do usuário, incluindo por exemplo, nome, endereço, altura, peso, sexo, salario, histórico de saúde e outros dados sensíveis.

O ERP SIGA Sistemas processa essas informações através de uma interface web chamada, *SigaWebClient*, na estação de trabalho dos usuários, em seguida realiza a transferência dos dados coletados para um datacenter na nuvem usando link de comunicação onde as informações são armazenadas em um banco de dados.

A solução proposta neste artigo é adicionar regras de segurança e privacidade no acesso e manipulação dos dados dos usuários em aplicações do mesmo segmento que a Siga Sistemas, seguindo o que é determinado pela LGPD.

2.8. Lei Geral de Proteção de Dados e Histórias de Requisitos de Usuários

A LGPD inclui vários artigos e consideramos os que se aplicam a sistemas de gestão de empresas que coletam e manipulam dados pessoais, mostrado na tabela 2. Usando esses artigos como base, foram compiladas as epopeias em histórias de requisitos de usuários que demonstram a necessidade de adequação do sistema de gestão de empresas SIGA Sistemas a LGPD.

No caso do projeto de Sistema de Gestão de empresas, SIGA Sistemas, os requisitos da LGPD são claramente definidos e mapeados em histórias de requisitos de usuários, mostrado na tabela 2. Essa mesma estratégia pode ser usada para qualquer projeto de mesma natureza. Funcionando como um trampolim universal para a criação de um projeto ágil.

Tabela 2 – História de requisitos de usuários catalogadas no *backlog* de produto (*Product Backlog*) para uma solução semelhante proposta neste artigo.

Épico	**Proteção de dados pessoal**
Tag	Proteção de dados: dados confidenciais
História de requisito de usuário	Como usuário, o objetivo é que os dados confidenciais sejam protegidos para que os indivíduos possam ter direito a privacidade e segurança.
Artigo	Artigo 46

Fonte – Elaborado pelo autor.

2.9 Execução da *Sprint*

Colocando-se tarefas (*sprints*) específicas do projeto sob cada história de requisito de usuário previamente catalogada e priorizada no *backlog* do produto (*Product Backlog*) e, deste modo, utilizando esta estratégia que une a metodologia *Agile* com conformidade a LGPD, qualquer empresa desenvolvendo qualquer projeto *Agile*, poderá rastrear sua conformidade a LGPD, ou seja, verificar sua necessidade de adequação, preparando-se para o projeto de implementação da LGPD.

A próxima etapa é atribuir *tags* às tarefas de privacidade de cada fase *(sprints)* e, em seguida, vincular essas tarefas às histórias de requisitos de usuário e suas respectivas *tags*. Tabela 3 mostra três tarefas (*sprints*) de privacidade agrupadas em uma história de requisito de usuário usando a tag apropriada.

Também é mostrado em tabela 3 uma lista de controles de privacidade e segurança, como aqueles que estão disponíveis em soluções de requisitos de segurança de aplicativos e gerenciamento de ameaças (SGPI).

Esses controles podem ser facilmente organizados usando *tags* para que a proteção de dados confidenciais esteja diretamente relacionada à conclusão de tarefas em um repositório de controles de segurança.

Tabela 3 – Vinculando tarefas (sprint) com o backlog do produto de acordo com as histórias de requisitos de usuários.

Épico	**Proteção de dados pessoal**
Tag	Proteção de dados: dados confidenciais
História de requisito de usuário	Como usuário, o objetivo é que os dados confidenciais sejam protegidos para que os indivíduos possam ter direito a privacidade e segurança.
Tarefas (*sprints*)	T171: Implementar política de perfil de acesso por usuário e grupos.Com regras de controle de acesso por senhas seguras e ou biometria. T189: Implementar protocolos de segurança e criptografias dos dados para transmitir as informações pela Intranet e Internet. T936: Testar se o aplicativo usa as funcionalidades implementadas com a segurança desejada.

Fonte – Elaborado pelo autor.

3. Considerações Finais

Tendo como o objetivo deste artigo é apresentar um guia prático para a implementação da LGPD, utilizando-se do *framework Scrum Agile*. Essa metodologia, em que o trabalho é feito em fases (*sprints*) devidamente priorizadas, permite que a LGPD seja pensada e aplicada desde o princípio do projeto para agregar valor ao negócio do cliente.

O gerenciamento do projeto, via metodologia *Agile Scrum*, tem como uma das vantagens o fato de que o trabalho é revisado a cada duas semanas (em média) com o acompanhamento em tempo real do cliente, evitando retrabalhos e garantindo maior assertividade nas entregas de cada fase (sprints). Através das figuras, é apresentado uma visão geral para a implementação da LGPD por meio de utilização de *tags*, epopeias e histórias de requisitos de usuários, fazendo a conformidade da LGPD.

Essa nova abordagem de histórias de requisitos de usuários, priorizadas no *backlog* do produto, podem agilizar a geração de tarefas *(sprints)* e auditoria em todas as fases do projeto, facilitando tanto o gerenciamento do projeto quanto a implementação em conformidade com a LGPD. Deste modo, une-se conformidade a LGPD ao gerenciamento de projeto por métodos *agiles*, garantindo à adequação do cliente a legislação da LGPD.

4. Referências

[1] BRASIL. Decreto n° 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais, Brasília*, DF, ago 2018. Disponível em: Acesso em: 12 mar. 2020.

[2] PEIXOTO, Mariana Maia. *Privacy Requirements Engineering in Agile Software Development: a Specification Method.* In: REFSQ Workshops. 2020.

[3] METADE, R . *Seis metodologias básicas de SDLC: Qual é o melhor?* 21 de novembro de 2017, https://www.roberthalf.com/blog/salaries- andskills/6-basic-sdlc-methodologies-which- oneis-best.

[4] KYRIAZOGLOU, John Vol 1, Editora: bookboom.com: Data Protection and Privacy Management System. 2016.

[5] GDPR, (2018 27 de abril) Lei n° 679. *Regulamento do Parlamento Europeu e do Conselho, dispõe sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.* Recuperado de https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT.

[6] BARBOSA, M. W.; CARVALHO, L. A.; SILVA, V. B. EU *Scrum: uma abordagem lúdica para o ensino de estórias de usuário e Scrum*. Revista Gestão de Projetos, São Paulo, v. 5, n. 3, p. 44-58, set./dez. 2014.

[7] AGILE MANIFESTO. *Manifesto for Agile Software Development.* 2001. Disponível em http://agilemanifesto.org/ Novembro, 2005

[8] SCHWABER K., *Agile Project 2004 Management With Scrum*. Microsoft,

[9] DUARTE, Luiz. Escritório de Projetos 2022. Disponível em: https://escritoriodeprojetos.com.br/papeis-do-scrum

1. Anexos e Apêndices

ANEXO A

Tabela 1 – Glossário com os principais termos-chave da LGPD

Termos-chave	Significado
Agentes de tratamento	O controlador e o operador
Anonimização	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada
Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais
Eliminação	Exclusão de dado ou de conjunto de dados armazenados em banco de dados, Independentemente do procedimento empregado
Tratamento	Toda operação realizada com dados pessoais
Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
Dado pessoal	Informação relacionada à pessoa natural identificada ou identificável
Autoridade nacional	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (ANPD)
Garantia da segurança da informação	Capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A Política Nacional de Segurança da Informação (PNSI) dispõe sobre a governança da segurança da informação aos órgãos e às entidades da administração pública federal em seu âmbito de atuação
Encarregado – (DPO)	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador

ANEXO B

Tabela 2 – História de requisitos de usuários catalogadas no *backlog* de produto (*Product Backlog*) para uma solução semelhante proposta neste artigo.

Épico	Tag	Historias de usuarios	Artigos
Coletar dados de privacidade	Proteção de dados: Anomimizado	Como Controlador, o objetivo é proteger os dados pessoais de forma que se possa fornecer privacidade aos titulares dos dados e não ser capaz de associar os dados pessoais processados a qualquer indivíduo específico.	Artigo 5
Coletar dados de privacidade	Proteção de dados: Integridade e Precisão	Como Controlador, o objetivo é verificar , manter , proteger a integridade e exatidão dos dados pessoais no sistema .	Artigo 6
Coletar dados de privacidade	Proteção de dados: Identificação Indireta	Como usuário, o objetivo é ser capaz de fornecer ou retirar consentimento para o uso de dados em identificadores que podem ser associados a indivíduos quando combinados com seus dados pessoais.	Artigo 5
Coletar dados de privacidade	Proteção de dados: Identificação Indireta	Como usuário, o objetivo é poder receber serviços customizados de um aplicativo sem ser identificado direta ou indiretamente para que os indivíduos possam proteger sua privacidade.	Artigo 5
Permissão de processamento de dados	Processamento: Consentimento	Como Controlador, o objetivo é acessar documentos sobre os motivos da necessidade de coletas de dados e poder obter o consentimento de processamento de dados pessoais para determinar a conformidade com o LGPD.	Artigo 7
Permissão de processamento de dados	Processamento: Consentimento	Como Controlador, o objetivo é saber sobre as atividades de processamento e o tipo de dados que estão sendo coletados para que as partes interessadas possam determinar os fundamentos legais para o processamento e coleta de tipos de dados.	Artigo 7
Obter consentimento para processamento de dados pessoais	Aquisição/ Cancelamento	Como um usuário, o objetivo é ser capaz de fornecer ou retirar o consentimento para o processamento de dados pessoais.Para que os indivíduos possam ter controle sobre como seus dados pessoais são processados.	Artigo 15
Seja transparente no processamento de dados pessoais	Transparência: Acesso a dados pessoal.	Como usuário, o objetivo é ser capaz de acessar facilmente informações sobre as atividades que envolvem dados pessoais de indivíduos de forma clara e linguagem compreensível para que possam exercer o seu direito de ver os seus dados pessoais processados.	Artigo 6
Seja transparente no processamento de dados pessoais	Transparência: Motivo manipulaão de dados pessoal.	Como usuário, o objetivo é receber informações sobre as atividades de processamento de dados , para que possam exercer o seu direito à informação sobre o motivo pelo qual os seus dados pessoais são processados no ambito comercial e industrial.	Artigo 6
Determinar de forma objetiva as razões para processamento de dados pessoal	Propósito: Identificãoe Limitação	Como usuário, o objetivo é conhecer a finalidade do processamento de dados pessoais e fornecer apenas as informações necessárias para cumprir essa finalidade, de forma que os indivíduos possam evitar a divulgação desnecessária de seus dados pessoais para proteger sua privacidade.	Artigo 6

Tabela 3 – Elaboração de cenário de implantação LGPD (continuação).

Permissão de processamento de dados	Dados sensíveis Categorias Especiais De dados	Como Controlador, o objetivo é acessar documentos sobre as bases legais para o processamento de dados confidenciais (incluindo dados de saúde e origem étnica) para que sua conformidade com a LGPD possa ser determinada.	Artigo 37
Permissão de processamento de dados	Processamento: Interesse legítimo	Como Controlador, o objetivo é acessar documentos sobre os motivos de interesses legítimos para o processamento de dados pessoais para que se possa determinar sua conformidade com a LGPD.	Artigo 37
Proteção de dados pessoal	Proteção de dados: dados confidenciais	Como usuário, o objetivo é que os dados confidenciais sejam protegidos para que os indivíduos possam ter privacidade e segurança.	Artigo 46
Realizar notificação ao usuário	Aviso: Aviso	Como usuário, o objetivo é obter informações sobre as atividades de processamento de dados pessoais durante sua operação, para que os indivíduos possam exercer o direito de saber como seus dados pessoais são processados e para qual a sua finalidade real.	Artigo 6
Implementar controle de Acesso a dados pessoal	Acesso: Informação	Como usuário, o objetivo é poder acessar informações sobre atividades de processamento de dados pessoais e ter informações sobre como os dados dos indivíduos são processados para que possam decidir se desejam continuar a usar um sistema.	Artigo 6
Proteção de dados pessoal	Proteção de dados: Identificação	Como Controlador, o objetivo é assegurar que apenas usuários com identidades verificadas tenham acesso aos dados pessoais para que a privacidade dos usuários possa ser protegida.	Artigo 46
Implementar controle de acesso a dados pessoais	Acesso: Editar / Atualizar	Como usuário, o objetivo é ser capaz de editar e atualizar informações em um sistema para que os indivíduos possam garantir a precisão e ter controle sobre seus dados.	Artigo 18
Implementar controle de acesso a dados pessoais	Acesso: Remoção	Como usuário, o objetivo é ser capaz de solicitar a remoção imediata de dados pessoais de um sistema sob certas condições, para que os indivíduos possam limitar a forma como seus dados são usados.	Artigo 18
Implementar controle d acesso a dados pessoais	Restrição de acesso	Como usuário, o objetivo é poder enviar um pedido para interromper as atividades de processamento de dados pessoais sob certas condições, para que os indivíduos possam exercer o seu direito de restringir o processamento dos seus dados pessoais.	Artigo 18
Implementar controle de acesso a dados pessoal	Acesso: portabilidade	Como usuário, o objetivo é exportar dados pessoais armazenados em um formato legível por meio digital para que os usuários possam enviá-los a outros controladores e ou empresas.	Artigo 18

Proteção de dados pessoal	Proteção de dados: Confidencialidade	Como Controlador, o objetivo é tomar medidas de segurança adequadas para que a confidencialidade dos dados do usuário possa ser protegida.	Artigo 46
Implementar segurança relatórios de risco	Gerenciamento de riscos: Gestão da segurança	Como Controlador, o objetivo é ter relatórios de risco. Para que os planos de mitigação de risco de controle de vazamento de dados pessoal possam ser desenvolvidos.	Artigo 37
Implementar privacidade relatórios de risco	Gerenciamento de riscos: Gestão da segurança	Como Controlador, o objetivo é ter relatórios de risco. Para que os planos de mitigação de risco de controle a acesos indevidos possam ser desenvolvidos.	Artigo 37
Coletar dados essenciais	Coleta de dados: dados Com Anomimizado	Como o usuário, o objetivo é que a quantidade mínima de dados pessoais seja coletada para atividades de processamento, para que os indivíduos possam evitar a divulgação desnecessária de seus dados.	Artigo 5
Criar e manter processamento de registros	Responsabilidade: Documentação/ Demonstração	Como Controlador, o objetivo é ter um registro do processamento de dados pessoais e das atividades do usuário, como fornecer consentimento, para que esses registros possam ser fornecidos ao orgão controlador.	Artigo 37
Enviar dados de notificações de violação	Auditoria: Incidente Comunicando	Como usuário, o objetivo é ser notificado imediatamente sobre as consequências de uma violação de dados para que os indivíduos possam se proteger de danos físicos e financeiros.	Artigo 48
Permissão de processamento de dados	Processamento: Consentimento	Como Controlador, o objetivo é acessar documentos sobre os fundamentos do processamento de dados pessoais para que se possa determinar sua conformidade com o LGPD.	Artigo 37
Permissão de processamento de dados	Conformidade: Escopo	Como Controlador, o objetivo é acessar documentos sobre o processamento de dados pessoais para que se possa determinar se o processamento é consistente dentro do escopo da LGPD.	Artigo 37

ANEXO C

Tabela 3 –Vinculando tarefas (*Sprints*) com o *backlog* de produto (*Product Backlog*) priorizada com as histórias de requisitos de usuários.

Épico	**Tag**	**História de requisito de usuário**	**Tarefas (*sprints*)**
Proteção de dados pessoal	Proteção de dados: dados confidenciais	Como usuário, o objetivo é que os dados confidenciais sejam protegidos para que os indivíduos possam ter direito a privacidade e segurança.	T171: Implementar política de perfil de acesso por usuário e grupos.Com regras de controle de acesso por senhas seguras e ou biometria. T189: Implementar protocolos de segurança e criptografias dos dados para transmitir as informações pela Intranet e Internet. T936: Testar se o aplicativo usa as funcionalidades implementadas com a segurança desejada.